## AGENDA

### Executive Session to discuss:
- **C.G.S. 1-200(6)[E]** – Preliminary drafts or notes that the public agency has determined that the public’s interest in withholding such documents clearly outweighs the public interest in disclosure. [1-210(b)(1)]
- **C.G.S. 1-200(6)[E]** – Records or the information contained therein pertaining to strategy and negotiations with respect to pending claims regarding Recovery Audit Contractor (RAC) Audits [1-210(b)(4)]
- **C.G.S. 1-200(6)[E]** – Records, reports and statements privileged by the attorney-client relationship. [1-210(b)(10)]
- **C.G.S. 1-200(6)[C]** – Records of standards, procedures, processes, software and codes not otherwise available to the public, the disclosure of which would compromise the security and integrity of an information technology system. [1-210(b)(20)]

### Opportunity for Public Comments
- None

### Minutes of the May 17, 2016 JACC Meeting
- Approval

### Storrs & UConn Health Significant Compliance Activities
- **Athletics – NCAA Compliance Update**
- Update

### Storrs & UConn Health Significant Audit Activities
- **Status of Audit Assignments**
- **Audit Follow-up Activity**
- **Status of Corrective Actions**
- Update

### 2017 Draft Audit and Compliance Plans
- Approval

### External Engagements
- Approval to Hire CohnReznick – UCONN 2000 Construction Project Expenditure Annual Audit and Agreed Upon Procedures
- Approval to Hire BKD – Annual NCAA Agreed-Upon Procedures to the Statements of Revenues and Expenses of the UConn Athletics Program
- Approval

### Auditor of Public Accounts
- Presentation

### Informational/Educational Items
- Compliance Newsletters – UConn & UConn Health
- Current Issues in Compliance Newsletters – UConn & UConn Health
- Information Only

### Conclusion of Full Meeting
- Information Session with OACE and External Auditors

---

*The next meeting of the JACC will be held on Wednesday, December 14, 2016 at 10:00 am*  
*Rome Commons Ballroom, Storrs*
University of Connecticut
&
UConn Health

Joint Audit & Compliance Committee Meeting
University of Connecticut & UConn Health
Joint Audit & Compliance Committee Meeting

Meeting Minutes from May 17, 2016

<table>
<thead>
<tr>
<th>Attendees</th>
<th>F. Archambault, S. Cantor, R. Carbray, T. Holt, T. Kruger, and D. Nayden</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustees / Directors Present:</td>
<td></td>
</tr>
<tr>
<td>State Auditors:</td>
<td>J. Carroll, W. Felgate, N. Freitas, J. Rasimas and G. Slupecki</td>
</tr>
<tr>
<td>RSM:</td>
<td>M. Bloom</td>
</tr>
</tbody>
</table>

The meeting of the Joint Audit and Compliance Committee (JACC) was called to order at 10:00 a.m. by Trustee Nayden.

**ON A MOTION** made by Trustee Nayden and seconded by Trustee Carbray, THE JACC VOTED to go into executive session to discuss:

- C.G.S. 1-200(6)[E] – Preliminary drafts or notes that the public agency has determined that the public’s interest in withholding such documents clearly outweighs the public interest in disclosure. [1-210(b)(1)]
- C.G.S. 1-200(6)[E] – Records or the information contained therein pertaining to strategy and negotiations with respect to pending claims regarding Recovery Audit Contractor (RAC) Audits. [1-210(b)(4)]
- C.G.S 1-200(6)[E] – Records, reports and statements privileged by the attorney-client relationship. [1-210(b)(10)]
- C.G.S. 1-200(6)[C] – Records of standards, procedures, processes, software and codes not otherwise available to the public, the disclosure of which would compromise the security and integrity of an information technology system. [1-210(b)(20)]


The Executive Session ended at 11:36 a.m. and the JACC returned to open session at 11:37 a.m.

There were no public comments.

**ON A MOTION** made by Trustee Nayden and seconded by Trustee Carbray the order of the agenda was adjusted to accommodate presenter’s availability.

**Tab 1 – Minutes of the Meeting**

**ON A MOTION** made by Trustee Nayden and seconded by Director Archambault the minutes of the February 3, 2016, JACC meeting were approved.
K. Fearney provided an update on the Minors Protection Program and Freedom of Information requests.

D. Galloway updated the committee on the proposed Annual Compliance Reports and a Three-Year Compliance Work Plan.

He also announced that Paul McCarthy will be joining OACE as Compliance Counsel in June.

Due to restricted time, I. Mauriello’s update on significant compliance activities was deferred.

C. Molin gave an overview of the Drug Free Schools and Workplace program at UConn Health.

J. Geoghegan provided an update on ICD-10 at UConn Health.

C. Chiaputti provided the JACC with an update on the status of audit assignments (Storrs and UConn Health). OACE completed five of the six audits presented and had fifteen audits in progress during this reporting period.

The committee was also provided with the status of OACE’s audit recommendation follow-up activities.

The Executive Risk Management and Compliance Committee – Storrs Charter was provided to the committee for information. There were no changes to the charter and no additional discussion.

M. Bloom of RSM presented the UConn 2000 Construction Projects’ Expenditures Annual Audit and Agreed Upon Procedures for FY15.


The committee was provided with the following:

- Compliance Newsletters – Storrs,
- Current Issues in Compliance Newsletters – Uconn and UConn Health.

There being no further business, ON A MOTION made by Trustee Nayden and seconded by Trustee Kruger, the meeting was adjourned at 12:15 p.m.

Respectfully submitted,

Angela Marsh
University of Connecticut & UConn Health

Joint Audit & Compliance Committee Meeting
SIGNIFICANT COMPLIANCE ACTIVITIES

STORRS

**Annual Compliance Training** – The 2015/2016 Compliance Training period concluded in June, with 100% of faculty and staff completing the training. We continue to work with the Graduate School and the Department of Human Resources on completion rates for new and continuing Graduate Assistants.

**Minor Protection Program** – A total of 89 University-sponsored youth activities registered with the Minor Protection Program during the period of April 1 – September 9, 2016. These programs collectively served 3,101 children and youth. During this same period, a total of 863 individuals successfully completed UConn’s minor protection training and 364 satisfied the University’s background check requirements for Authorized Adults.

In an effort to continue to provide targeted technical assistance and validate compliance with formal requirements, the Minor Protection Program will begin to incorporate on-site visits to its monitoring and evaluation efforts. Other initiatives underway include, incorporating Protection of Minors provisions into Facilities Use Agreements with entities who use or lease University property to operate youth activities, continuing to assess and address emerging risks (including for activities beyond the current scope of the Policy), and enhancing existing training and educational resources.

Though still in its first year of implementation, UConn’s minor protection efforts were recently highlighted at the 2016 Higher Education Compliance Conference, and the September/October 2016 edition of the American Camp Association (ACA) Camping Magazine. We hope to continue to raise awareness of leading Protection of Minors practices and the University of Connecticut’s efforts in that area.

**University Policy Protocol** – OACE has proposed a single, University-wide policy to address the approval, revision and decommissioning of official University policies. The policy will apply to the Storrs, Regional and UConn Health campuses.
SIGNIFICANT COMPLIANCE ACTIVITIES

UConn Health

• Overpayment refunds –
  o There are no new overpayment refunds to report since the May 2016 JACC meeting.

• Compliance Monitoring –
  o Work is underway to use a data analytic tool (ACL) to data mine as a means of monitoring compliance with various CMS payment rules.

• 2016 Annual Compliance and HIPAA training – Launch of annual training is planned for the Fall of 2016.

• Key Compliance Programs: OACE continues to work with the UConn Health administration to develop formal documented compliance programs for a variety of key compliance areas:
  o Fitness-for-Duty Privacy – resides with management in final stages
  o Workplace Violence, Violence Against Healthcare Workers – resides with management for action
  o Stark Process Flowcharting – initial stages of evaluation by compliance
  o HIPAA Privacy and Security – Taskforce approach. Privacy benchmark study conducted to include ten similarly situated Academic Medical Centers. Results will be discussed in taskforce meeting.
  o Drug-Free Schools, Drug-Free Workplace – management required actions are underway.
  o Non-discrimination compliance – collaborative committee with key stakeholders and the Office of Institutional Equity.
  o Higher Education Opportunities Act – initial stages of compliance review.
  o Medical Identity Theft Process Flowcharting – completed by compliance. Next steps are committee review.
  o Office of Civil Rights Phase II Audits Readiness for HIPAA compliance - High Risk component review underway. This review resulted in a project for identification and tracking of all Business Associate Agreements at UConn Health. This project is nearing completion.
PROSPECTIVE STUDENT ATHLETES

A prospective student-athlete (also referred to as a PSA or recruit), is an individual who has started classes for the ninth grade. In addition, any individual receiving benefits from the University of Connecticut would trigger prospect status.

A prospective student-athlete remains a prospect even after he or she has signed a National Letter of Intent to attend the University of Connecticut.

RECRUITING

Recruiting is any intentional effort to solicit an individual for the purpose of securing the enrollment and ultimately the athletic participation at the institution.

Recruiting is the responsibility of and conducted by the coaches of each sports program. Recruiting may also involve members of UConn Division of Athletics or campus faculty. It is not permissible for any representatives of athletics’ interest, general public or fans to recruit on behalf of UConn.

• YOU MAY be of assistance by forwarding all information about PSAs to coaches.

• YOU MAY continue to maintain friendships previously developed (prior to the individual entering the 9th grade) with prospects. However, NCAA rules governing benefits may still apply in some circumstances, and should be approved by the Office of Athletics Compliance.

INSTITUTIONAL RESPONSIBILITY

The University of Connecticut must abide by the rules and regulations established by the NCAA and the applicable conferences (American Athletic Conference, Big East and Hockey East) as they apply to all aspects of its athletics program. In addition to ensuring that all of its coaches, administrators, and student-athletes are aware of and following the NCAA rules, The University of Connecticut is responsible for the actions of any individual who is deemed to be a representative of UConn’s athletic interests.

CONTACT US

If you have additional questions or concerns about the rules and how they apply to your involvement with our student-athletes or prospective student-athletes, please contact the UConn Office of Athletics Compliance.

Office of Athletics Compliance
University of Connecticut
2095 Hillside Road, U-1173
Storrs, CT 06269-1173

(860) 486-1211
Fax: (860) 486-2245

UConnHuskies.com

@UConnCompliance

INTERCOLLEGIATE ATHLETICS
DONOR & FAN GUIDE
REPRESENTATIVE OF ATHLETICS INTERESTS

You are considered a “representative of UConn’s athletics interest” if you have ever:

- Been a member of the UConn Club or any group which supports athletic teams.
- Contributed to any UConn athletics program.
- Purchased season tickets for athletics contests.
- Participated as a varsity student-athlete at UConn and/or are an alumnus of UConn.

OFFERS AND INDUCEMENTS

UConn staff members or representatives of athletics’ interest may not directly or indirectly provide or arrange for the provision of, or offer of any financial aid or other benefits to a prospect (or the prospect’s relatives, legal guardians or friends) other than expressly permitted by the NCAA regulations. This shall apply regardless of whether similar financial aid benefits or arrangements are available to prospective students in general.

Specifically prohibited items include, but are not limited to:

- Arranging employment for a prospect’s relatives;
- Free or reduced-cost services, rentals or purchases of any type;
- A gift of clothing, merchandise or any tangible item;
- Co-signing of a loan;
- Providing a loan to a prospect’s relatives and friends;
- Cash or like items;
- Free or reduced-cost housing;
- Sponsorship of, or arrangement for, an awards banquet for high school, preparatory school or two-year college athletes by an institution, its athletics representatives, or its alumni groups or booster groups.

CURRENT AND FORMER STUDENT-ATHLETES

Under NCAA legislation, any extra benefit provided to a UConn student-athlete (his/her relatives, legal guardian or friends) would be considered impermissible.

Extra benefits include, but are not limited to the following:

- Cash or loans in any amount;
- Co-signing or arranging a loan;
- Gifts or free services (airline tickets, restaurant meals, summer storage space, event tickets);
- Use of an automobile;
- Rent-free or reduced-cost housing;
- Employment of a student-athlete at a higher rate than wages paid for similar work;
- Payment to a student-athlete for work not performed;
- Transportation;
- Promise of employment after college graduation;

PERMISSIBLE WAYS TO GET INVOLVED

Representatives of athletics’ interest are permitted to host an occasional meal in their home for a team or group of student-athletes. All meals must be pre-approved by the UConn Office of Athletics Compliance, and there are monthly and annual limits to the number of meals that can be provided. Transportation may also be provided for student-athletes eating such a meal at a representative’s home.

POSSIBLE PENALTIES FOR IMPROPER ACTIONS

Violations of NCAA rules are a serious matter. There are many penalties the institution or NCAA may impose upon a student-athlete, an institution, a coach, or a representative of UConn athletics’ interests. In some instances, the NCAA may impose penalties on an institution even if the student-athlete involved in the violation has no eligibility remaining or is no longer attending the school. Some penalties the NCAA may impose on an institution include:

- Ceasing recruitment of the prospective student-athlete;
- Loss of eligibility of an enrolled student-athlete;
- Having to sit out competition for a limited period of time (enrolled student-athletes);
- Forfeiture of competitions;
- Prohibiting a coach from recruiting off-campus for a period of time;
- Institutional fines;
- Suspension of a coach for one or more competitions;
- Reduction in the number of scholarships an institution may award in a sport(s);
- Reduction in the number of expense-paid recruiting visits that an institution may provide;
- Prohibiting a team from participating in postseason competition;
- Institutional probation;
- Complete disassociation of relations with a representative of athletics’ interests for a specified period of time.
University of Connecticut
&
UConn Health

Joint Audit & Compliance
Committee Meeting

TAB 3
THIS PAGE INTENTIONALLY LEFT BLANK
### Status of Assignments

<table>
<thead>
<tr>
<th>Audit Project</th>
<th>Storrs or UConn Health (UH)</th>
<th>Planning</th>
<th>Fieldwork</th>
<th>Pre-draft Draft Reporting</th>
<th>Final Draft Report Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty Consulting FY 15</td>
<td>Storrs/UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Emergency Preparedness</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Correctional Managed Health Care Pharmacy</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Transportation &amp; Parking Services</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hartford Campus Relocation Project – Report 1</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Clinical Overtime Payment</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Regenerative Medicine Research Fund Awarded Project Expenditures – FY16</td>
<td>Storrs/UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>LCD: Outpatient Physical &amp; Occupational and Speech Therapy Services</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Research Data Security</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>2nd Change Order Monitoring Review - (on hold)</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Cash Receipts / Cash Handling</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Innovation Partnership Building (IPB)</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Space Management Process</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Cancer Center</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Foundation – FY16</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Clinical Contracts</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>UConn Health One Implementation Audit</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Travel</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Respiratory Therapy</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Purchasing – Contract Administration</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Mandatory Training Compliance</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Energy Service Corporation Project</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Family Medical Leave Act (FMLA)</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Family Medical Leave Act (FMLA)</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>School of Law Financial Aid</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Pharmacy IT</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>TOTAL AUDITS (26)</td>
<td></td>
<td>(06)</td>
<td>(10)</td>
<td>(01)</td>
<td>(09)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Special Projects/Consulting</th>
<th>Storrs or UConn Health (UH)</th>
<th>Planning</th>
<th>Field Work</th>
<th>Review Pre-draft</th>
<th>Project Final</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center on Aging</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Self-Pay Refund</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Construction</td>
<td>Storrs/UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Cardiology</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Speech and Hearing Clinic</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Treasury Services</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>TOTAL SPECIAL PROJECTS/CONSULTING (06)</td>
<td></td>
<td>(02)</td>
<td>(00)</td>
<td>(01)</td>
<td>(03)</td>
</tr>
</tbody>
</table>
High Risk Overdue by Functional Area

Storrs and Regional Campuses

Campus and Functional Area

- Enrollment Services
- Information Technology
- President's Office
- Psychiatry
- Public Safety

Enrollment Services: 0
Information Technology: 4
President's Office: 1
Psychiatry: 2
Public Safety: 26
Open Overdue Items by Audit - Based on Original Due Date

Number of Open Overdue Items

Audit Name:
07-51 UITS Active Directory
07-70 HIPAA Security Storrs
10-11 UCHC Human Subjects Research
11-05 Peoplesoft - Student Administration
11-08 NCAA Rules Compliance Program
11-10 Dining Services
11-20 Grant Expenditures & Cost Transfers
12-01 UCHC Banner
12-04 CT Health Information Network (CHIN)
12-32 Diagnostic Imaging
12-38 Stamford Business Operations and IT
12-40 Overtime Payments - Public Safety
12-42 University Server Physical Security
12-45 Daily Campus
12-49 UConn Health Asset Management
12-50 Library Business Process
13-01 Emergency Preparedness
13-07 Export Controls
13-11 American Disability Act (ADA)
13-13 User Authentication and Account Administration
13-21a Tuition Fees - Student Accounts Receivable and Financial Aid
13-21b Student Administration Systems - Jenzabar
13-22 Lab Safety
13-31b JDH Pharmacy Charge Capture
13-33 International Faculty and Students
13-38 Medicare Enrollment - Provider Data
14-06 Law School Foundation
14-09 Federal Grants - Cost Sharing
14-11 Server Implementation and Security
14-12 Husky One Card Office
14-14 Advanced Beneficiary Notices
14-17 Avery Point Information Technology
14-18 UH Cash Handling
14-19 1st Change Order Monitoring Review - Storrs
14-21 HIM Patient Record Management
14-24 UH Medical Device Security Audit
14-25 Extra Benefits and Camps and Clinics
14-25 NCAA Rules Compliance
14-31 SHS Business and Healthcare
14-31 SHS Clinical Systems Security
14-33 Marching and Pep Bands
15-01 AxiUm Dental System
15-06 Dentist Record Management
15-04 Storrs Firewall Security
15-12 Research Laboratory Safety
15-16 Storrs PCI
15-18 Human Subject Incentive Payments
Open Items by Finding Category - UConn Health

Finding Category

- Business Process
- Monitoring
- Physical Security of Assets
- Policy
- Procedures
- Regulatory Compliance
- Security
- Segregation of Duties
- Technology
- Training

UConn Health
Open Overdue Items by Functional Area - Based on Original Due Date

- Storrs and Regional Campuses
- UConn Health
Implemented

High 13
Medium 16
Low 46

Open OverDue Items by Risk Level

High 35
Medium 94
Low 131
Audit Finding Rating Definitions

Low

Meaningful reportable issue for client consideration that in the Auditor’s judgment should be communicated in writing. The finding results in minimal exposure to the University or UConn Health and has little or no impact on the University’s or UConn Health’s compliance with laws and regulations. The issues related to this control weakness will typically not lead to a material error.

Medium

Significant exposure to the area under review within the scope of the audit. The finding results in the potential violation of laws and regulations and should be addressed as a priority to ensure compliance with University’s or UConn Health’s policies and procedures. The significance of the potential errors related to this control weakness makes it important to correct.

High

Significant exposure to the University or UConn Health that could include systemic University or UConn Health wide exposure. The finding could result in a significant violation of laws and regulations and should be viewed as a highest priority which the University or UConn Health must address immediately.
<table>
<thead>
<tr>
<th>AUDIT</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RESEARCH/GENERAL COMPLIANCE</strong></td>
<td></td>
</tr>
<tr>
<td>Faculty Consulting (07/01/14-06/30/15)* - evaluate the effectiveness of the established faculty consulting activity approval and oversight procedures and compliance with state regulations and University policies and procedures</td>
<td>In Process</td>
</tr>
<tr>
<td>Family Medical Leave Act (FMLA) - evaluate the process for managing implementation of FMLA to verify compliance with Federal and State laws</td>
<td>In Process</td>
</tr>
<tr>
<td>CI Stem Cell Research Grants FY16 Expenditures* - CT Stem Cell Research Grants Program requires an annual audit to verify that program expenditures comply with the terms of each Agreement</td>
<td>In Process</td>
</tr>
<tr>
<td>Sub-Recipient Monitoring - evaluate the procedures for monitoring payments and activities of sub-recipients to verify compliance with University policies and procedures, and federal regulations</td>
<td></td>
</tr>
<tr>
<td>Controlled Substances / Restricted Purchases in Research – evaluate the internal controls surrounding advance authorization for use of controlled substances and compliance with applicable regulations for purchase, use, storage, tracking and disposal of these materials</td>
<td></td>
</tr>
<tr>
<td>Faculty Consulting (07/01/15-06/30/16)* - evaluate the effectiveness of the established faculty consulting activity approval and oversight procedures and compliance with state regulations and University policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Effort Reporting - evaluate whether internal controls are adequate to properly manage, account for, monitor, and report salary and wage costs charged to sponsored projects in compliance federal regulations and determine whether salaries and wages charged to sponsored projects are allowable, allocable, and reasonable based on federal cost principles</td>
<td></td>
</tr>
<tr>
<td>Debarment, Sanctions and Exclusions – assess compliance with federal debarment and suspension regulations that restrict awards, subawards, and contracts with certain parties that are debarred, suspended, or otherwise excluded from or ineligible for participation in Federal assistance programs or activities</td>
<td></td>
</tr>
<tr>
<td>Clery Act – evaluate the University’s compliance with Clery Act logging, reporting, and policy and procedure requirements</td>
<td></td>
</tr>
<tr>
<td>Fair Labor Standards Act (FLSA) – assess compliance with recent revisions to the FLSA</td>
<td></td>
</tr>
<tr>
<td>CI Stem Cell Research Grants FY17 Expenditures* - CT Stem Cell Research Grants Program requires an annual audit to verify that program expenditures comply with the terms of each Agreement</td>
<td></td>
</tr>
<tr>
<td>AUDIT</td>
<td>STATUS</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>CONSTRUCTION/UCONN 2000</strong></td>
<td>In Process</td>
</tr>
<tr>
<td>Construction Life Cycle Review(s) – continuous monitoring initiation through close out – verify compliance with federal, state and University requirements, reasonableness of construction costs, and agreement with terms and conditions of the contract for:</td>
<td></td>
</tr>
<tr>
<td>• Hartford Campus Relocation – Report 1</td>
<td></td>
</tr>
<tr>
<td>• IPB</td>
<td></td>
</tr>
<tr>
<td>• Monteith Renovations</td>
<td></td>
</tr>
<tr>
<td>• Putnam</td>
<td></td>
</tr>
<tr>
<td>• Engineering Building</td>
<td></td>
</tr>
<tr>
<td>Energy Savings Company (ESCO) Project – Report 1</td>
<td>In Process</td>
</tr>
<tr>
<td>Deferred Maintenance /Facilities Operations - determine whether the use of funds provided through UConn 2000 bonding comply with state regulations</td>
<td></td>
</tr>
<tr>
<td><strong>INFORMATION TECHNOLOGY (IT)</strong></td>
<td>In Process</td>
</tr>
<tr>
<td>Research Data Security - assess general controls and compliance with IT security policies</td>
<td></td>
</tr>
<tr>
<td>Storrs Confidential Data/Activity Logging and Review Policy - assess the effectiveness of standards and procedures implemented for compliance with the University’s Confidential Data/Activity Logging and Review Policy</td>
<td>In Process</td>
</tr>
<tr>
<td>Cogeneration Power Plant – review of general IT controls used to manage and secure systems</td>
<td></td>
</tr>
<tr>
<td>CLAS IT (Selected IT Department) - assess general controls and compliance with IT security policies</td>
<td></td>
</tr>
<tr>
<td>Public Safety Systems – review of general IT controls used to manage and secure systems</td>
<td></td>
</tr>
<tr>
<td>Web Application – assess the security of University hosted web applications</td>
<td></td>
</tr>
<tr>
<td>SAIT – review of general IT controls used to manage and secure systems</td>
<td></td>
</tr>
<tr>
<td>Incident Response – review of processes used to respond to security breaches</td>
<td></td>
</tr>
<tr>
<td>School of Pharmacy – review of general IT controls used to manage and secure systems</td>
<td></td>
</tr>
<tr>
<td>Waterbury – review of general IT controls used to manage and secure systems</td>
<td></td>
</tr>
</tbody>
</table>
## Financial & Operational

<table>
<thead>
<tr>
<th>Audit</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash Receipts/Cash Handling – assess the effectiveness of internal controls and operational efficiencies for non-student revenue sources throughout the University and compliance with applicable state laws and regulations and institutional policies and procedures</td>
<td>In Process</td>
</tr>
<tr>
<td>Space Management System - evaluation of the policies and procedures surrounding the assignment, tracking and utilization of space to verify optimization of existing resources and compliance with federal regulations</td>
<td>In Process</td>
</tr>
<tr>
<td>Purchasing Contract Management - assess the internal controls surrounding the contracts related to the purchase of goods and services to verify compliance with applicable state and federal regulations and University policies and provide for effective and efficient operations</td>
<td>In Process</td>
</tr>
<tr>
<td>Transportation and Parking - review of business operations to assess compliance with applicable regulations and institutional policies and procedures, effectiveness of internal controls and operational efficiencies</td>
<td>In Process</td>
</tr>
<tr>
<td>Foundation Receipts and Disbursements FY16* - examine Foundation disbursements for compliance with University policies related to the disbursement of Foundation funds and gifts to the Foundation for compliance with Connecticut General Statute (CGS) Section 4-37 et seq., and University policies concerning the deposit of funds at the Foundation</td>
<td>In Process</td>
</tr>
<tr>
<td>School of Law Financial Aid - review of financial aid operations to assess effectiveness of internal controls and operational efficiencies, and compliance with applicable regulations and institutional policies and procedures</td>
<td>In Process</td>
</tr>
<tr>
<td>Non-Tuition Accounts Receivable – review of business operations related to invoicing, revenue recognition, accounts receivable tracking, and bad debt write-off for revenue generating activities that are not accounted for through the Student Administration System</td>
<td>In Process</td>
</tr>
<tr>
<td>Student Payroll Post Implementation- assess the internal controls in the student payroll function to verify compliance with state / federal regulations and University policies and provide for effective and efficient operations</td>
<td>In Process</td>
</tr>
<tr>
<td>Special Payroll – analyze payments to faculty and staff in excess of base institutional salary; review internal controls and approval process</td>
<td>In Process</td>
</tr>
<tr>
<td>Building / Room Access Controls - evaluate the effectiveness of internal controls implemented to selectively restrict access to various physical locations to authorized individuals, deter intruders, and protect the University community and resources</td>
<td>In Process</td>
</tr>
<tr>
<td>AUDIT</td>
<td>STATUS</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Events and Conference Services - review of business operations to</td>
<td></td>
</tr>
<tr>
<td>assess compliance with applicable state regulations and institutional</td>
<td></td>
</tr>
<tr>
<td>policies and procedures, effectiveness of internal controls and</td>
<td></td>
</tr>
<tr>
<td>operational efficiencies</td>
<td></td>
</tr>
<tr>
<td>Asset Management (Including Controllable Property) - assess</td>
<td></td>
</tr>
<tr>
<td>management’s asset tracking system to verify compliance with</td>
<td></td>
</tr>
<tr>
<td>policies and procedures, &amp; University, state and federal regulations</td>
<td></td>
</tr>
<tr>
<td>on maintenance, disposal, safeguarding and reporting assets</td>
<td></td>
</tr>
<tr>
<td>Selected Center/Institute/Department including research administration</td>
<td></td>
</tr>
<tr>
<td>- evaluate the effectiveness of management oversight procedures and</td>
<td></td>
</tr>
<tr>
<td>determine whether appropriate financial and programmatic controls</td>
<td></td>
</tr>
<tr>
<td>have been established to verify compliance with State and Federal</td>
<td></td>
</tr>
<tr>
<td>regulations and university policies and procedures</td>
<td></td>
</tr>
<tr>
<td>International Travel – Faculty, Staff and Student - review of</td>
<td></td>
</tr>
<tr>
<td>international travel to assess the effectiveness of existing</td>
<td></td>
</tr>
<tr>
<td>policies and procedures to verify the health and safety of</td>
<td></td>
</tr>
<tr>
<td>travelers participating in academic, research, and/or</td>
<td></td>
</tr>
<tr>
<td>professional development activities abroad</td>
<td></td>
</tr>
<tr>
<td>Foundation Receipts and Disbursement FY17* - examine Foundation</td>
<td></td>
</tr>
<tr>
<td>disbursements for compliance with University policies related to</td>
<td></td>
</tr>
<tr>
<td>the disbursement of Foundation funds and gifts to the Foundation</td>
<td></td>
</tr>
<tr>
<td>for compliance with Connecticut General Statute (CGS) Section 4-37</td>
<td></td>
</tr>
<tr>
<td>et seq., and University policies concerning the deposit of funds at</td>
<td></td>
</tr>
<tr>
<td>the Foundation</td>
<td></td>
</tr>
<tr>
<td>Facilities Operations - review of business operations to assess</td>
<td></td>
</tr>
<tr>
<td>compliance with applicable regulations and institutional policies</td>
<td></td>
</tr>
<tr>
<td>and procedures, effectiveness of internal controls and</td>
<td></td>
</tr>
<tr>
<td>operational efficiencies</td>
<td></td>
</tr>
<tr>
<td>Procurement Card – assess whether existing internal controls</td>
<td></td>
</tr>
<tr>
<td>detect and/or prevent significant errors or irregularities in a</td>
<td></td>
</tr>
<tr>
<td>timely manner, administration of the Procard program is efficient,</td>
<td></td>
</tr>
<tr>
<td>and compliance with University policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Software Licensing - assess controls over the procurement of</td>
<td></td>
</tr>
<tr>
<td>software licenses, compliance with license agreements and practices</td>
<td></td>
</tr>
<tr>
<td>related to software upgrades and maintenance</td>
<td></td>
</tr>
</tbody>
</table>

**ATHLETICS**

Selected NCAA Compliance Areas

- Recruiting
- Playing & Practice Sessions
- Ticketing
- Equipment

NCAA Division 1-A Membership Requirements* - annual agreed upon procedures to assist in evaluating whether NCAA Division I membership requirements have been met
<table>
<thead>
<tr>
<th>AUDIT</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>Ongoing</td>
</tr>
<tr>
<td>ACL Consulting &amp; Script Writing</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Follow-up Audit Activities</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Contingencies/Special Projects/Investigations/Consulting</td>
<td>Ongoing</td>
</tr>
</tbody>
</table>
# Draft UConn Health Audit Plan – FY17

**Status Codes:** *=Required

<table>
<thead>
<tr>
<th>AUDIT</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLINICAL: FINANCIAL / OPERATIONAL / COMPLIANCE</strong></td>
<td></td>
</tr>
<tr>
<td>Respiratory Therapy – evaluate whether services are performed as ordered and in accordance with internal policy and charges are recorded in compliance with new billing guidelines</td>
<td>In Progress</td>
</tr>
<tr>
<td>Select Local Coverage Determination (LCD) Monitoring, ACL – utilize data analytics (ACL) to determine whether coverage conditions for particular items and services provided to Medicare beneficiaries comply with coverage conditions published by the National Government Services publishes</td>
<td>In Progress, Additional LCDs for FY17</td>
</tr>
<tr>
<td>Cancer Center Revenue Cycle (registration through collections processes) – evaluate the effectiveness of policies and procedures related to achieving complete, accurate and timely processing of documentation and transactions and compliance with governmental regulations and the reimbursement requirements of various payers</td>
<td>In Progress</td>
</tr>
<tr>
<td>Dental Charge Capture and Billing - new system for capturing charges and billing; evaluate the effectiveness of policies and procedures related to achieving compliance with governmental regulations, internal policy and payer reimbursement requirements</td>
<td></td>
</tr>
<tr>
<td>Inpatient Outlier Payments - evaluate management’s procedures for monitoring Medicare outlier payments</td>
<td></td>
</tr>
<tr>
<td>Inpatient Stays - decision to admit and supporting documentation including an assessment of compliance with two midnight rule</td>
<td></td>
</tr>
<tr>
<td>Lab Panel Billing Monitoring, ACL – utilize data analytics (ACL) to determine whether a single payment for bundled labs is consistent with the provisions specified in contracts with various insurance</td>
<td></td>
</tr>
<tr>
<td>Urgent Care - assess whether services billed by two relatively new Urgent Care practice locations were ordered, provided and documented in compliance with governmental regulations, payer requirements and the associated charges are complete, accurate and timely</td>
<td></td>
</tr>
<tr>
<td>JDH/UMG Outpatient Billing for CMHC - evaluate the internal controls surrounding JDH/UMG billing practices for outpatient services provided to DOC inmates and billed to CMHC to verify the accuracy, completeness and timeliness of billings</td>
<td></td>
</tr>
<tr>
<td>Billing Modifier 25 – assess clinical documentation to verify proper use of the modifier when an evaluation service is significant, separately identifiable, and above and beyond the usual pre and postoperative work of a medical procedure</td>
<td></td>
</tr>
<tr>
<td>CMHC site review – comprehensive review of clinical operations at one selected facility to evaluate the effectiveness of internal controls to verify compliance with state and federal regulations, contractual requirements and internal policies and procedures</td>
<td></td>
</tr>
<tr>
<td>AUDIT</td>
<td>STATUS</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Cl Stem Cell Research Grants, FY 16 Expenditures*</td>
<td>In Process</td>
</tr>
<tr>
<td>- CT Stem Cell Research Grants Program requires that the internal</td>
<td></td>
</tr>
<tr>
<td>audit department verify that program expenditures comply with the</td>
<td></td>
</tr>
<tr>
<td>terms of each Agreement</td>
<td></td>
</tr>
<tr>
<td>Faculty Consulting (07/01/14-06/30/15)* - evaluate the effectiveness</td>
<td>In Process</td>
</tr>
<tr>
<td>of the established faculty consulting activity approval and</td>
<td></td>
</tr>
<tr>
<td>oversight procedures and compliance with state regulations and</td>
<td></td>
</tr>
<tr>
<td>University policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Mandate Consulting (07/01/14-06/30/15)* - evaluate the effectiveness</td>
<td>In Process</td>
</tr>
<tr>
<td>of the established faculty consulting activity approval and</td>
<td></td>
</tr>
<tr>
<td>oversight procedures and compliance with state regulations and</td>
<td></td>
</tr>
<tr>
<td>University policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Family Medical Leave Act (FMLA) - evaluate the process for managing</td>
<td>In Process</td>
</tr>
<tr>
<td>implementation of FMLA to verify compliance with Federal and State</td>
<td></td>
</tr>
<tr>
<td>laws</td>
<td></td>
</tr>
<tr>
<td>Conflicts of Interest in Research - assess the policies and procedures</td>
<td>In Process</td>
</tr>
<tr>
<td>surrounding conflict of interest in research including disclosure</td>
<td></td>
</tr>
<tr>
<td>and conflict management to verify compliance with federal regulation</td>
<td></td>
</tr>
<tr>
<td>Cl Stem Cell Research Grants, FY 17 Expenditures*</td>
<td>In Process</td>
</tr>
<tr>
<td>- CT Stem Cell Research Grants Program requires that the internal</td>
<td></td>
</tr>
<tr>
<td>audit department verify that program expenditures comply with the</td>
<td></td>
</tr>
<tr>
<td>terms of each Agreement</td>
<td></td>
</tr>
<tr>
<td>Mandatory Training Compliance – assess whether employees are</td>
<td></td>
</tr>
<tr>
<td>properly assigned mandatory trainings, that the completion of</td>
<td></td>
</tr>
<tr>
<td>such trainings is monitored and appropriate action is taken for</td>
<td></td>
</tr>
<tr>
<td>non-compliance</td>
<td></td>
</tr>
<tr>
<td>Faculty Consulting (07/01/15-06/30/16)* - evaluate the effectiveness</td>
<td>In Process</td>
</tr>
<tr>
<td>of the established faculty consulting activity approval and</td>
<td></td>
</tr>
<tr>
<td>oversight procedures and compliance with state regulations and</td>
<td></td>
</tr>
<tr>
<td>University policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Family Medical Leave Act (FMLA) - evaluate the process for managing</td>
<td>In Process</td>
</tr>
<tr>
<td>implementation of FMLA to verify compliance with Federal and State</td>
<td></td>
</tr>
<tr>
<td>laws</td>
<td></td>
</tr>
<tr>
<td>Conflicts of Interest in Research - assess the policies and procedures</td>
<td>In Process</td>
</tr>
<tr>
<td>surrounding conflict of interest in research including disclosure</td>
<td></td>
</tr>
<tr>
<td>and conflict management to verify compliance with federal regulation</td>
<td></td>
</tr>
<tr>
<td>Cl Stem Cell Research Grants, FY 17 Expenditures*</td>
<td>In Process</td>
</tr>
<tr>
<td>- CT Stem Cell Research Grants Program requires that the internal</td>
<td></td>
</tr>
<tr>
<td>audit department verify that program expenditures comply with the</td>
<td></td>
</tr>
<tr>
<td>terms of each Agreement</td>
<td></td>
</tr>
<tr>
<td>Grant, Sub Recipient Monitoring - evaluate the procedures for</td>
<td>In Process</td>
</tr>
<tr>
<td>monitoring payments and activities of sub-recipients to verify</td>
<td></td>
</tr>
<tr>
<td>compliance with University policies and procedures, and federal</td>
<td></td>
</tr>
<tr>
<td>regulations</td>
<td></td>
</tr>
<tr>
<td>Effort Reporting - evaluate whether internal controls are adequate to</td>
<td>In Process</td>
</tr>
<tr>
<td>properly manage, account for, monitor, and report salary and wage</td>
<td></td>
</tr>
<tr>
<td>costs charged to sponsored projects in compliance with federal</td>
<td></td>
</tr>
<tr>
<td>regulations and determine whether salaries and wages charged to</td>
<td></td>
</tr>
<tr>
<td>sponsored projects are allowable, allocable, and reasonable based</td>
<td></td>
</tr>
<tr>
<td>on federal cost principles</td>
<td></td>
</tr>
<tr>
<td>Federal Financial Aid - review of financial aid operations to assess</td>
<td>In Process</td>
</tr>
<tr>
<td>effectiveness of internal controls and operational efficiencies,</td>
<td></td>
</tr>
<tr>
<td>and compliance with applicable federal regulations and institutional policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Controlled Substances/Restricted Purchases in Research - evaluate the internal controls surrounding advance authorization for use of controlled substances and compliance with applicable regulations for purchase, use, storage, tracking and disposal of these materials</td>
<td></td>
</tr>
<tr>
<td>AUDIT</td>
<td>STATUS</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Clinical Trial Billing – assess the controls surrounding clinical trials billing including the identification of research subjects and the proper determination of billable services</td>
<td></td>
</tr>
<tr>
<td><strong>FINANCIAL / OPERATIONAL</strong></td>
<td></td>
</tr>
<tr>
<td>Emergency Preparedness - a review of the respective EOPs and current emergency management activities for UH and JDH to evaluate compliance with regulations that define requirements for evacuation, emergency response and preparedness</td>
<td>In Process</td>
</tr>
<tr>
<td>Clinical Contracts – evaluate whether clinical contract related payments to or from UH were supported by contractual terms and conditions and assess the effectiveness of internal controls designed to administer clinical contracts and process the related income or payments</td>
<td>In Process</td>
</tr>
<tr>
<td>Overtime Payments / Clinical Areas – assess the internal controls in the area of overtime in selected clinical departments to verify compliance with state / federal regulations, collective bargaining agreements, UH policies and procedures and provide for effective and efficient operations</td>
<td>In Process</td>
</tr>
<tr>
<td>Travel – review of travel to assess the effectiveness of existing policies and procedures to verify compliance with state/federal regulations, UH policies and procedures and provide effective and efficient operations</td>
<td>In Process</td>
</tr>
<tr>
<td>Software Licensing – assess controls over the procurement of software licenses, compliance with license agreements and practices related to software upgrades and maintenance</td>
<td></td>
</tr>
<tr>
<td>Workers Compensation – verify that injuries are properly reported to human resources and the third party administrator, that human resources coordinates all employment aspects of lost time claims including wage audits, timecard instructions and return to work and the manager appropriately assigns the employee based upon their work status</td>
<td></td>
</tr>
<tr>
<td>CMHC Payroll – assess the internal controls in the payroll function to verify compliance with state / federal regulations, UH policies and provide for effective and efficient operations</td>
<td></td>
</tr>
<tr>
<td>Selected Center/Institute/Department including research administration - evaluate the effectiveness of management oversight procedures and determine whether appropriate financial and programmatic controls have been established to verify compliance with State and Federal regulations and UH policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Transportation and Parking - review of business operations to assess compliance with applicable regulations and institutional policies and procedures, effectiveness of internal controls and operational efficiencies</td>
<td></td>
</tr>
</tbody>
</table>

Status Codes: *=Required
<table>
<thead>
<tr>
<th>AUDIT</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement Card - assess whether existing internal controls detect and/or prevent significant errors or irregularities in a timely manner, administration of the Procard program is efficient, and in compliance with policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Kreg System - evaluate the contract management system to assess whether the terms of the payer contracts are properly recorded and that the system accurately calculates expected insurance payments</td>
<td></td>
</tr>
<tr>
<td>Purchasing, Procurement of Goods and Services and Competitive Bidding Process – assess the internal controls surrounding the purchase of goods and services to verify compliance with applicable state and federal regulations, UH policies and procedures and provide for effective and efficient operations</td>
<td></td>
</tr>
<tr>
<td>Co-Pay and Deductibles- evaluate the process for collecting co-pays and deductibles at selected JDH and UMG practice locations to determine the completeness, accuracy and timeliness of collections</td>
<td></td>
</tr>
</tbody>
</table>

**CONSTRUCTION / UCONN 2000**

Owner Controlled Insurance Program – verify that the specific lines of insurance have been properly procured and managed, the potential cost savings have been achieved, and claims management procedures are working to reduce the risk of fraudulent claims

Construction Life Cycle Reviews of Selected Projects (includes change order monitoring):

- New Patient Tower
- Hospital Renovation

**INFORMATION TECHNOLOGY (IT)**

Pharmacy Systems IT – assess general IT controls used to manage and secure systems

UConn Health One Implementation – review of governance throughout the EPIC implementation

Public Safety Systems - assess general IT controls used to manage and secure systems

Mobile Devices – review of processes used for securing data stored, accessed or processed using mobile devices

Wireless Network – review of Wireless network administration processes and configurations for compliance with industry standards and UConn Health policy

Security Policy Review – review of selected information technology/security policy implementation and management
<table>
<thead>
<tr>
<th>Audit Activity</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Follow-up Audit Activities</td>
<td>Ongoing</td>
</tr>
<tr>
<td>ACL Consulting &amp; Script Writing</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Contingencies/Special Requests/Investigations/Consulting</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Program Element</td>
<td>Activities</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Collaborative Relationships | - Participate on rules based and other University-wide committees in order to enhance awareness of emerging compliance concerns, business operations and to maintain collegial relationships across campus.  
  - Review partnership with UConn Health on specific compliance issues with University-wide impact, such as University Policies and Privacy.  
  - Active membership with professional organizations such as NACUA, SCCE, IAPP, ARMA, YPNHE and ACUPA to increase collaborations with peer and aspirant institutions.  |
| Education/Awareness and Specialized Training | - Continued efforts to ensure proper compliance education of new faculty and staff. Efforts include: video message in New Employee Orientation, “Policy of the Week” and quarterly newsletters.  
  - Collaborate with Human Resources on new online training capabilities, including tracking and follow-up.  
  - Provide targeted Compliance Training for units with specialized responsibilities. Training will focus on policy violation detection and prevention.  
  - 2017 Annual Compliance Training to include topics related to the University Code of Conduct, the State Code of Ethics, Sponsored Programs, Capital Equipment and Controllable Property.  
  - Work with University administration to enhance educational efforts specific to new and revised policies.  
  - Facilitate proper Privacy/HIPAA/FERPA training for impacted entities.  
  - Continue to expand Records and Information Management efforts University-wide. Promote online resources to the University community.  
  - Enhance online compliance resources and tools to continue optimizing outreach and communication efforts.  |
| Monitoring               | - Expand current Higher Education Opportunities Act (HEOA) monitoring efforts.  
  - Implement a monitoring program for the Minor Protection Program.  
  - Launch a post-data incident response monitoring program.  |
<table>
<thead>
<tr>
<th>Program Element</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Pilot a “self-monitoring” program with selected departments to ensure adequate understanding and evaluation of compliance obligations while empowering units to carry out their own compliance monitoring responsibilities.</td>
</tr>
<tr>
<td></td>
<td>- Continue to work with the Executive Risk Management and Compliance Committee (ERMCC) to ensure proper monitoring of developing areas of compliance risk.</td>
</tr>
<tr>
<td>Policy</td>
<td>- Continue promoting review of existing University policies for relevance to current operations, campus applicability and elimination of duplication where appropriate.</td>
</tr>
<tr>
<td></td>
<td>- Collaborate with University archives to ensure preservation of policy history in a more accessible digital format.</td>
</tr>
<tr>
<td></td>
<td>- Institute a University-wide Policy Protocol for Storrs, Regional and UConn Health Campuses.</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>- Coordinate guidance for activities currently covered and not covered (i.e. non-university activities, 4-H programs, dually-enrolled students, activities sponsored by student organization, visits/tours, etc.) under the existing Protection of Minors Policy.</td>
</tr>
<tr>
<td></td>
<td>- Assess existing Minor Protection training and educational resources to determine whether adjustments to the content or method of delivery are necessary.</td>
</tr>
<tr>
<td></td>
<td>- Track key compliance indicators across all registered youth activities to measure program effectiveness, promote accountability, and gauge overall levels of compliance.</td>
</tr>
<tr>
<td></td>
<td>- Review administrative functions currently under the responsibility of Compliance. Areas include FOIA, Privacy, Policy and HEOA disclosure webpage.</td>
</tr>
<tr>
<td>Investigations</td>
<td>- Formalize collaborative investigative process with Faculty and Staff Labor Relations, Office of Institutional Equity and Ombuds to eliminate redundancies and effectively manage the review of allegations that span multiple areas.</td>
</tr>
<tr>
<td></td>
<td>- Work with senior leadership to ensure proper review and response to matters that come to the attention of the office but do not rise to the level of a policy violation.</td>
</tr>
<tr>
<td></td>
<td>- Collaborate with the Employees of Concern Team to ensure proper monitoring and intervention where appropriate.</td>
</tr>
<tr>
<td>Program Element</td>
<td>Activities</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Performance Incentives</td>
<td>Engage University administration in reviewing and piloting a compliance incentive program. This program may include recognition letters from senior leadership, feature articles in the Compliance Newsletter or a Compliance and Ethics awards event.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Reporting to the Executive Risk Management and Compliance Committee (ERMCC) and Joint Audit and Compliance Committee (JACC) on significant compliance initiatives and developments.</td>
</tr>
</tbody>
</table>

Approved by the Joint Audit & Compliance Committee at their __________ Meeting
<table>
<thead>
<tr>
<th>Program Element</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaborative Relationships</td>
<td>✤ Participate on and /or chair committees in order to enhance awareness of emerging compliance concerns, business operations and to maintain collegial relationships across campus.</td>
</tr>
<tr>
<td></td>
<td>• JDH/UMG regulatory committees, including but not limited to: Meaningful Use, Recovery Audit Contractors (RAC); Health Information Management Committees, JDH Ethics Committee, HHS Nondiscrimination Committee and Workplace Violence Prevention Committee.</td>
</tr>
<tr>
<td></td>
<td>• Construction/BioScience</td>
</tr>
<tr>
<td></td>
<td>• Research Col Management Committees – Individual and Institutional</td>
</tr>
<tr>
<td></td>
<td>• Clinical Col Management Committee</td>
</tr>
<tr>
<td></td>
<td>• Executive Policy Committee</td>
</tr>
<tr>
<td></td>
<td>• Background and Sanctions Checking Executive Compliance Group</td>
</tr>
<tr>
<td></td>
<td>• Open Payments Advisory Committee</td>
</tr>
<tr>
<td></td>
<td>• Epic Implementation Work Groups</td>
</tr>
<tr>
<td></td>
<td>• Overpayment Committee</td>
</tr>
<tr>
<td></td>
<td>• Privacy Taskforce</td>
</tr>
<tr>
<td></td>
<td>• Drug-Free Schools/Workplace Compliance Committee</td>
</tr>
<tr>
<td></td>
<td>• HHS Section 1557 Nondiscrimination Work Group</td>
</tr>
<tr>
<td></td>
<td>✤ Work collaboratively with departments to assure resident supervision consistent with hospital by-laws, policy and CMS Conditions of Participation.</td>
</tr>
<tr>
<td></td>
<td>✤ Provide compliance guidance for new or evolving services and as requested.</td>
</tr>
<tr>
<td></td>
<td>✤ Active membership with professional organizations including: AAMC Forums and Workgroups - Compliance Officers, Privacy, and Chairperson of Peer Evaluation Workgroup; Health Care Compliance Association; Society for Corporate Compliance &amp; Ethics; CT Hospital Association Compliance Forum; Healthcare Financial Management Association; Health Ethics Trust.</td>
</tr>
<tr>
<td></td>
<td>✤ Continue partnership with UCONN on specific compliance issues with University-wide impact, such as: University-wide Policies, Privacy, Non-discrimination, research compliance.</td>
</tr>
<tr>
<td></td>
<td>✤ Coordinate activities with UConn Health Senior Counsel and the Assistant Attorney General’s Office.</td>
</tr>
<tr>
<td>Program Element</td>
<td>Activities</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Education/Awareness and Specialized Training | Continued efforts to ensure proper compliance education of faculty and staff by providing the following:  
  - Annual Training:  
    - Compliance, including Code of Conduct, State Code of Ethics and current regulatory topics  
    - State Code of Ethics for employees involved in negotiating, managing and/or overseeing contracts  
    - HIPAA Privacy and Security including HITECH updates  
    - Financial Aid Code of Conduct for student financial aid employees  
    - Semi-annual Management Development Education - Understanding UConn Health Compliance  
  - Orientations and Initial Trainings:  
    - Bi-weekly Compliance overview for new employees  
    - Annual resident and student orientations  
    - Online orientation Compliance training  
  - Focused, topic-specific individual or departmental education as needed/requested, including follow-up to address internal or external audit findings.  
  - Collaborate with Human Resources on refinement of institutional orientation and manager training.  
  - Work with administration to enhance efforts specific to policy and procedure templating revisions with the goal of improved policy awareness and compliance.  
  - Enhance online compliance website resources.  
  - Quarterly Compliance Courier & Monthly Current Issues in Compliance Newsletters  
  - Monthly Compliance Quandary Q & A on website  
  - National Compliance and Ethics Week activities |
| Monitoring                               | Develop monitors with stakeholders for FY 17 utilizing ACL audit tool whenever possible  
  - OIG Workplan review with stakeholders fall-winter 2016 and 2017  
  - Expand privacy monitoring to target OCR audit categories of risk  
  - Local and National Coverage Determinations monitors (LCDs/NCDs)  
  - Identity Theft Prevention and Identification  
  - Overpayment Corrective Action Monitoring |
<table>
<thead>
<tr>
<th>Program Element</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy</strong></td>
<td>Assure that the Executive Risk Management and Compliance Committee (ERMCC) is aware of developing areas of compliance risk requiring assessment and continued monitoring.</td>
</tr>
<tr>
<td></td>
<td>Assist with policy development/revision as requested by any UConn Health department and/or to comply with any regulatory changes – in 2017 expect: Medical identity theft process refinement, Stark and anti-kickback policy development, Overpayment Refunds, policy review and revision on non-discrimination, workplace violence, drug free schools and workplace.</td>
</tr>
<tr>
<td></td>
<td>HIPAA/HITECH policy updates</td>
</tr>
<tr>
<td></td>
<td>Finance Policies Review Project</td>
</tr>
<tr>
<td></td>
<td>Assure implementation of the Institutional CoI in Research Policy revisions</td>
</tr>
<tr>
<td></td>
<td>Manage the UConn Health Executive Policy Committee – accept and process policies for committee review and approval, assure posting and archiving, review for relevance to current operations, applicability to specific domains and elimination of duplication across domains of UConn Health where appropriate.</td>
</tr>
<tr>
<td></td>
<td>Institute the UConn Health Campus portion of the University-wide Policy Protocol.</td>
</tr>
<tr>
<td><strong>Regulatory Compliance</strong></td>
<td>Support compliance with regulatory requirements FY17 (including but not limited to):</td>
</tr>
<tr>
<td></td>
<td>• HITECH Rule (continue to await expected changes)</td>
</tr>
<tr>
<td></td>
<td>• Meaningful Use and quality reporting move to MACRA</td>
</tr>
<tr>
<td></td>
<td>• CMS/DPH mandates (with emphasis on yearly IPPS and OPPS Rules impact to operations)</td>
</tr>
<tr>
<td></td>
<td>• Changing Federal and CT legislation affecting healthcare</td>
</tr>
<tr>
<td></td>
<td>• CoIs, Consulting activity and Open Payments Rule</td>
</tr>
<tr>
<td></td>
<td>Various accreditation initiatives</td>
</tr>
<tr>
<td></td>
<td>Various initiatives to prepare for potential Office of Civil Rights Audit Readiness under the HIPAA Program to include: Business Associate identification and tracking, Policy/Procedure readiness, remote access agreement implementation as needed with identified Business Affiliates, Epic system EHR privacy considerations.</td>
</tr>
<tr>
<td></td>
<td>Review administrative functions directly under the responsibility of Compliance. Areas include Privacy, Executive Policy management, Monthly Exclusions Checking Program and Overpayment Committee.</td>
</tr>
</tbody>
</table>
## UConn Health
### Joint Audit & Compliance Committee Meeting
### Draft Compliance Plan – FY17

<table>
<thead>
<tr>
<th>Program Element</th>
<th>Activities</th>
</tr>
</thead>
</table>
| Investigations  | ✓ Track and trend all compliance investigations  
                  ✓ Collaborate with Labor Relations, Office of Institutional Equity, Medical Staff Office, Police Department, Quality Departments of JDH, UMG, and Dental School, and Patient Relations when necessary to address allegations that span multiple areas.  
                  • Directly responsible for all allegations requiring investigations in the following areas:  
                    • Privacy – evaluate on a continuous basis the resources needed to conduct Privacy investigations specifically  
                    • State Ethics Law  
                    • Overpayment Evaluations and Management  
                    • Collaborate with IT Security when HIPAA security breaches are reported |
| Reporting       | ✓ Reporting to the Executive Risk Management and Compliance Committee (ERMCC) and Joint Audit and Compliance Committee (JACC) on significant compliance initiatives and developments. |

Approved by the Joint Audit & Compliance Committee at their __________ Meeting
University of Connecticut & UConn Health

Joint Audit & Compliance Committee Meeting
## Status of External Audit Projects

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Area</th>
<th>Scope</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marcum, LLP</td>
<td>UConn Health</td>
<td>Audits of the John Dempsey Hospital and Dental Clinics (Clinical Programs Fund), including the OHCA filings, UConn Medical Group (UMG) and the University of Connecticut Health Center Finance Corporation for FY2016.</td>
<td>FY2016 engagement is underway.</td>
</tr>
<tr>
<td>CohnReznick, LLP</td>
<td>Storrs, Regionals &amp; UConn Health</td>
<td>Annual audit of UCONN 2000 named projects substantially completed and deferred maintenance projects with designated budgets substantially completed in FY2016, 2017, and 2018, and annual agreed upon procedures performed on total UCONN 2000 expenditures (named projects, deferred maintenance and equipment) for FY2016, 2017, and 2018.</td>
<td>OACE will request JACC approval to hire CohnReznick for FY2016, 2017, and 2018 at their September meeting.</td>
</tr>
<tr>
<td>BKD</td>
<td>Storrs Athletics</td>
<td>NCAA agreed upon procedures performed on all revenues, expenses, and capital expenditures for or on behalf of the University’s Athletics Program for FY2016, 2017, and 2018.</td>
<td>OACE will request JACC approval to hire BKD for FY2016, 2017, and 2018 at their September meeting.</td>
</tr>
</tbody>
</table>
TO: Members of the Joint Audit & Compliance Committee

FROM: David Galloway
Chief Audit & Compliance Officer

DATE: September 27, 2016

SUBJECT: Appointment of UConn 2000 Auditors – CohnReznick LLP

RECOMMENDATION

It is recommended that the Joint Audit and Compliance Committee (JACC) approve the appointment of the accounting firm of CohnReznick LLP as independent auditors of UCONN 2000 expenditures for the 2016 through 2018 fiscal years. The engagement requires the audit of UCONN 2000 named projects and standalone deferred maintenance projects substantially completed during each fiscal year and agreed upon procedures performed on total UCONN 2000 expenditures, including deferred maintenance and equipment for the years ending June 30, 2016, 2017, and 2018. The proposed fee for the above services for year one of the engagement, the 2016 fiscal year, is $112,055 plus $2,430 in out-of-pocket expenses for a total combined fee of $114,485. The fee for the second and third year of the engagement, the 2017 and 2018 fiscal years, may increase or decrease based on modest hourly rate increases, the number of projects substantially completed and total expenditures for each period.

Year one of the engagement will commence on September 28, 2016, and is expected to be completed no later than June 30, 2017. In accordance with the terms of the contract and prevailing legislation, the University may elect to utilize the services of CohnReznick, LLP to conduct subsequent audits (the 2019 and 2020 fiscal years) of UCONN 2000 project expenditures on an annual basis for a total of five consecutive years.

BACKGROUND

Section 10a-109z of the Connecticut General requires that “the Board of Trustees for the University of Connecticut shall select and appoint independent auditors, as defined in subdivision (7) of section 4-230, to annually conduct an audit of any project of UConn 2000, as defined in subdivision (25) of section 10a-109c. Such audit shall review invoices, expenditures, cost allocations and other appropriate documentation in order to reconcile project costs and verify conformance with project budgets, cost allocation agreements and applicable contracts.” A bid process was conducted through the University of Connecticut Purchasing Department to select the independent accounting firm to perform audit and agreed upon procedures for fiscal years 2016, 2017, and 2018. Five firms submitted compliant proposals.
A committee of five employees representing the University and the Health Center, independently evaluated the five proposals based on a set of predetermined qualifications. Evaluation criteria included: quality of the proposed plan and ability to meet the University’s goals and objectives; experience in providing similar services to large public research institutions; capability of staff to manage and conduct audits and evaluate risk; and competitive pricing.

The Purchasing Department collected and tabulated the committee members’ scoring and the committee elected to interview each of the five firms on July 18, 2016. The committee voted to select CohnReznick LLP pending approval of the JACC. The firm’s profile is enclosed for your review.

OACE seeks JACC approval to move forward with this engagement.
CohnReznick is a national audit, tax, and business advisory firm founded in 1919. As one of the top accounting firms in the United States, CohnReznick provides forward-thinking service across nearly two dozen industries and serves businesses ranging from multigenerational family-run enterprises to public companies in the Fortune 1000. We have the deep resources and technical acumen of a large national accounting firm without sacrificing the hands-on, entrepreneurial approach that today's dynamic business environment demands. This combination allows us to offer the proactive insight and guidance our clients need as they grow and evolve. CohnReznick has developed specialized practices in key industries allowing us to specifically target relevant service offerings and knowledgeable personnel to each client. Because of our depth of resources across service lines, we serve in a variety of client service roles, including primary auditor, advisor, tax consultant, and other specialized roles. In addition to solid capabilities in core practice areas, CohnReznick has expanded the breadth of our service offerings in response to our clients' needs. We foster collaborative connections across every level and branch of our organization so that the professionals who will serve you will have access to our firm-wide depth of resources. An overview of our service offerings includes:

<table>
<thead>
<tr>
<th>ACCOUNTING AND ASSURANCE SERVICES</th>
<th>TAX SERVICES</th>
<th>ADVISORY</th>
<th>AFFILIATED COMPANIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audits, Reviews, and Compilations</td>
<td>Tax Compliance and Preparation</td>
<td>Bankruptcy and Restructuring</td>
<td>Capital Markets Securities</td>
</tr>
<tr>
<td>Employee Benefit Plans</td>
<td>Strategic Tax Planning</td>
<td>Computer Forensics and eDiscovery</td>
<td>CohnReznick Benefits Consultants</td>
</tr>
<tr>
<td>IFRS</td>
<td>Corporate Tax Outsourcing</td>
<td>Cybersecurity</td>
<td>CohnReznick UIC Insurance Consulting, Inc.</td>
</tr>
<tr>
<td>SOC 1 (SSAE 16), 2, and 3 Examinations</td>
<td>Private Clients</td>
<td>Forensic and Litigation</td>
<td>CohnReznick Real Estate LLC</td>
</tr>
<tr>
<td>Agreed-upon Procedures</td>
<td>Federal Tax</td>
<td>Governance, Risk and Compliance</td>
<td>CohnReznick Wealth Management LLC</td>
</tr>
<tr>
<td>Accounting Outsourcing and Consultations</td>
<td>Trust and Estate International Tax</td>
<td>Government and Public Sector Management Consulting and CFO Advisory</td>
<td>WJ Technologies</td>
</tr>
<tr>
<td>Public Company Services</td>
<td>State and Local Tax Transfer Pricing</td>
<td>Real Estate Advisory / NOI Strategies</td>
<td></td>
</tr>
<tr>
<td>IT Audit and Controls Review</td>
<td>Cost Segregation Studies</td>
<td>Technology and Digital Services</td>
<td></td>
</tr>
<tr>
<td>New Market Tax Credits</td>
<td>Tax Specialty Services</td>
<td>Transactional Advisory and M&amp;A Consulting</td>
<td></td>
</tr>
<tr>
<td>Tax Credit Advisory</td>
<td></td>
<td>Valuation</td>
<td></td>
</tr>
</tbody>
</table>

*Foreign offices are subsidiaries of CohnReznick*

CohnReznick is a Leading audit, tax, and advisory firm in the United States with 300+ partners/principals, 2,700+ employees, more than $575 million in annual revenue. Offices in 30 cities throughout California, Connecticut, Georgia, Illinois, Maryland, Massachusetts, New Jersey, New York, North Carolina, Pennsylvania, Texas, Virginia, Washington, D.C., Cayman Islands*, India*, Australia*, Canada*. CohnReznick has an international reach via Nexia member firms in more than 100 countries.
TO: Members of the Joint Audit and Compliance Committee

FROM: David Galloway
Chief Audit and Compliance Officer

DATE: September 27, 2016

SUBJECT: Appointment of NCAA Financial Agreed Upon Procedures Auditors – BKD

RECOMMENDATION

It is recommended that the Joint Audit and Compliance Committee (JACC) approve the appointment of the accounting firm BKD to provide audit services for the years ended June 30, 2016, 2017 and 2018. These services include reporting on the application of agreed-upon procedures in compliance with The National Collegiate Athletic Association (NCAA) Financial Reporting Requirements. The proposed fee for the first year of the engagement is $25,750 plus a 4% administrative fee of $1,030 for a total combined fee of $26,780. The fee for the second and third year of the engagement, the 2017 and 2018 fiscal years, may increase based on hourly rate increases in an amount not to exceed the appropriate Consumer Price Index, and/or changes in duties or responsibilities due to new rules, regulations and accounting or auditing standards.

Year one of the engagement will commence on or about September 28, 2016 and is expected to be completed no later than January 16, 2017. In accordance with the terms of the contract, the University may elect to utilize BKD to provide NCAA financial audit services on an annual basis for up to five consecutive years.

BACKGROUND

NCAA Constitution 3.2.4.15 and 3.2.4.15.1 require that “an institution shall submit financial data detailing operating revenues, expenses and capital related to its intercollegiate athletics program to the NCAA on an annual basis in accordance with the financial reporting policies and procedures... The report shall be subject to annual agreed-on verification procedures approved by the membership (in addition to any regular financial reporting policies and procedures of the institution) and conducted by a qualified independent accountant who is not a staff member of the institution and who is selected by the institution’s chancellor or president or by an institutional administrator from outside the athletics department designated by the chancellor or president. The independent accountant shall verify the accuracy and completeness of the data prior to submission to the institution’s chancellor or president and the NCAA. The institution’s chancellor or president shall certify the financial report prior to submission to the NCAA.”
A bid process was conducted through the University of Connecticut Purchasing Department to select the independent accounting firm to perform the agreed upon procedures. Seven accounting firms submitted proposals.

A committee of five UConn employees independently evaluated the seven proposals based on a set of predetermined qualifications. Evaluation criteria included: quality of the proposed plan and ability to meet the University’s goals and objectives; experience in providing similar services to large public research institutions; capability of staff to manage and conduct audits and evaluate risk; and competitive pricing.

The Purchasing Department collected and tabulated the committee members’ scoring and the committee elected to interview the firms with the three highest total matrix scores on August, 24, 2016. The committee voted to select BKD LLP pending approval of the JACC.

OACE seeks JACC approval to move forward with this engagement.
University of Connecticut & UConn Health

Joint Audit & Compliance Committee Meeting
INTRODUCTION .................................................................................................................... 1
COMMENTS .......................................................................................................................... 2
FOREWORD .......................................................................................................................... 4
Autonomy ............................................................................................................................ 4
UConn 2000....................................................................................................................... 5
Recent Legislation ............................................................................................................. 6
UConn 2000 Authorizations ............................................................................................. 8
Enrollment Statistics ........................................................................................................ 8
RÉSUMÉ OF OPERATIONS ............................................................................................... 9
STATE AUDITORS’ FINDINGS AND RECOMMENDATIONS ........................................... 13
Section 4-33a Reporting Requirements ............................................................................. 13
Deferred Maintenance ...................................................................................................... 14
Non-Competitive Procurement ...................................................................................... 16
Separation Agreement And General Release .................................................................. 17
Excessive Compensation .................................................................................................. 20
Excess Payment For Unused Vacation Accrual ................................................................. 20
Separation Payments ...................................................................................................... 21
Financial System Access Controls .................................................................................. 23
Service Organization Control Reports ............................................................................. 25
Internal Control Over Equipment ................................................................................... 25
Food Services Employees ............................................................................................... 27
Credit Cards ...................................................................................................................... 29
Ethics Certifications ........................................................................................................ 31
Outpatient Pavilion ........................................................................................................ 31
Mileage Logs .................................................................................................................. 34
RECOMMENDATIONS ....................................................................................................... 35
CONCLUSION ..................................................................................................................... 41
We have audited certain operations of the University of Connecticut (UConn) in fulfillment of our duties under Section 2-90 of the Connecticut General Statutes. UConn is a component unit of the University of Connecticut system, which includes UConn, the University of Connecticut Health Center (UConn Health) and the University of Connecticut Foundation, Inc. We also audit the financial statements of UConn and UConn Health and report on those audits separately.

UConn’s financial statements are reflected in the state’s CAFR as part of a major enterprise fund titled University of Connecticut and Health Center. This fund reflects the balances and activity of UConn and UConn Health. The University of Connecticut Foundation, Inc. is reported on separately as a component unit of the state in the CAFR; the University of Connecticut Law School Foundation, Inc. is not included in the CAFR.

The scope of our audit included, but was not necessarily limited to, the fiscal years ended June 30, 2014 and 2015. The objectives of our audit were to:

1. Evaluate UConn’s internal controls over significant management and financial functions.

2. Evaluate UConn’s compliance with policies and procedures internal to the university or promulgated by other state agencies, as well as certain legal provisions.

3. Evaluate the economy and efficiency of certain management practices and operations, including certain financial transactions.

Our methodology included reviewing written policies and procedures, financial records, minutes of meetings, and other pertinent documents; interviewing various personnel of the university, as well as certain external parties; and testing selected transactions. We obtained an understanding of internal controls that we deemed significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in
operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violations of contracts, grant agreements, or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We conducted our audit in accordance with the standards applicable to performance audits contained in Government Auditing Standards, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

The accompanying Résumé of Operations is presented for informational purposes. This information was obtained from UConn’s management and was not subjected to the procedures applied in our audit of UConn. For the areas audited, we identified:

1. Deficiencies in internal controls;
2. Apparent noncompliance with legal provisions; and
3. Need for improvement in management practices and procedures that we deemed to be reportable.

The State Auditors’ Findings and Recommendations in the accompanying report presents any findings arising from our audit of UConn.

**COMMENTS**

**FOREWORD**

UConn, a constituent unit of the state system of higher education, operates generally under the provisions of Title 10a, Chapter 185b, Part III, of the General Statutes. UConn is governed by the Board of Trustees of the University of Connecticut, consisting of 21 members appointed or elected under the provisions of Section 10a-103 of the General Statutes. The board makes rules for the government of the university and determines the general policies of the university pursuant to duties set forth in Section 10a-104 of the General Statutes. The members of the board as of June 30, 2015 were:

Ex officio members:

Dannel P. Malloy, Governor
Sanford Cloud Jr., Chairperson of the UConn Health Center Board of Directors
Steven K. Reviczky, Commissioner of Agriculture
Catherine H. Smith, Commissioner of Economic and Community Development
Dianna R. Wentzell, Commissioner of Education

Appointed by the Governor:

Lawrence D. McHugh, Middletown, Chair
Louise M. Bailey, West Hartford, Secretary
Andy F. Bessette, West Hartford
Charles F. Bunnell, East Haddam
Shari G. Cantor, West Hartford
Andrea Dennis-LaVigne, Simsbury
Marilda L. Gandara, Hartford
Juanita T. James, Stamford
Thomas E. Kruger, Stamford
Rebecca Lobo, Granby
Denis J. Nayden, Stamford
Thomas D. Ritter, Esq., Hartford

Elected by alumni:

Richard T. Carbray Jr., Rocky Hill
Donny E. Marshall, Coventry

Elected by students:

Michael K. Daniels, Plainville
Jeremy L. Jelliffe, Willimantic

Dannel P. Malloy served as Governor during the audited period.

Brien T. Buckman of Stamford; Peter S. Drotch of Framingham, Massachusetts; Lenworth M. Jacobs, M.D., of West Hartford; Wayne J. Shepperd of Danbury; and Richard Treibick of Greenwich completed their terms on June 30, 2013. They were succeeded by Andy F. Bessette of West Hartford, Charles F. Bunnell of East Haddam, Shari G. Cantor of West Hartford, Michael K. Daniels of Plainville and Andrea Dennis-LaVigne of Simsbury, effective July 1, 2013.

Francis X. Archambault, Jr., of Storrs completed his term on August 31, 2013 and was succeeded by Donny E. Marshall of Coventry, effective September 1, 2013. Rose Barham of Newington completed her term effective June 30, 2014 and was succeeded by Jeremy L. Jelliffe of Willimantic, effective July 1, 2014. Stefan Pryor served as Commissioner of Education until he was succeeded by Dianna R. Wentzell in January 2015.

Michael K. Daniels of Plainville and Juanita T. James of Stamford completed their terms on June 30, 2015. Michael K. Daniels was succeeded by David Rifkin of Glastonbury, effective July 1, 2015.
Pursuant to Section 10a-108 of the General Statutes, the board of trustees is to appoint a president of UConn to be the chief executive and administrative officer of the university and the board. Susan Herbst was appointed on December 20, 2010 and serves as the 15th president of the university.

UConn’s main campus is located in Storrs, Connecticut. The university maintains additional facilities and carries out programs at locations across the state. These facilities and programs include:

Avery Point:

Undergraduate and Graduate Programs at Avery Point
Connecticut Sea Grant College Program
Northeast Underwater Research, Technology & Education Center

Farmington:

UConn Health

Greater Hartford:

Undergraduate and Graduate Programs at Hartford
UConn School of Law
School of Social Work
Graduate Business Learning Center

Stamford:

Undergraduate and Graduate Programs at Stamford
Connecticut Information Technology Institute

Torrington:

Undergraduate Programs at Torrington

Waterbury:

Undergraduate and Graduate Programs at Waterbury

Operations of UConn Health are examined and reported upon separately by the Auditors of Public Accounts.

Autonomy

Statutes governing the state’s constituent institutions of higher education provide UConn notable autonomy and flexibility. Public Act 91-256 greatly expanded certain limited authorities
This independence is most notable with respect to procurement. Institutions of higher education may, under Section 10a-151b of the General Statutes, purchase equipment, supplies and contractual services, execute personal service agreements or lease personal property without the approval of the Comptroller, the Secretary of the Office of Policy and Management, or the Commissioner of the Department of Administrative Services. Personal service agreements are not subject to the restrictions codified under Sections 4-212 through 4-219 of the General Statutes. As a compensating measure, personal service agreements executed by institutions of higher education must satisfy the same requirements generally applicable to other procurement actions.

Under Section 3-25 of the General Statutes, higher education institutions may, subject to the approval of the Comptroller, pay most non-payroll expenditures (those funded from the proceeds of state bond issues being an exception) directly instead of through the Comptroller. UConn issues checks that are drawn on a zero balance checking account controlled by the State Treasurer. Under the approved procedures, funds are advanced from the university’s operating fund (a civil list fund) to a Treasurer’s cash management account. These advances are recorded as higher education operating expenses on the Comptroller’s books. The Treasurer transfers funds from the cash management account to UConn’s zero balance direct disbursement checking account on a daily basis, as needed to satisfy checks that have cleared.

All UConn payments, except for certain transactions involving student receipts, are made through the zero balance checking account. UConn’s operating fund is reimbursed on a daily basis for payments made on behalf of UConn’s non-civil list funds (UConn 2000 bond proceeds and UConn’s special local fund); the University of Connecticut Research Foundation Fund reimburses the operating fund on a monthly basis. The reimbursements are posted to the operating fund by crediting higher education operating expenses.

Although Section 3-25 clearly states that “payments for payroll…shall be made solely by the Treasurer….” UConn pays the majority of its food service employees directly. This arrangement is discussed in more detail in the State Auditors’ Findings and Recommendations section of this report.

UConn also enjoys a significant degree of autonomy with respect to personnel matters. Section 10a-108 of the General Statutes grants the board of trustees the authority to employ the faculty and other personnel needed to operate and maintain the institutions under its jurisdiction and establish the terms and conditions of employment. Section 10a-154b allows institutions of higher education to establish positions and approve the filling of vacancies within the limits of available funds.

**UConn 2000**

Public Act 95-230, known as The University of Connecticut 2000 Act, authorized a massive infrastructure improvement program to be managed by UConn. Subsection (c) of Section 7 of the
act, codified as Section 10a-109g subsection (c) of the General Statutes, provided that the securities issued to fund this program are to be issued as general obligations of UConn. However, the act committed the state to fund the debt service on these securities, both principle and interest, almost entirely from the resources of the General Fund. Per subsection (c) of Section 5 of the act, codified as Section 10a-109e subsection (c) of the General Statutes, “As part of the contract of the state with the holders of the securities secured by the state debt service commitment and pursuant to section 21 of this act, appropriation of all amounts of the state debt service commitment is hereby made out of the resources of the general fund and the treasurer shall pay such amount in each fiscal year, to the paying agent on the securities secured by the state debt service commitment or otherwise as the treasurer shall provide.”

These securities, to the extent that related debt service will be funded from the state debt service commitment, are considered to be indebtedness of the state for purposes of the bond limitation established by Section 3-21 of the General Statutes. However, they are not considered to be a state bond issue as referred to in Section 3-25 of the General Statutes. Therefore, UConn is able to make payments related to the program directly, rather than through the Comptroller.

Subdivision (1) of subsection (b) of Section 9 of Public Act 95-230 established a permanent endowment fund, the net earnings on the principal of which are to be dedicated and made available for endowed professorships, scholarships and programmatic enhancements. To encourage donations, the act provided for state matching funds for eligible donations deposited into the fund, subject to specific caps. Effective July 1, 1998, Section 28 of Public Act 98-252 explicitly authorized the deposit of state matching funds in a foundation operating pursuant to Sections 4-37e and 4-37f to clarify that state matching funds could become foundation assets.

The enabling legislation for this program was subsequently amended, extending it through the fiscal year ending June 30, 2014 and modifying the matching percentage. However, Public Act 05-3, codified as Section 10a-8c of the General Statutes, effectively ended the program by providing that the matching funds are not to be disbursed unless the state’s budget reserve (rainy day fund) equals ten percent of the net General Fund appropriation for the fiscal year in progress.

Recent Legislation

Noteworthy legislation affecting UConn and UConn Health that became effective during the period under review and thereafter is presented below:

- Public Act 13-118, Section 5, removed the responsibility of the Board of Regents for Higher Education to approve new academic programs at UConn, leaving the authority to approve new academic programs to the Board of Trustees of the University of Connecticut.

- Public Act 13-143 requires a report from the Board of Regents for Higher Education and the Board of Trustees for the University of Connecticut regarding administrative salaries and the ratio of administrators to faculty and students.
Public Act 13-177, Section 1, established a process for the awarding of design-build contracts by UConn. Section 3 of the act amended Section 10a-151b of the General Statutes to allow for noncompetitive purchases of agricultural products in an amount of $50,000 or less.

Public Act 13-233 established the Next Generation Connecticut initiative as part of the UConn 2000 program, increasing the authorized amount of state bond funding by $1,551,000,000.

Public Act 14-98, Section 2, authorized the issuance of state bonds for the Comptroller for enhancements and upgrades to the Core-CT human resources system at UConn, not exceeding $7,000,000. Section 30 of the act reduced the amount authorized for the development of a technology park at UConn from $172,500,000 to $169,500,000.

Public Act 14-112 clarified the university’s authority to acquire and dispose of land.

Public Act 14-217, Section 221, makes members of UConn’s police department unclassified (instead of classified) state employees, but leaves them within the bargaining unit that represents protective services employees.

Public Act 15-1, June Special Session, Sections 2 and 21, authorized $156,000,000 for the office of Policy and Management for information and technology capital investment program, directing that $41,000,000 be made available for the purchase and implementation of an integrated electronic medical records system at UConn Health. It also authorizes UConn to revise, delete, or add a particular project or projects in its UConn 2000 infrastructure improvement program to finance the implementation of the electronic medical records system at UConn Health.

Public Act 15-1, December Special Session, Section 19, directs that $8,500,000 and $3,000,000 be transferred from UConn and UConn Health operating funds, respectively, to the state’s General Fund for the fiscal year ended June 30, 2016. Section 19 of the act also released UConn from any liability for overstated fringe benefit assessments charged to the state’s General Fund in fiscal years ending June 30, 2003 to June 30, 2015, inclusive, due to an allocation error in the state’s accounting system.

Public Act 15-5, June Special Session, Section 416, allows UConn to provide health care coverage for graduate assistants and others through the partnership plan (the state-administered plan for non-state public or nonprofit employers), provided the related premiums and expenses are not charged to the state’s General Fund (consistent with past practice with respect to such costs).

Public Act 15-244, Section 49, provides that for the fiscal years ending June 30, 2016 and June 30, 2017, UConn expenditures for institutional administration, defined as system office, executive management, fiscal operations and general administration,
exclusive of expenditures for logistical services, administrative computing and
development, shall not exceed three and thirty-five hundredths per cent of the annual
General Fund appropriation and operating fund expenditures, exclusive of capital
bond and fringe benefit funds.

**UConn 2000 Authorizations**

As of June 30, 2015, projects totaling $4,619,300,000 were authorized by the legislature
under the enabling legislation for the UConn 2000 program. The estimated costs do not represent
spending caps at the project level or in the aggregate.

<table>
<thead>
<tr>
<th>Authorizing Legislation</th>
<th>Cumulative Estimated Costs</th>
<th>Cumulative Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>UConn Bonds</td>
</tr>
<tr>
<td>PA 95-230</td>
<td>$1,250,000,000</td>
<td>$962,000,000</td>
</tr>
<tr>
<td>PA 02-3</td>
<td>2,598,400,000</td>
<td>2,262,000,000</td>
</tr>
<tr>
<td>PA 10-104</td>
<td>2,805,400,000</td>
<td>2,469,000,000</td>
</tr>
<tr>
<td>PA 11-75</td>
<td>3,068,300,000</td>
<td>2,731,900,000</td>
</tr>
<tr>
<td>PA 13-233</td>
<td>4,619,300,000</td>
<td>4,282,900,000</td>
</tr>
</tbody>
</table>

[a] Under Section 5 subsection (b) of Public Act 95-230, the funding for UConn 2000 included $18,000,000 in state
general obligation bonds authorized under Section 1 of Public Act 95-270 and $962,000,000 in UConn bonds
authorized under Section 4 subsection (a) of Public Act 95-230.

The legislature authorized additional funding through the issuance of state general obligation
bonds. These bonds are obligations of the state and are not included as debt in the UConn
financial statements. Several projects were funded in this manner; the most significant was the
provision, under Section 92 of Public Act 11-57, as amended by Section 30 of Public Act 14-98,
of up to $169,500,000 for the development of a technology park at the university.

**Enrollment Statistics**

Statistics compiled by the UConn registrar present the following enrollments in the
university’s credit programs during the audited period and during the preceding year.

<table>
<thead>
<tr>
<th>Student Status</th>
<th>Fall 2012</th>
<th>Fall 2013</th>
<th>Fall 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undergraduates</td>
<td>22,301</td>
<td>22,595</td>
<td>22,973</td>
</tr>
<tr>
<td>Graduates</td>
<td>6,613</td>
<td>6,555</td>
<td>6,830</td>
</tr>
<tr>
<td>Professional (School of Law and Doctor of Pharmacy)</td>
<td>814</td>
<td>782</td>
<td>761</td>
</tr>
<tr>
<td>Medicine – Students</td>
<td>359</td>
<td>368</td>
<td>384</td>
</tr>
<tr>
<td>Medicine – Other (1)</td>
<td>625</td>
<td>645</td>
<td>650</td>
</tr>
<tr>
<td>Dental – Students</td>
<td>169</td>
<td>174</td>
<td>171</td>
</tr>
<tr>
<td>Dental – Other (1)</td>
<td>117</td>
<td>114</td>
<td>110</td>
</tr>
<tr>
<td>Totals</td>
<td>30,998</td>
<td>31,233</td>
<td>31,879</td>
</tr>
</tbody>
</table>

(1) Other includes residents, interns and post-graduate clinical enrollment.
RÉSUMÉ OF OPERATIONS

Under the provisions of Section 10a-105 subsection (a) of the General Statutes, fees for tuition are fixed by the board of trustees. The following summary presents annual tuition charges during the audited period.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Undergraduates</td>
<td>$9,256</td>
<td>$28,204</td>
<td>$16,198</td>
<td>$9,858</td>
<td>$30,038</td>
<td>$17,250</td>
</tr>
<tr>
<td>Graduates</td>
<td>11,456</td>
<td>29,740</td>
<td>20,048</td>
<td>12,202</td>
<td>31,674</td>
<td>21,354</td>
</tr>
<tr>
<td>School of Law</td>
<td>23,818</td>
<td>50,134</td>
<td>41,682</td>
<td>25,366</td>
<td>53,392</td>
<td>44,390</td>
</tr>
</tbody>
</table>

Generally, the Comptroller accounts for UConn operations in:

- General Fund appropriation accounts.
- The University of Connecticut Operating Fund.
- The University of Connecticut Research Foundation Fund.
- Accounts established in other funds for appropriations financed primarily with bond proceeds.

UConn maintains additional accounts that are not reflected in the state’s civil list financial system. The most significant relate to the UConn 2000 infrastructure improvement program. They are used to account for the proceeds of UConn 2000 bonds and related expenditures.

UConn’s financial statements are prepared in accordance with all relevant Governmental Accounting Standards Board (GASB) pronouncements. UConn utilizes the proprietary fund method of accounting whereby revenue and expenses are recognized on the accrual basis.

UConn’s financial statements are adjusted as considered necessary and incorporated into the state’s Comprehensive Annual Financial Report. The financial balances and activity of the university are combined with those of UConn Health, including John Dempsey Hospital, and presented as an enterprise fund titled University of Connecticut and Health Center.

UConn employment grew slightly during the audited period. UConn reported 4,757, 4,816 and 4,801 full and part-time faculty and staff (excluding adjunct faculty and other special payroll employees, graduate assistants, dining services employees and student labor) as of the Fall 2013, 2014 and 2015 semesters, respectively.

UConn’s financial report for the year ended June 30, 2014 reflects the restatement of amounts presented for the fiscal year ended June 30, 2013 in accordance with the provisions of
Governmental Accounting Standards Board (GASB) Statement No. 65. The restatement decreased UConn’s total net position as of June 30, 2013 by $12,631,459 to $1,439,421,293. The decrease reflected the change in the treatment of fees associated with issuance of long-term bonds. Previously accrued and amortized over the life of the bonds, these costs were retroactively reclassified as expenses of the year in which the bonds were issued.

UConn’s total net position increased by $4,060,893 from $1,439,421,293 as of June 30, 2013, as restated, to $1,435,360,400 as of June 30, 2014. It then decreased by $437,761,126 to $997,599,275 as of June 30, 2015. This decrease was primarily attributable to the adoption of GASB Statements No. 68 and 71, which required UConn to recognize a liability for its proportionate share of the net pension liability of the state’s defined benefit pension plans in its stand-alone financial statements.

UConn recorded a prior year adjustment for pensions to its beginning total net position for the fiscal year ended June 30, 2015 of $577,593,380. As of June 30, 2015, UConn’s net pension liability, net of associated deferred outflows and inflows, was $588,299,586. The decrease in total net position caused by the adoption of GASB Statements No. 68 and 71 was partially offset by the allocation of $131,500,000 for the development of a technology park at UConn as authorized under Section 10a-110m of the General Statutes.

UConn’s unrestricted net position balance decreased by $22,672,034 from $153,490,047 as of June 30, 2013, as restated, to $130,818,013 as of June 30, 2014. It decreased again by $560,092,561 to a deficit balance of $429,274,548 as of June 30, 2015. The decrease of $560,092,561 reflects UConn’s recognition of its proportionate share of the net pension liability of the state’s defined benefit pension plans, which was applied entirely to unrestricted net position.

UConn’s cash and cash equivalents balance declined during most of the last several fiscal years. The June 30, 2011 balance of $276,484,964 fell by $9,690,367 to $266,794,597 as of June 30, 2012, by $22,008,793 to $244,785,804 as of June 30, 2013 and by $26,595,630 to $218,190,174 as of June 30, 2014. It recovered slightly in the following year, increasing by $14,761,367 to $232,951,541 as of June 30, 2015.

UConn revenues, operating and non-operating, and other additions totaled $1,142,545,855 and $1,348,837,834 for the fiscal years ended June 30, 2014 and 2015, respectively. General Fund support, in the form of annual appropriations for operating expenses, in-kind fringe benefit support, the state debt service commitment for principle and interest on UConn 2000 related bonds and capital funding allocations, was UConn’s largest source of revenue. It totaled $430,485,717 (38 percent) and $585,264,257 (43 percent) of total revenues and other additions for the fiscal years ended June 30, 2014 and 2015, respectively. The increase in the second year of the audited period was primarily attributable to the allocation of funding under Section 10a-110m of the General Statutes, as discussed above.

Other significant sources of revenue included student tuition and fees, sales and services of auxiliary enterprises, and grant and contract revenues. Student tuition and fees were $279,577,280 and $308,174,254 for the fiscal years ended June 30, 2014 and 2015, respectively.
Sales and services of auxiliary enterprises were $195,524,781 and $201,065,628 for the fiscal years ended June 30, 2014 and 2015, respectively. Grant and contract revenues (federal, state and local and non-governmental) totaled $162,623,098 and $170,848,520 for the fiscal years ended June 30, 2014 and 2015, respectively.

UConn expenses, operating and non-operating, and other deductions totaled $1,146,606,747 and $1,209,005,580 for the fiscal years ended June 30, 2014 and 2015, respectively. Most were classified as operating expenses. A schedule of operating expenses by functional classification follows:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction</td>
<td>353,250,856</td>
<td>382,255,349</td>
</tr>
<tr>
<td>Research</td>
<td>79,483,638</td>
<td>73,596,010</td>
</tr>
<tr>
<td>Public Service</td>
<td>41,918,518</td>
<td>48,883,867</td>
</tr>
<tr>
<td>Academic Support</td>
<td>125,556,692</td>
<td>131,913,698</td>
</tr>
<tr>
<td>Student Services</td>
<td>36,787,251</td>
<td>36,954,846</td>
</tr>
<tr>
<td>Institutional Support</td>
<td>54,484,055</td>
<td>57,329,806</td>
</tr>
<tr>
<td>Operations and Maintenance of Plant</td>
<td>105,147,738</td>
<td>114,888,599</td>
</tr>
<tr>
<td>Depreciation</td>
<td>95,376,695</td>
<td>95,990,463</td>
</tr>
<tr>
<td>Student Aid</td>
<td>8,796,255</td>
<td>9,126,577</td>
</tr>
<tr>
<td>Auxiliary Enterprises</td>
<td>196,934,393</td>
<td>209,633,188</td>
</tr>
<tr>
<td>Total Operating Expenses</td>
<td>1,097,736,091</td>
<td>1,160,572,403</td>
</tr>
</tbody>
</table>

The non-operating expenses during the audited period consisted primarily of interest payments. Interest expense was $45,955,335 and $46,420,112 for the fiscal years ended June 30, 2014 and 2015, respectively. Most of this expense involved UConn general obligation bonds and was offset by General Fund support in the form of the state debt service commitment for interest, which was $42,090,775 and $46,635,328 for the fiscal years ended June 30, 2014 and 2015, respectively. As the state debt service commitment for interest is based on the payment of interest to bond holders it can differ from interest expense per se, which also reflects the amortization of bond premiums and discounts and gains/losses on refundings.
UConn did not hold significant endowment and similar fund balances during the audited period, as it has been the university’s longstanding practice to deposit funds raised with the University of Connecticut Foundation, Inc. or the University of Connecticut Law School Foundation, Inc. The University of Connecticut Foundation, Inc. provides support for UConn and UConn Health. Its financial statements reflect balances and transactions associated with both entities, not only those exclusive to the university. A summary of the two foundations’ assets, liabilities, net assets, revenue and support, expenses and other changes, as per those audited financial statements, follows:

<table>
<thead>
<tr>
<th></th>
<th>University of Connecticut Foundation, Inc.</th>
<th></th>
<th>Law School Foundation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fiscal Year Ended</td>
<td>Fiscal Year Ended</td>
<td></td>
</tr>
<tr>
<td></td>
<td>June 30, 2014</td>
<td>June 30, 2015</td>
<td>June 30, 2014</td>
</tr>
<tr>
<td>Assets</td>
<td>$489,928,000</td>
<td>$482,433,000</td>
<td>$21,143,701</td>
</tr>
<tr>
<td></td>
<td>$482,433,000</td>
<td>$22,854,584</td>
<td></td>
</tr>
<tr>
<td>Liabilities</td>
<td>53,019,000</td>
<td>46,651,000</td>
<td>6,041</td>
</tr>
<tr>
<td></td>
<td>46,651,000</td>
<td>6,041</td>
<td>2,633</td>
</tr>
<tr>
<td>Net Assets</td>
<td>436,909,000</td>
<td>435,782,000</td>
<td>21,137,660</td>
</tr>
<tr>
<td></td>
<td>21,137,660</td>
<td>22,851,951</td>
<td></td>
</tr>
<tr>
<td>Revenue and Support</td>
<td>91,426,000</td>
<td>53,422,000</td>
<td>3,940,115</td>
</tr>
<tr>
<td></td>
<td>3,940,115</td>
<td>3,384,953</td>
<td></td>
</tr>
<tr>
<td>Expenses</td>
<td>68,004,000</td>
<td>54,422,000</td>
<td>1,444,997</td>
</tr>
<tr>
<td></td>
<td>1,444,997</td>
<td>1,670,662</td>
<td></td>
</tr>
<tr>
<td>Other Changes</td>
<td>18,000</td>
<td>(127,000)</td>
<td></td>
</tr>
</tbody>
</table>
STATE AUDITORS’ FINDINGS AND RECOMMENDATIONS

Our review of the financial records of the University of Connecticut disclosed certain areas requiring attention, as discussed in this section of the report.

SECTION 4-33A REPORTING REQUIREMENTS

Criteria: Under Section 4-33a of the General Statutes, state agencies are required to promptly notify the Auditors of Public Accounts and the Comptroller of any unauthorized, illegal, irregular or unsafe handling or expenditure of state funds or breakdowns in the safekeeping of any other resources of the state or contemplated action to do the same within their knowledge. Section 4-33a requires notification in cases of proven malfeasance or breakdowns in internal control affecting the safekeeping of any state resources.

Condition: In February 2015, it came to our attention that National Science Foundation funds administered by UConn were used to purchase 15 specialized acoustic modems during April through August 2013 at a total cost of $253,500 from AquaSeNT, a privately held company founded by UConn faculty. The transactions, which were processed as sole source purchases, were initiated by faculty that had interests in AquaSeNT.

These sole source transactions appear to have violated provisions of Section 1-84 of the General Statutes which address such conflicts of interest and 2 CFR 215.42, which prohibits the participation of individuals with an interest in the firm selected in the procurement process. Although UConn administrators were aware of the specifics of the incident, they failed to notify us as required under Section 4-33a.

Effect: Central state agencies have responsibilities with respect to the matters described in Section 4-33a. If state agencies do not promptly notify them of incidents falling under the statute, they cannot fulfill their responsibilities by responding appropriately in a timely manner.

Cause: We were unable to determine why UConn did not promptly report this matter as required.

Recommendation: The University of Connecticut should promptly report as required under Section 4-33a of the General Statutes as soon as a reasonable suspicion exists that a reportable incident has occurred. Any doubt as to whether an incident is reportable under Section 4-33a should be resolved by reporting it. (See Recommendation 1.)

Agency Response: “Over the past few years, the University has taken a number steps to improve compliance with the reporting requirement of Section 4-33a of
Auditors of Public Accounts

the General Statutes. A report of property lost, stolen or vandalized is provided to the Auditors of Public Accounts and the Comptroller on a monthly basis. A soon to be implemented policy, titled The Prevention and Reporting of Fraud and Fiscal Irregularities, more clearly defines faculty, staff and other community members’ responsibility for protecting University assets, and reporting suspected fraud and other fiscal irregularities. This policy also formally establishes a centralized process to coordinate the identification and assessment of such matters to facilitate timely and appropriate reporting.”

DEFERRED MAINTENANCE

Criteria:
Section 10a-109ee of the General Statutes requires UConn to “provide that all funds allocated to UConn 2000...for the purpose of deferred maintenance...be expended for such purpose.” In an October 2010 memorandum, UConn’s bond counsel addressed the use of UConn 2000 deferred maintenance funding. The counsel concluded that the funds allocated for deferred maintenance cannot be used for the construction of new buildings or additions to existing buildings. The counsel referred to the statutory definition of deferred maintenance and the related federal Accounting Standards Advisory Board definitions, emphasizing that “Maintenance excludes activities aimed at expanding the capacity of an asset or otherwise upgrading it to serve needs different from, or significantly greater than, those originally intended.”

Condition:
We reviewed requests for project approval submitted to the University of Connecticut Board of Trustees in connection with 20 of the larger recent deferred maintenance projects. We noted that the primary objective of 10 of the 20 projects was to expand the capacity of, or otherwise upgrade, assets.

These 10 projects, with budgeted amounts, included:

- 901820 – $23,000,000 to renovate Putnam Refectory in order to increase dining hall seating capacity from 400 to 700.
- 201630 – $4,700,000 to construct an fMRI Center in the Philips Communication Sciences Building.
- 901735 – $6,591,000 for pedestrian safety improvements that will enhance the campus.
- 901629 – $4,000,000 for pedestrian safety improvements that will enhance the campus.
- 901726 – $3,000,000 for pedestrian safety improvements that will enhance the campus.
- 901422 – $2,300,000 to increase water delivery capacity by installing a new 16” water main and to bury electrical lines.
Auditors of Public Accounts

University of Connecticut 2014 and 2015

- 901757 – $1,865,000 to renovate two existing laboratories into state-of-the-art research laboratories.
- 901812 – $1,500,000 for site improvements at the intersection of Route 195 and Bolton Road.
- 901730 – $1,300,000 to convert rooms in the Pharmacy/Biology Building into laboratory and office space to accommodate new faculty and relocate existing faculty and programs.
- 901368 – $850,000 for a sludge discharge filter press to reduce disposal costs by about $125,000 annually.

Effect: Funds allocated for deferred maintenance were used for purposes not authorized by statute. In addition to creating a condition of noncompliance with statutory provisions, this appears to have hampered efforts to reduce the backlog of actual deferred maintenance.

Cause: We could not determine why UConn used deferred maintenance funds for these projects.

Recommendation: The University of Connecticut should move ongoing projects that are not consistent with the statutory definition of deferred maintenance to different funding sources. Legislative authorization should be sought for projects that do not constitute deferred maintenance and are not otherwise named in Section 10a-109e of the General Statutes. (See Recommendation 2.)

Agency Response: “The University, like all state agencies, does not have access to sufficient funding to make all the necessary and appropriate repairs to its facilities and infrastructure. As a result, the University intentionally designs projects to repair under-maintained facilities and infrastructure up to current standards. The University views this capital planning process as an efficient and effective use of state resources generally, as well as an appropriate use of DM/Renovation funding under UCONN 2000.

We agree that Deferred Maintenance/Code/ADA Renovation funding should not be utilized to construct new buildings or to expand the footprint of existing buildings. The principal basis of any project utilizing this funding is for the repair or renovation of an under-maintained facility or infrastructure to bring it to current standards. The University has consistently reported this utilization of such funding to the legislature and other state agencies without objection.

After Deferred Maintenance/Code/ADA Renovation funding has been allocated to a project, the project may change in scope in a way that requires the University to reconsider whether such allocation remains appropriate. In these and other situations, the statutes authorize the
University to reallocate project funding to a different named-line under UCONN 2000. See Section 10a-109e(d).

Accordingly, the University will review ongoing projects, including those identified above, to determine whether any such reallocation is necessary or appropriate.

In addition, the University will consider pursuing the technical legislative changes suggested above for the sake of added clarity going forward.

NON-COMPETITIVE PROCUREMENT

Criteria: Section 10a-151b of the General Statutes requires constituent units of the state system of higher education to solicit competitive bids or proposals by public notice, when possible, when contracting for professional services. The statutory requirement for open, competitive procurement is intended to facilitate obtaining goods and services at the lowest prices, avoiding favoritism, and awarding public contracts in an equitable manner.

In some instances, there may be only one source for goods or services. If so, competition is not possible. This type of non-competitive procurement action is commonly referred to as a sole source purchase.

Condition: In our test of selected expenditures for the 2015 fiscal year, we noted three transactions that were misclassified as sole source procurements. Documentation on file indicated that the selected vendors were chosen after a limited review of alternatives. If these procurement actions had truly been sole source procurements, there would not have been any alternatives to review. Though there was a limited review of alternatives, the procedures followed did not meet the requirements of Section 10a-151b of the General Statutes. UConn did not begin the process by soliciting competitive proposals or bids by public notice, a procedure that is critical to an open, competitive procurement process.

Misclassified transactions we noted included:

A contract for the purchase of electron microscopes from a leading technology company for an amount not to exceed $12,000,000. As of November 2015, $6,258,903 had been expended under this contract. Documentation on file indicates that, although UConn considered purchasing these instruments from this vendor to be the most appropriate solution, there are a number of instrument manufacturers producing competing products.
A contract for the provision of services related to the study abroad program in Italy. Expenditures under this contract totaled $1,257,988. Documentation on file indicates that there were at least three alternatives to the vendor UConn contracted with.

A contract for the provision of services related to the study abroad program in England. Expenditures under this contract totaled $1,036,963. Documentation on file indicates the presence of numerous alternatives.

Effect: These transactions did not comply with the provisions of Section 10a-151b. It is possible that the goods and services could have been obtained at a lower price if an open, competitive procurement process had been followed. In addition, other potential vendors were denied the opportunity to bid on the contracts. Open access to state contracts is in the public interest.

Cause: It appears UConn felt that an open, competitive procurement process was not needed for these transactions.

Recommendation: The University of Connecticut should comply with the competitive procurement requirements of Section 10a-151b of the General Statutes. Procurement actions should not be characterized as sole source purchases unless no other source exists that is capable of meeting the requirements. (See Recommendation 3.)

Agency Response: “The State Auditor recommends that “Procurement actions should not be characterized as sole source purchases unless no other source exists that is capable of meeting the requirements.” UConn acknowledges this recommendation. In the case of the electron microscopy instruments, a thorough and detailed scholarly analysis was performed.”

SEPARATION AGREEMENT AND GENERAL RELEASE

Background: A separation agreement and general release addresses the terms of an employee's separation from employment, including a release of claims against the employer, in consideration for certain separation or severance benefits the employee would otherwise not be entitled to receive. Although benefits generally accrue to both parties, these agreements are primarily designed to protect the employer.

Non-disparagement clauses are common to such agreements. Non-disparagement clauses generally specify that the departing employee will not make any negative or disparaging statements about the employer, its officers, or members of its board. Similarly, the employer usually agrees not to make any negative comments about the employee.
Restrictions such as non-disparagement clauses can have a chilling effect on the willingness of employees to report inappropriate activity. This is a serious concern, as evidenced by recent actions taken by federal agencies.

The Equal Employment Opportunity Commission (EEOC) brought an enforcement action against CVS Pharmacy (CVS), maintaining language in the company’s agreement carving out the employee’s right to “participate in a proceeding with any appropriate federal, state or local government agency enforcing discrimination laws” was insufficient to offset a covenant forbidding “any statements that disparage the business or reputation” of the company. The EEOC contended that this did not clearly communicate to non-attorney CVS employees that they retain the right to file a charge of discrimination.

In April 2015, the Securities and Exchange Commission (SEC) announced its first enforcement action against a company for using improperly restrictive language in confidentiality agreements with the potential to stifle the whistleblowing process. The defendant voluntarily amended its confidentiality statement by adding language making clear that employees are free to report possible violations to the SEC and other federal agencies without approval or fear of retaliation.

**Criteria:**

When a state agency is party to a separation agreement that contains a non-disparagement clause, the agreement should make it clear that the non-disparagement clause does not in any way restrict the employee’s right to file a whistleblower complaint under Section 4-61dd of the General Statutes. The language used should be plain and unambiguous so that non-attorney employees will understand that they will not be penalized for filing a complaint even if statements included in the complaint could be viewed as disparaging. The agreement should incorporate similar disclosures addressing other actions that are protected by state or federal law or are not in the public interest to obstruct.

**Condition:**

As a matter of policy, managerial and confidential employees who are involuntarily separated from UConn are generally required to execute a separation agreement and general release in order to receive separation benefits. We reviewed language used by UConn in such agreements.

UConn’s agreements do not inform employees that they will not be penalized for filing a whistleblower complaint, even if statements included in the complaint could be viewed as disparaging. Additionally, they do not include exceptions for statements that could be viewed as disparaging made in connection with other actions that are protected by state or federal law or are in the public interest.
One agreement executed in March 2014 provided that the employee “not make any derogatory or defamatory statements about his employment at UConn, about UConn, about any previous or current officer or employee of UConn, or any pervious or current member of the UConn Board of Trustees or the University of Connecticut Health Center Board of Directors.” The only exception we noted was that implied by the statement that the employee “shall cooperate fully with UConn in connection with any investigation and/or hearing…” involving any violations that may have occurred during the employee’s term of employment and “nothing in this agreement shall be construed as limiting or influencing…cooperation or testimony in any such proceeding or investigation.”

Another executed in October 2015 provided that UConn and the employee “agree not to make any defamatory statements about each other.” Similarly, the only exception we noted was implied by the statement that the employee “fully cooperate with the University and the Office of the Attorney General in connection with any litigation or proceedings that may arise from any alleged acts or omissions” that may have occurred during the employee’s term of employment.

Effect: This condition could hinder the effective operation of the state’s whistleblower program by discouraging the reporting of inappropriate activity.

Cause: We were unable to determine why UConn did not include exceptions for complaints filed under Section 4-61dd of the General Statutes as standard language in its separation agreements.

Recommendation: The University of Connecticut should clearly state in any separation agreements incorporating non-disparagement clauses that the clause does not in any way restrict the employee’s right to file a whistleblower complaint under Section 4-61dd of the General Statutes. The agreement should incorporate similar language addressing other actions that are protected by state or federal law or are not in the public interest to obstruct. (See Recommendation 4.)

Agency Response: “The law in this area is evolving. Future non-disparagement clauses will make clear that the clause does not restrict an employee’s right to file a complaint under Section 4-61dd of the General Statutes. We will monitor developments in the law with regard to other protected activity and draft such clauses to make them compliant with applicable law.”
EXCESSIVE COMPENSATION

Criteria: Compensation paid should be commensurate with work performed. When a managerial employee steps down from a position, the compensation should be reduced to a level appropriate to the new job duties.

Condition: It came to our attention that an administrator stayed on the UConn payroll, with no reduction in his $202,829 salary, for a year after stepping down from his management position. Per the employment agreement he was to function, essentially, as a part time consultant. The agreement stated that, though he would have access to office space, his “advisory and consultative duties will primarily be conducted off-site.”

Effect: The employee’s compensation during his final year of employment was not justified by the amount of work he was required to perform.

Cause: None of the documentation on file indicates that the employee’s decision to step down was initiated by the employee.

Recommendation: The University of Connecticut should compensate employees who step down from management positions at a level consistent with the work they are performing, not at a level appropriate for their former positions. (See Recommendation 5.)

Agency Response: “In the absence of a separation agreement, as described in the University response to the Separation Payments finding below, we agree that employees that step down from management positions should be compensated at a level consistent with the work they are performing, not at a level appropriate for their former positions.”

EXCESS PAYMENT FOR UNUSED VACATION ACCRUAL

Criteria: By policy, UConn limits vacation accruals by managerial and confidential exempt and non-represented faculty to 60 days. Exceptions to the 60-day limit are allowed with the approval of the appropriate administrator.

However, UConn’s policy clearly provides that, irrespective of the amount accrued, payments for unused vacation accruals upon separation will be limited to a maximum of 60 days. The policy allows for modification of this limit by the board of trustees.

Condition: We reviewed payments for unused accumulated leave balances made to 25 employees during the period from July 2013 through January 2015. We found that one managerial employee was paid $90,461 for 120 days of unused accrued vacation balance, twice the maximum allowable amount.
Although we were told that this payment was in accordance with an agreement between UConn and the employee, UConn was not able to provide us with a copy of this agreement when we requested it. We did note the presence of memorandums authorizing the employee to accrue more than 60 days of vacation, but there was no indication that the excess accruals would be paid out on separation.

The language of the policy indicates that board of trustees’ approval would be necessary to modify this benefit. We found no indication that the board of trustees approved the payment for an additional 60 days of vacation accruals.

**Effect:** An unauthorized payment of $45,230 was made to the employee.

**Cause:** There appeared to have been a general belief that the payment was in accordance with an agreement between UConn and the employee. However, UConn was not able to provide us with a copy of this agreement.

**Recommendation:** The University of Connecticut should follow its policy regarding vacation payout upon separation. The university should attempt to recover the unauthorized payment of $45,230. (See Recommendation 6.)

**Agency Response:** “Upon separation from the University, managerial employees are paid for their unused accrued vacation, up to a maximum of 60 days. In unusual and unique circumstances, payment of unused vacation days in excess of 60, up to a maximum of 120, may be authorized. Going forward, the University will obtain board approval for such payments in accordance with policy. With respect to the finding above, the individual transferred to UConn from another state agency which had a higher vacation balance and payout threshold. This employee was permitted to “carryover” excess vacation days that remained on the books at the end of each calendar year. Authorization was granted from the Associate Vice President for Human Resources and Payroll Services to pay out the employee’s vacation balance of 120 days when he separated from the University. The final payout was consistent with the prior state employer’s accrual and payout practices.”

**SEPARATION PAYMENTS**

**Criteria:** Under UConn’s *Separation Policy for Unclassified Board of Trustees Exempt Managers and Confidential Employees*, management employees who are involuntarily separated from UConn for reasons unrelated to their job performance may be eligible for separation benefits. At UConn’s
discretion, it may offer written notice in advance of the effective date of separation, a lump sum payment of salary in lieu of notice or a combination of the two.

Unless the relationship with an employee has deteriorated to the point that the employee’s continued presence on site would be a detriment, offering notice is the fiscally prudent alternative. Because the same cost would be incurred either way, any services the employee is able to provide would be a net benefit to UConn.

**Condition:** During a test of employees on leave with pay, we noted six instances that constituted payment of salary in lieu of notice to managerial employees. Instead of making a single lump sum payment, UConn paid the equivalent on an installment basis by placing the employees on leave with pay for a period of time immediately prior to their separation date.

We were told that in five of the six instances, the employees were involuntarily separated for reasons unrelated to their job performance. We calculated that, based on the periods of leave with pay and the employees’ rates of pay, the payments to the five employees during the periods of leave with pay totaled $337,455.

**Effect:** UConn lost the opportunity to benefit from the services these employees could have provided.

**Cause:** We were unable to determine why UConn did not elect to provide notice instead of making separation payments.

**Recommendation:** The University of Connecticut should provide notice instead of making separation payments to terminating employees in instances of involuntary separation for reasons unrelated to job performance. (See Recommendation 7.)

**Agency Response:** “As acknowledged in the finding above, there are situations in which an employee’s continued presence on site would be a detriment and offering notice may be more fiscally prudent. UConn’s *Separation Policy for Unclassified Board of Trustees Exempt Managers and Confidential Employees* explicitly provides for notice, or payment in lieu of notice, to employees prior to the effective date of a layoff, position elimination or other separation not related to performance or misconduct. The policy also permits continuation of health insurance and provision of outplacement services. In most cases, a management or confidential employee that has been issued a layoff notice is expected to continue providing service to UConn in an advisory or consultative capacity to either transition their responsibilities to others or to wind down their pending tasks and projects. For a variety of business reasons, such as security concerns and other risk...
management issues, UConn has adopted a policy that gives management the option to either release the employee during the notice period or have the employee work remotely. Finally, working for the full notice period with no separation payment may not be sufficient consideration necessary to enforce the required separation agreement and general release.”

Auditors’ Concluding Comment: In instances in which management feels that the payment in lieu of notice option is the prudent alternative because of security and/or other risk management concerns, written documentation should be prepared that evidences management’s consideration of these factors and clearly describes the basis for management’s conclusion.

FINANCIAL SYSTEM ACCESS CONTROLS

Criteria: Logical access controls are tools used for identification, authentication, authorization, and accountability in computer information systems. They work in conjunction with physical access controls, which address interactions with hardware in the physical environment. Logical access controls need to be properly designed and implemented to safeguard critical systems, programs, processes, and information by preventing access by unauthorized users. A continuing, documented process for identifying and authorizing the appropriate access for individual employees based on business needs is the foundation that supports an organization’s access control measures.

Condition: We reviewed 64 employees with access to Kuali Financial System (KFS), UConn’s financial system. Approved access control forms were not on file for 11(17 percent) of the 64. We also reviewed 226 current or former employees whose access to KFS should have been completely disabled. We found that 11(5 percent) of the 226 still had full or partial access to the system.

Effect: Unauthorized access to the financial system could jeopardize the integrity of the data stored on the system and the business processes it is used to carry out.

Cause: When UConn implemented KFS, access profiles existing in the old financial system were brought forward to KFS without review. UConn has not followed up by performing review and approval processes addressing the access rights of all employees on an individual basis.

Additionally, though procedures are in place to notify information technology administrators when employees separate from UConn, they do not encompass all relevant personnel actions. Administrators are not
notified when individuals are put on administrative leave, end special payroll assignments, end affiliate assignments, end student worker assignments, or are put on leave with pay prior to termination as a form of separation payment.

**Recommendation:** The University of Connecticut should ensure that properly approved access control forms are on file for all individuals with access to KFS. Notification procedures intended to identify all individuals whose access should be disabled should be expanded to encompass all relevant personnel actions. (See Recommendation 8.)

**Agency Response:** “In May of 2012, the KFS Implementation Team reviewed the Security Overview plan for KFS with the Governance Council. This approved plan included the migration of active legacy financial system (FRS) users – who have prior authorization, into KFS with “user” level access. Management believes this was an appropriate course of action, and poses no additional risk to the University. To address this recommendation, management will investigate an electronic user access re-certification process which will recertify all current and legacy users.

Management believes that additional measures are needed to ensure that employees who separate from the University outside of the normal procedure are removed from KFS in a timely manner. Recognizing this, Finance Systems has already put in place several mitigations to identify these users and remove or limit access. These mitigations include: quarterly reviews of all KFS users to determine if identity records are still active in the University ID System, bi-weekly reviews of HR separation reports, setting duration limits of 1 year on all student and affiliate KFS access requests, and working with University Information Technology Services to receive emails when a user inactivation has been requested by Labor Relations. Management will continue to investigate other options to ensure that the access for employees who have separated or are away from the University for a prolonged period of time are promptly disabled and/or removed from KFS.”
SERVICE ORGANIZATION CONTROL REPORTS

**Criteria:** Service Organization Control (SOC) reports are used to gain assurance over outsourced operations. SOC 1 reports focus on internal control over financial reporting. SOC 2 and SOC 3 reports focus on compliance or operational controls relevant to security, availability, confidentiality, processing integrity, and privacy. An effective way of managing the risk of utilizing service organizations is by obtaining and reviewing the appropriate SOC reports. Documentation of the review process should include follow-up action taken in response to any reported deficiencies.

**Condition:** UConn utilizes service organizations to perform various operations. We noted several instances in which SOC reports were available, but were not obtained and reviewed.

**Effect:** The lack of due diligence for prospective service organizations and governance oversight of current service organizations may put UConn at risk.

**Cause:** Overall responsibility for acquiring and reviewing SOC reports has not been assigned.

**Recommendation:** The University of Connecticut should develop a centralized process for monitoring and obtaining assurance over service organizations. (See Recommendation 9.)

**Agency Response:** “When available, the University will ask major technology service providers to provide their SOC reports. The University is modifying its contract language to include this requirement. It is the responsibility of each procuring department to monitor vendor performance with respect to specific terms and conditions. This will be reinforced generally as well as specifically for this additional contract language via direct interactions with central purchasing and via a general communication to the University community.”

INTERNAL CONTROL OVER EQUIPMENT

**Criteria:** In order to provide adequate internal control over equipment, the inventory control system must accurately reflect the location of the equipment and the last date it was physically inventoried.

**Condition:** UConn inventory control procedures require those responsible for equipment items to enter all movements of equipment in the financial system’s capital asset management module. However, during our annual physical inventory, we found 21 out of 74 tangible capital equipment
items selected for testing (28 percent) at a different location than that shown in the inventory records.

Furthermore, we noted that changing certain location attributes of an asset in the financial system’s capital asset management module will update the last inventory date field – giving the incorrect impression that the existence and location of the equipment item has been physically verified. This condition affected at least two of the equipment items in our selection. In one instance, documentation on file indicated that the item was not at the location shown at the time the last inventory date field was updated. In the second, the item had not yet been tagged and documentation on file indicated that it was at sea on a research vessel and unavailable at the time the last inventory date field was updated.

**Effect:**

The conditions noted above weaken internal control over equipment, increasing the likelihood that assets could be misappropriated or lost.

**Cause:**

It does not appear that the requirement to enter all movements of equipment in the financial system’s capital asset management module is being enforced. Allowing the last inventory date field to update when the existence and location of the equipment item has not been physically verified is a design flaw.

**Recommendation:**

The University of Connecticut should enforce the existing procedural requirement that those responsible for equipment items enter all movements of equipment in the financial system’s capital asset management module. The last inventory date field should only be updated when the existence and location of the equipment item has been physically verified. (See Recommendation 10.)

**Agency Response:**

“The Inventory Control unit completes an annual physical inventory of approximately 15,600 pieces of equipment with an original cost of $5,000 or more. Equipment within departments and buildings is mobile and, as such, is often moved from one room to another to facilitate sharing. For instance a piece of equipment may move from one lab to another lab on the same day. It is impractical to record the frequent and recurring movement of such mobile equipment. Centralized Inventory Control staff tag and cycle University equipment and also rely on departments to assist in tagging, recording the movement and the physical inventory of equipment.

The Inventory Control unit of the Controller’s division does provide communication and training on the University requirement to enter movements of equipment in the financial system but cannot monitor all equipment location changes given the decentralized and mobile nature of the University’s equipment. Equipment locations not updated on a daily
basis are updated in the annual physical inventory process as required by Section 4-36 of the General Statutes of Connecticut.

In addition, the last inventory date field is updated when equipment existence is verified but this verification may be done by the department itself, Inventory Control, or by electronic documents approved in the Kuali Financial System. In the case of the item on a research vessel out to sea, the department had relayed to Inventory Control that they had full knowledge of the equipment being located on the research vessel before it went to sea. Thus Inventory Control staff updated the last inventory date field based on the department’s representation on this piece of equipment.

The Inventory Control office must rely on departments and financial systems to assist in the effort to track University equipment.”

FOOD SERVICES EMPLOYEES

Background: The Associated Student Commissaries was an association of student-operated commissaries occupying UConn residences that was formed to provide central administrative services for the member commissaries. It operated as an activity fund established under the authority of Section 4-53 of the General Statutes, in accordance with procedures established by the Comptroller.

In 1979, the Connecticut State Board of Labor Relations was asked to determine whether the employer of cooks and kitchen assistants in the member commissaries was the Associated Student Commissaries or the individual member commissaries. The Board of Labor Relations concluded that they were employed by the individual student commissaries, as the power to hire, discharge and discipline the kitchen employees, as well as to control the wages, hours, and other conditions of employment, was vested in the individual commissaries, not in the Associated Student Commissaries.

Employees of the member commissaries comprised only a portion of the UConn food service employees at that time. Employees serving in the large dining halls were state employees paid through the Comptroller.

The degree of independence and authority possessed by the member commissaries gradually eroded over time. Eventually, the smaller dining halls formerly controlled by the member commissaries closed and the Associated Student Commissaries activity fund effectively ceased operations.
Currently, students are served by several large dining halls operated by the Department of Dining Services of the Division of Student Affairs. The power to hire, discharge and discipline staff and to control the wages, hours, and other conditions of employment rests with UConn administrators. However, most of the food service operations employees staffing these large dining halls are now paid directly by UConn in a manner similar to the way the former employees of the member commissaries were compensated.

Most food service operations employees are not members of the state retirement system. Instead, they are eligible to participate in two other retirement plans, the Department of Dining Services Money Purchase Pension Plan or the University of Connecticut Department of Dining Services 403(b) Retirement Plan.

UConn filed a request for a ruling regarding the status of the Department of Dining Services pension plans on May 17, 1999. In a ruling dated February 24, 2000, the Internal Revenue Service agreed that the food service operations employees are employees of an agency or instrumentality of the state and that the plans are governmental plans.

**Criteria:**

Under Section 10a-108 of the General Statutes, the board of trustees has the authority to “employ the faculty and other personnel needed” and “fix the compensation of such personnel.” The board’s authority to fix compensation does not extend to employees in state classified service. The work done by most food service operations employees appears to be the type typically performed by employees in state classified service. Section 10a-108 does not address participation in retirement plans.

Section 3-25 of the General Statutes authorizes constituent units of the state system of higher education to pay certain claims directly, rather than through the Comptroller. However, Section 3-25 specifically excludes payments for payroll.

**Condition:**

The approximately 500 food service operations employees at UConn are generally referred to as dining services employees to distinguish them from other UConn employees. However, the Department of Dining Services is a unit of UConn and, therefore, of the state. Accordingly, the employees of UConn’s food service operation are employed by the state.

Unlike other UConn employees, they are paid directly by UConn instead of through the Comptroller. Additionally, as noted above, they participate in separate retirement plans.

We first reported this condition in a report issued July 2, 2012, almost four years ago. We recommended that UConn seek clear statutory authorization
for the direct payment of wages to its food service operations staff and for their participation in separate retirement plans. We repeated our recommendation in subsequent reports issued August 27, 2014 and July 29, 2015. UConn’s response, as included in our report issued July 29, 2015, is that it is actively investigating alternatives that will continue to meet the operational needs of Dining Services and will clarify the relationship between UConn and this workforce consistent with statutory requirements.

We appreciate that this is a difficult issue to address. However, as it is a matter of statutory compliance, we feel that UConn should make its resolution a priority.

**Effect:**

Though there are sound operational reasons for UConn’s method of compensating its food service operations employees, the legal basis for the direct payment of wages by UConn is unclear, as is the participation of these employees in separate retirement plans.

**Cause:**

UConn did not seek clear statutory authority to compensate its dining service operations employees in this manner.

**Recommendation:**

The University of Connecticut should seek clear statutory authority for the direct payment of wages to its food service operations staff and for their participation in separate retirement plans. (See Recommendation 11.)

**Agency Response:**

“In response to the Auditors’ concerns, the University is actively pursuing a solution that will continue to meet the operational needs of Dining Services and will clarify the relationship between the University and this workforce consistent with statutory requirements. UConn agrees it should be a priority”

---

**CREDIT CARDS**

**Background:**

Under the University of Connecticut MasterCard Purchasing Card Program, cardholders can pay for goods and services using a University Purchasing Card, a credit card issued by JP Morgan Chase. This is a procurement tool that provides an alternative to the standard UConn procurement processes.

**Criteria:**

Credit card purchases are not subject to the controls established for standard UConn procurement processes. Completion and approval of a monthly purchasing card log listing all purchases for each card is a key compensating control.
The cardholder signs the log, certifying that it, and by extension, the listed transactions, are consistent with UConn policies and procedures. Another staff member, designated as the record manager, then reviews and signs the report, attesting to the accuracy of the cardholder’s statement.

**Condition:**

In a report issued August 27, 2014, we noted that record managers signing off on the purchasing logs may be co-workers, subordinates, lower level staff or the cardholders themselves. We recommended that the responsibility for signing off on purchasing card logs be assigned to staff with supervisory authority over the cardholder. We repeated our recommendation in a report issued July 29, 2015. UConn responded that other controls exist, but did not explain its reluctance to require supervisory signoff on credit card purchases.

Though they can be cost effective, purchasing card programs do present a heightened risk of inappropriate procurement actions. Supervisory review of credit card usage is standard practice and an effective way to address this risk. We do not understand why UConn does not want to institute this simple and effective control.

**Effect:**

Independent review and signoff on credit card purchases can be a valuable control. However, the effectiveness of this key control is greatly reduced when the individual reviewing and approving the purchases has no authority over, or is under the authority of, the cardholder.

**Cause:**

It is unclear why UConn does not require that the responsibility for signing off on purchasing card logs be assigned to staff with supervisory authority over the cardholders.

**Recommendation:**

The University of Connecticut should require that purchasing card logs be approved by a staff member with supervisory authority over the cardholder. (See Recommendation 12.)

**Agency Response:**

“The University has established robust controls and active, oversight of the PCARD Program and the reconciliation of program transactions including a daily review of all transactions. These included the re-enforcement of the separation of duties pertaining to financial activities within the system of record.

The University will work to establish a supervisory oversight control mechanism to occur after the reconciliation process by the record manager. The existing programmatic and financial system roles will remain the same, with ultimate financial approval remaining as the responsibility of the defined fiscal officer. The University anticipates this transition to occur over the next year.”
ETHICS CERTIFICATIONS

Criteria: Per Section 4-252 of the General Statutes, entities entering into large state contracts must provide certifications, commonly referred to as ethics certifications, set forth in the statute. Furthermore, for continuing contracts, updated certifications must be submitted not later than fourteen days after the twelve-month anniversary of the most recently filed certification or updated certification. Governor M. Jodi Rell’s Executive Order 7C and Governor Dannel P. Malloy’s Executive Order 49 extended this requirement to all state contracts with value of $50,000 or more in a calendar or fiscal year.

Condition: We noted problems with obtaining required ethics certifications in a report issued August 27, 2014. Similar problems were noted during our next review; we addressed them in a report issued July 29, 2015. During the current audit, we noted four instances in which annual updated ethics certifications were not obtained for periods ranging from three months to over two years after the twelve-month anniversary of the most recently filed certification or updated certification.

Effect: With respect to these transactions, UConn did not comply with state requirements designed to encourage ethical behavior.

Cause: We were told that various unrelated administrative errors caused delays in obtaining the required certifications.

Recommendation: The University of Connecticut should obtain updated ethics certifications within fourteen days after the twelve-month anniversary of the most recently filed certification or updated certification. (See Recommendation 13.)

Agency Response: “The collection of the certifications is the responsibility of multiple departments throughout the University. The University generally complies with this requirement. Due to the variableness of the terms of these relationships, relative to the annual renewal requirement, it is reasonable to assume that a relative nominal number of omissions will occur. Every effort is made to comply with the requirements. In an effort to assure compliance and to address the variability of renewals, the University is exploring an annual, systemic renewal effort regardless of the expiration term.”

OUTPATIENT PAVILION

Background: Section 10a-109e subsection (f) of the General Statues provides that “The University of Connecticut Health Center shall…(2) provide for
Auditors of Public Accounts

construction of a new ambulatory care center through debt or equity financing obtained from one or more private developers who contract with the university to construct such new ambulatory care center.” It appears the legislature intended that this project be pursued as a public-private partnership. Typically, a public-private partnership involves the assumption of a significant degree of risk by the private partner. Additionally, it can provide the public partner with off-balance-sheet financing.

Criteria: In its Guidelines for Public Debt Management, the International Monetary Fund clearly articulates the main objective of public debt management. It is to ensure that the government's financing needs and its payment obligations are met at the lowest possible cost over the medium to long term, consistent with a prudent degree of risk.

Condition: UConn determined that it was not feasible to fund the ambulatory care center project through debt or equity financing obtained from one or more private developers, as directed by the legislature. Accordingly, in December 2012, UConn, acting through the University of Connecticut Health Center Finance Corporation, secured a $203,000,000 loan from TIAA-CREF to fund the project. The TIAA-CREF loan bears interest at a rate of 4.809 percent. Interest payments over the life of the loan will total $158,595,860. In December 2012, UConn issued special revenue refunding bonds with a total interest cost of 2.480 percent. If the TIAA-CREF loan bore the same interest rate, interest payments over the life of the loan would total $81,787,842, or $76,808,018 less.

To provide the lender, TIAA-CREF, with assurance regarding the collectability of this loan, UConn asked the Attorney General to “confirm that: (i) the financial obligations of the Health Center under the Lease are not subject to appropriation risk; and (ii) in the extraordinary unlikely event that the Health Center were to default on its Lease obligations, these obligations would become general, unrestricted legal obligations of the State of Connecticut and unrelated to any appropriation to the Health Center.” The Attorney General concluded that “(1) although in the normal course required payments under the Lease will be made from available Health Center funds, the Lease payment obligations of the Health Center create legal obligations to the State of Connecticut; and (2) as a legal obligation of the State of Connecticut, required payments under the Lease are not subject to the risk of legislative non-appropriation for the Lease payments. Rather, like any claim against the State, a claim against the Health Center could proceed as provided by law.”

Effect: This transaction will burden the state with significant unnecessary interest costs. As the Attorney General has determined, the promissory note is a general obligation of the state. In practice, it exposes the state to the same
level of risk as would a standard bond issuance, but at a far higher interest cost.

Also, UConn Health is subsidized from the state’s General Fund. Any profit or loss related to ancillary operations of UConn Health, such as the ambulatory care center, will affect the amount that must be provided from the General Fund. Therefore, excessive costs incurred by ancillary operations of UConn Health will, in the end, be borne by the state.

Additionally, issuing general obligation debt instruments may fall within the broad powers granted the University of Connecticut Health Center Finance Corporation by Section 10a-254 of the General Statutes. However, in addition to the excessive interest costs involved, the propriety of issuing this promissory note without obtaining specific legislative approval seems questionable, given the existing legislative directive to proceed in a different fashion.

Cause: When it became apparent that it was not feasible to fund the ambulatory care center project through debt or equity financing obtained from one or more private developers, UConn sought an alternative financing method. UConn determined that the TIAA-CREF loan was the lowest cost alternative it had the authority to pursue. UConn sought and obtained the approval of the state’s Office of Policy and Management before it executed the promissory note.

Recommendation: The University of Connecticut should seek legislative authorization for the issuance of state bonds to refinance the TIAA-CREF loan when market conditions are appropriate. The cost savings that can be achieved will vary depending on both the state general obligation bond interest rate and, due to a yield maintenance prepayment penalty on the TIAA-CREF loan, current Treasury rates. (See Recommendation 14.)

Agency Response: “Because current state fiscal conditions have caused the Legislature to deauthorize previously approved bonding, making it highly unlikely that they would approve an additional $200 million in new authorization for this purpose, UConn has not formally requested legislative authorization for the issuance of state bonds to refinance the TIAA CREF loan. The Legislature has been informed of this recommendation through the Auditors of Public Accounts 2012 and 2013 Departmental Report. In addition, UConn has discussed the recommendation with the Governor’s Office, Office of Policy and Management and several members of the Legislative leadership. UConn agrees that it is sound policy to achieve savings whenever possible, and will further communicate to the Legislature regarding the auditor’s recommendation.”
MILEAGE LOGS

Criteria: UConn’s *Driving and Motor Vehicle Policy*, revised August 22, 2012, incorporates Department of Administrative Services General Letter 115 by reference. Per UConn’s Office of the General Counsel, staff is required to comply with the requirements of General Letter 115 as it is specifically referenced in the policy. General Letter 115, revised April 2012, requires that daily mileage logs be kept for all state-owned vehicles to record where the vehicle was driven.

Condition: We found that UConn’s Transportation Services department does not require daily mileage logs for UConn vehicles. While this is not a problem with respect to utility vehicles used solely on campus, it is a potential issue with respect to vehicles that are used for off-campus travel.

Effect: This control procedure is designed to help prevent the inappropriate personal use of state-owned vehicles. Without it, the possibility that such inappropriate personal use could take place is increased.

Cause: There appeared to be confusion on the part of UConn’s Transportation Services department as to the applicability of General Letter 115 to UConn.

Recommendation: The University of Connecticut should maintain daily mileage logs for all vehicles that are used for off campus travel. (See Recommendation 15.)

Agency Response: “This year, Transportation Services launched a pilot program utilizing Verizon Networkfleet as a fleet management solution for UConn vehicles. Verizon Networkfleet monitors real time GPS tracking, mileage reporting, and driver information. UConn Transportation Services is transitioning to Networkfleet tracking in all vehicles regularly operated outside of the Storrs campus, including the university’s regional campuses and vehicles on university business travel. Verizon Networkfleet tracking will not be required in university utility/service vehicles. This program will provide the necessary control procedure to help prevent the inappropriate personal use of state-owned vehicles.”
RECOMMENDATIONS

Status of Prior Audit Recommendations:

In our previous report on the audit examination of the University of Connecticut, we presented 11 recommendations pertaining to university operations. The following is a summary of those recommendations and the actions taken thereon:

- Seek legislative authorization for the issuance of state bonds to refinance the TIAA-CREF loan when market conditions are appropriate. This recommendation has been repeated. (See Recommendation 14.)

- Make business continuity and disaster recovery planning a priority. UConn conducted a successful disaster recovery test and continues to make business continuity and disaster recovery a priority. This recommendation is not being repeated.

- Ensure that computer hard drives are securely erased by experienced personnel after they are transferred to Central Stores. UConn has implemented this recommendation.

- Do not pay performance bonuses without first developing a structured plan with criteria for determining when bonuses should be awarded and the amounts to be paid. There were no bonus payments during the current audit. This recommendation is not being repeated.

- Seek clear statutory authority for the direct payment of wages to food service operations staff and for their participation in separate retirement plans. This recommendation is being repeated. (See Recommendation 11.)

- Track voluntary uncommitted cost sharing in the time and effort reporting system. UConn has not been able to identify a cost effective means of complying with our recommendation. This recommendation is not being repeated.

- Require supervisory approval of purchasing card logs. This recommendation is being repeated. (See Recommendation 12.)

- Comply with the competitive procurement requirements of Section 10a-151b of the General Statutes. This recommendation is being repeated. (See Recommendation 3.)

- Prepare receiving reports when advance payment is required. This issue was not noted during the current audit. This recommendation is not being repeated.
Comply with the applicable General Statutes and executive orders of Governor M. Jodi Rell regarding ethics certifications. This recommendation is being restated and repeated. (See Recommendation 13.)

Ensure that daily field reports always identify who conducted the review and prepared the report and formally approve project coordination meeting minutes. This issue was not noted during the current audit. This recommendation is not being repeated.

Current Audit Recommendations:

1. **The University of Connecticut should promptly report as required under Section 4-33a of the General Statutes as soon as a reasonable suspicion exists that a reportable incident has occurred. Any doubt as to whether an incident is reportable under Section 4-33a should be resolved by reporting it.**

Comment:

Faculty with interests in a privately-held company initiated the sole source purchase of equipment costing $253,500 from the company. These transactions appear to have violated state statutory and federal regulatory requirements. Though UConn administrators were aware of the specifics of the incident, they failed to notify APA as required under Section 4-33a.

2. **The University of Connecticut should move ongoing projects that are not consistent with the statutory definition of deferred maintenance to different funding sources. Legislative authorization should be sought for projects that do not constitute deferred maintenance and are not otherwise named in Section 10a-109e of the General Statutes.**

Comment:

Maintenance excludes activities aimed at expanding the capacity of an asset or otherwise upgrading it to serve needs different from, or significantly greater than, those originally intended. We reviewed requests for project approval submitted to the University of Connecticut Board of Trustees in connection with 20 of the larger recent deferred maintenance projects. We noted that the primary objective of 10 of the 20 projects was to expand the capacity of, or otherwise upgrade, assets rather than maintain assets. Section 10a-109ee of the General Statutes requires UConn to “provide that all funds allocated to UConn 2000...for the purpose of deferred maintenance...be expended for such purpose.”

3. **The University of Connecticut should comply with the competitive procurement requirements of Section 10a-151b of the General Statutes. Procurement actions should not be characterized as sole source purchases unless no other source exists that is capable of meeting the requirements.**
Comment:

In our test of selected expenditures for the 2015 fiscal year, we noted three that had been misclassified as sole source procurements. Documentation on file indicated that the selected vendors were chosen after a limited review of alternatives. If these procurement actions had truly been sole source procurements, there would not have been any alternatives to review. Though there was a limited review of alternatives, the procedures followed did not meet the requirements of Section 10a-151b of the General Statutes. UConn did not begin the process by soliciting competitive proposals or bids by public notice, a procedure that is critical to an open, competitive procurement process.

4. The University of Connecticut should clearly state in any separation agreements incorporating non-disparagement clauses that the clause does not in any way restrict the employee’s right to file a whistleblower complaint under Section 4-61dd of the General Statutes. The agreement should incorporate similar language addressing other actions that are protected by state or federal law or are in the public interest.

Comment:

Restrictions such as non-disparagement clauses can have a chilling effect on the willingness of employees to report inappropriate activity. This is a serious concern, as evidenced by recent actions taken by federal agencies. Though a number of separation agreements we reviewed incorporated non-disparagement clauses, UConn did not include carve-outs for complaints filed under Section 4-61dd of the General Statutes.

5. The University of Connecticut should compensate employees who step down from management positions at a level consistent with the work they are performing, not at a level appropriate for their former positions.

Comment:

A UConn administrator stayed on the UConn payroll, with no reduction in his $202,829 salary, for a year after stepping down from his management position, during which period the employee was expected to work primarily off-site. The employee’s compensation was not justified by the amount of work our review indicated was performed; it may have been intended to reward the employee for stepping down voluntarily.

6. The University of Connecticut should follow its policy regarding vacation payout upon separation. The university should attempt to recover the unauthorized payment of $45,230.

Comment:

UConn’s policy clearly provides that, irrespective of the amount accrued, payments to managerial and confidential exempt and non-represented faculty for unused vacation accruals upon separation will be limited to a maximum of 60 days. We found that one
managerial employee was paid $90,461 for 120 days of unused accrued vacation balance, twice the maximum allowable amount.

7. The University of Connecticut should provide notice instead of making separation payments to terminating employees in instances of involuntary separation for reasons unrelated to job performance.

Comment:

We noted five instances in which UConn elected to pay separation payments to managerial employees involuntarily separated for reasons unrelated to their job performance instead of providing notice. We calculated that, based on the periods of leave with pay and the employees’ rates of pay, the payments to the five employees during the periods of leave with pay aggregated $337,455. Unless the relationship with an employee has deteriorated to the point that the employee’s continued presence on site would be a detriment, offering notice is the fiscally prudent alternative. Because the same cost will be incurred either way, any services the employee is able to provide will be a net benefit to UConn.

8. The University of Connecticut should ensure that properly approved access control forms are on file for all individuals with access to KFS. Notification procedures intended to identify all individuals whose access should be disabled should be expanded to encompass all relevant personnel actions.

Comment:

We reviewed 64 employees with access to Kuali Financial System (KFS), UConn’s financial system. Approved access control forms were not on file for 11 (17 percent) of the 64. We also reviewed 226 current or former employees whose access to KFS should have been completely disabled. We found that 11 (5 percent) of the 226 still had full or partial access to the system.

9. The University of Connecticut should develop a centralized process for monitoring and obtaining assurance over service organizations.

Comment:

UConn utilizes service organizations to perform various operations. We noted several instances in which SOC reports were available, but were not obtained and reviewed. The lack of due diligence for prospective service organizations and governance oversight of current service organizations may put UConn at risk.

10. The University of Connecticut should enforce the existing procedural requirement that those responsible for equipment items enter all movements of equipment in the financial system’s capital asset management module. The last inventory date field should only be updated when the existence and location of the equipment item has been physically verified.
Comment:

During our annual physical inventory, we found 21 out of 74 tangible capital equipment items selected for testing (28 percent) at a different location than that shown in the inventory records. Furthermore, we noted that changing certain location attributes of an asset in the financial system’s capital asset management module will update the last inventory date field – giving the incorrect impression that the existence and location of the equipment item has been physically verified. This condition affected at least two of the equipment items in our selection.

11. The University of Connecticut should seek clear statutory authority for the direct payment of wages to food service operations staff and for their participation in separate retirement plans.

Comment:

Section 3-25 of the General Statutes authorizes constituent units of the state system of higher education to pay certain claims directly, rather than through the Comptroller. However, Section 3-25 specifically excludes payments for payroll. Unlike other UConn employees, food service operations employees are paid directly by UConn instead of through the Comptroller. They also participate in separate retirement plans, although there is no clear statutory authority for this. This condition, first reported in a report issued July 2, 2012, was repeated in subsequent reports issued August 27, 2014 and July 29, 2015. UConn’s response, as included in our report issued July 29, 2015, is that it is actively investigating alternatives that will continue to meet the operational needs of Dining Services and will clarify the relationship between UConn and this workforce consistent with statutory requirements.

12. The University of Connecticut should require that purchasing card logs be approved by a staff member with supervisory authority over the cardholder.

Comment:

We recommended supervisory approval of purchasing card logs in a report issued August 27, 2014. We repeated our recommendation in a report issued July 29, 2015. Though they can be cost effective, purchasing card programs do present a heightened risk of inappropriate procurement actions. Supervisory review of credit card usage is standard practice and an effective way to address this risk.

13. The University of Connecticut should obtain updated ethics certifications within fourteen days after the twelve-month anniversary of the most recently filed certification or updated certification.
Auditors of Public Accounts

Comment:

We noted problems with obtaining required ethics certifications in a report issued August 27, 2014. Similar problems were noted during our next review; we addressed them in a report issued July 29, 2015. During the current audit, we noted four instances in which annual updated ethics certifications were not obtained for periods ranging from three months to over two years after the twelve-month anniversary of the most recently filed certification or updated certification.

14. The University of Connecticut should seek legislative authorization for the issuance of state bonds to refinance the TIAA-CREF loan when market conditions are appropriate. The cost savings that can be achieved will vary depending on both the state general obligation bond interest rate and, due to a yield maintenance prepayment penalty on the TIAA-CREF loan, current Treasury rates.

Comment:

In December 2012, UConn, acting through the University of Connecticut Health Center Finance Corporation, secured a $203,000,000 loan from TIAA-CREF. The TIAA-CREF loan bears interest at a rate of 4.809 percent. Interest payments over the life of the loan will total $158,595,860. In December 2012, UConn issued special revenue refunding bonds with a total interest cost of 2.480 percent. If the TIAA-CREF loan bore the same interest rate, interest payments over the life of the loan would total $81,787,842, or $76,808,018 less. The TIAA-CREF loan is a debt instrument that the Attorney General has determined is a general obligation of the state, but bears a far higher interest rate than the state could have obtained through a standard bond issuance.

15. The University of Connecticut should maintain daily mileage logs for all vehicles that are used for off-campus travel.

Comment:

We found that UConn’s Transportation Services department does not require daily mileage logs for UConn vehicles. While this is not a problem with respect to utility vehicles used solely on campus, it is a potential issue with respect to vehicles that are used for off-campus travel. This control procedure is designed to help prevent the inappropriate personal use of state-owned vehicles. Without it, the possibility that such inappropriate personal use could take place is increased.
CONCLUSION

We wish to express our appreciation to the staff of the University of Connecticut for the cooperation and courtesies extended to our representatives during this examination.

Natercia Freitas
Principal Auditor

Approved:

John C. Geragosian
Auditor of Public Accounts

Robert M. Ward
Auditor of Public Accounts
Joint Audit & Compliance Committee Meeting
THIS PAGE INTENTIONALLY LEFT BLANK
Minor Protection Program –
First Summer Highlights

This summer marked the first busy season for campus youth activities since the implementation of UConn’s Minor Protection Program in April. University-sponsored activities involving minors were hosted by multiple areas throughout the summer. The Minor Protection Program partnered with each of these units to provide support, assess program activities and identify ways to mitigate associated risks.

Selected accomplishments include:

- Development, design, and implementation of a central registration system to maintain current and historical records of University youth activities, track those individuals involved in activities, and validate compliance with established standards.
- Creation and execution of an online Minor Protection Training.
- Creation and launch of the Minor Protection website: [http://minorprotection.edu/](http://minorprotection.edu/)
- Development and dissemination of a series of educational guides and resources related to applicable laws, policies, and best practices.

Much has been accomplished in a short period of time, and the Minor Protection Program has plans to build upon this foundation. Many initiatives are underway including:

- Incorporating Protection of Minors provisions into Facilities Use Agreements with entities who use or lease University property to operate youth activities.
- Further developing resources and updating training materials.
- Enhancing the central registration application.
- Conducting monitoring visits.

We are proud of the progress that has already been accomplished and are confident that additional strides will be made during the next half of the year.
What is Fraud?

A common question that often comes to our office is “What is fraud?” Fraud is a deliberate deception or misrepresentation practiced in order to gain something of value that results in harm or loss to the institution. Unintentional errors, mistakes or policy violations are not necessarily fraud. Common examples of fraud include: diverting cash, supplies or equipment for personal use; requesting reimbursement for personal expenses or for expenses in excess of actual and necessary business costs; and misrepresenting education or credentials to gain employment.

Fraud is most often perpetrated by an individual with complete or inappropriate ownership of a business process, for example by someone who:

- Approves his/her own expenses, reimbursements, timecards or voids
- Has access to others’ passwords, signature stamps or workflows
- Never takes time off or allows anyone else to perform a function
- Has the ability to override and/or circumvent established internal controls
- Opens the mail, makes the deposit and applies the payment
- Creates a vendor, makes a purchase, and receives and applies the payment
- Performs a reconciliation that no one else reviews or understands

Other conditions that may enable fraud include no requirement for original documentation or receipts to substantiate a claimed business expense and a lack of a management review and approval process.

If you suspect the occurrence of fraud at the University, please contact OACE’s Reportline at 1-888-685-2637 or on the web at www.compliance-helpline.com/uconncares.jsp. Please call the Police at 486-4800 if direct theft occurs (e.g. personal items are stolen).

For more information on the University’s Policy on the Prevention and Reporting of Fraud and Fiscal Irregularities, visit: http://policy.uconn.edu/?p=6794.

Internal Controls: Policies and Procedures

An evaluation of a department’s internal controls, which are used to identify specific audit risks, is a key area of focus during the audit process. The lack of written departmental policies and procedures is the most common “red flag” indicating weak internal controls encountered by the audit staff.

Written policies and procedures illustrate that managers are aware of a department’s mission and goals and knowledgeable about the department’s financial operations.

Written procedures should include:

- A brief description of the flow of major business operations and transactions that are processed, from initiation to recording in departmental records and financial accounts.
- Staff responsibility for initiating transactions and controlling the movements of assets.
- The identification of "control points" (i.e., the safeguard functions that staff perform to minimize risk of error, theft, or loss).

Departments might use a detailed description or flowchart to describe the operation of the internal control system, identify the control procedures in place and the staff that perform relevant tasks.

Special Feature: A Word from the OACE Auditors
Smoking Policy Update

Institutions of Higher Education across the country are taking strides to curtail smoking on their campuses. UConn is one of the latest Universities to enact further measures to reduce smoking, and its adverse effects, on our Storrs and Regional campuses. Effective June 7th of this year, individuals who smoke must now do so at least 25 feet away from any campus building. The new “25 foot rule” will help prevent smoke from flowing into building windows, vents and other passage ways, ultimately promoting a healthier working and learning environment for all. The policy also reinforces that smoking is not allowed in state-owned/leased buildings, facilities and vehicles.

Several offices across the University are working together to support compliance. Facilities Operations and Building Services is in the process of planning for the relocation of ash receptacles. Planning, Architectural and Engineering Services is actively inventorying locations for signage and will be collaborating with the sign shop for installation. Additionally, other offices and student organizations will be exploring the development of smoking cessation, smoke-free initiatives and other educational programs to support the University Community.

The full policy is available at http://policy.uconn.edu/?p=1038 This policy is co-owned by the Division of Environmental, Health and Safety, Department of Human Resources and the Office of Faculty and Staff Labor Relations.

Please note UConn Health has a separate Smoke and Tobacco-Free Environment Policy in place. Visit http://health.uconn.edu/policies for more information.

OACE Word Search

- Acronym for the CT law regulating the controlled release of requested public records.
- Term used to describe an intentional or deliberate act, omission or concealment with the intent of obtaining an unauthorized benefit by deception or other unethical means.
- Acronym for the federal law affording students certain rights regarding their educational records.
- ____________ data requires the highest level of privacy.
- Any inappropriate or unsubstantiated action taken or threatened against an employee because the individual has, in good faith, made an allegation concerning the violation of state or federal law, University policy, rule or regulation, or has participated in any manner with an investigation of such allegation.
- Code of ____________ is a section of the Connecticut General Statutes that all state employees, including University employees, must observe.
- An act requiring institutions of higher education (participating in Title IV financial aid) to disclose information about crime on their campuses and in the surrounding communities.
- A ____________ of interest exists when a state employee, in the discharge of their official duties, is required to take an action that would affect a financial interest of the employee, the employee’s family member (spouse, parent, sibling, child or spouse of a child), or a business with which the employee is associated with.

Instructions:

Print this page and use the clues to the left to find and circle the words and terms hidden within the word search below. Words will appear horizontally, vertically and diagonally. They will not be spelt backwards.

For the answer key, go to http://audit.uconn.edu/2016-wordsearchanswerkey/
THIS PAGE INTENTIONALLY LEFT BLANK
Title VI of the U.S. Civil Rights Act (1964) prohibits entities such as UConn Health who receive funds from the U.S. Department of Health and Human Services (HHS) from discriminating against individuals on the basis of national origin. This prohibition includes engaging in policies or practices that have the effect of precluding or inhibiting equal access to a recipient's programs and activities for patients of limited English proficiency. Please review and familiarize yourself with the policies and procedures UConn Health has established to assure equal access and effective communication with those to whom we provide services, including Affirmative Action, Non-discrimination and Equal Opportunity, Persons with Disabilities, Interpreter Services at UConn Health, SODM Dental Clinic Manual(2015) and Reporting Compliance Concerns.

For more information, please refer to the following educational resources from the Office for Civil Rights, Effective Communication in Hospitals, Disability Resources for Effective Communication, and Limited English Proficiency (LEP) Resources for Effective Communication.

For any questions about this article, contact Margaret DeMeo, Associate Compliance Officer, x1226 or email at Demeo@uchc.edu.

Disclosure of Necessary Expenses

When a UConn Health employee presents at a conference, participates on a discussion panel, writes an article or conducts some other activity in his or her “official state capacity”, payment or reimbursement of “necessary expenses” associated with that event may be accepted. These expenses include transportation to and from the activity (coach travel), lodging (standard cost of room for the nights before, of, and immediately following the event), meals and related conference expenses. Within 30 days of receipt, employees must report the payment or reimbursement directly to the Office of State Ethics (OSE) using the online “Report of Necessary Expenses” (ETH-NE form) and instruction guide.

For questions please contact Ginny Pack, Ethics Liaison, at x1280 or pack@uchc.edu or the Office of State Ethics at (860) 263-2400.

Did You Know?

- We feature a monthly Compliance Quandary on our website which may be found at: http://audit.uconn.edu/uconn-health-quandaries/
- Previous editions of our quarterly newsletter may be found at: http://audit.uconn.edu/uconn-health-compliance-courier/
Top Ten State Code of Ethics Rules

1. **Always seek advice.**

2. In general, you may not accept gifts from a lobbyist or anyone doing business with or seeking to do business with UConn Health. There are some exceptions but they must be carefully considered.

3. Decline or return gifts that do not meet the gift exception criteria.

4. Gifts exchanged between supervisors and subordinates may be valued at no more than $99.99 per gift.

5. You may not use your state position or take official action if it results in a financial gain or loss for you, your family, or a business with which you are associated.

6. Use state time, personnel, materials or equipment only for State business.

7. You may not accept outside employment that impairs your independence of judgment or that requires you to disclose confidential information learned from your UConn Health position.

8. If you, your family or an associated business seek to enter a contract with the State, certain rules must be followed.

9. A supervisor may not hire a subordinate to work for his or her outside business; it is also impermissible for a subordinate to hire a supervisor.

10. When you leave State service, there are restrictions on where you may work and what actions you may take. Some restrictions last one year; others a lifetime.

* Adapted from the Office of State Ethics [Top Ten Ethics Rules](#).

For more information about the State Code of Ethics, refer to the [Office of Audit, Compliance and Ethics](#) or [Office of State Ethics](#) websites.

For questions or for guidance regarding a specific situation, contact Ginny Pack, UConn Health Ethics Liaison at 860-679-1280 or pack@uchc.edu. You may also contact the Office of State Ethics directly at 860-263-2400 or ethics.code@ct.gov.
SUMMARY

Following are excerpts from news articles having a risk management or compliance impact. The full article may be seen at the referenced source (some may require subscription to access). Topics for this month include the following:

- Discrimination
- Drones
- Human Resources
- Information Security

Discrimination

EEOC Enters Transgender Bathroom Debate With New Guide

*Corporate Counsel* – May 3, 2016

The Equal Employment Opportunity Commission has entered the fray in the transgender bathroom access debate that has sprung up in North Carolina and along the presidential campaign trail.

On Monday, the commission issued a new guide for employers on how Title VII of the Civil Rights Act applies to transgender people in the workplace. The document affirms the commission’s previously held views supporting transgender workers’ rights to use whichever bathroom they choose.

Citing previous EEOC rulings on transgender employees, the guide emphasizes that failing to provide transgender employees with equal access to the bathroom corresponding with their gender identity constitutes sex discrimination.

It provides clarity on two key related issues as well. One is that an employer cannot condition a worker’s right to use the bathroom they prefer on proof that they have had surgery or other medical procedures. The other is that employers cannot force a transgender worker to use a single-user bathroom, although the employer can certainly make one available to any employee, transgender or not, who wants to use it.

And according to the guidance, “gender-based stereotypes, perceptions, or comfort level” must not interfere with the ability of transgender people to be free from discrimination and harassment in the workplace.

Notably, the EEOC calls out states that have tried and succeeded in passing legislation to restrict the bathroom choices of the transgendered. “Contrary state law is not a defense under Title VII,” the guide says.

Some states have passed laws or tried to pass laws restricting transgender rights when it comes to bathroom usage and other aspects of life at work. But other states, as well as cities and other municipalities, have actually echoed the EEOC’s stance by adopting gender identity as a protected characteristic.

They may even expand on the EEOC’s coverage, says Dori Stibolt, a partner at Fox Rothschild, because while the commission only covers companies with 15 or more employees, other more local laws may apply to smaller businesses too. “There has been a real push by various human rights organizations to change laws via local activity and they’ve been very successful at it,” Stibolt says.

Experts say ensuring compliance with the EEOC guidance on restrooms shouldn’t be burdensome for companies. Anti-discrimination and anti-harassment policies should now cite the rights of transgender people, including their restroom access, says Cynthia Augello, a partner at Cullen and Dykman. “People who haven’t updated their policies in a few years probably should to include [these protections],” she says. “They should engage in training their employees so they make sure they know that this is now covered.”

Companies concerned about giving workers privacy can also add a new single-use bathroom to their facility, Augello adds. As long as transgender people aren’t forced to use this bathroom as their only option, it shouldn’t raise the ire of the EEOC.
On May 13, 2016, the U.S. Departments of Education and Justice (Departments) issued a “Dear Colleague” letter regarding transgender students. Some of the key points made in the letter include the following:

- Title IX of the Education Amendments of 1972 (Title IX) and its implementing regulations prohibit sex discrimination in educational programs and activities operated by recipients of Federal financial assistance. This prohibition encompasses discrimination based on a student’s gender identity, including discrimination based on a student’s transgender status.

- As a condition of receiving Federal funds, a school agrees that it will not exclude, separate, deny benefits to, or otherwise treat differently on the basis of sex any person in its educational programs or activities unless expressly authorized to do so under Title IX or its implementing regulations. The Departments treat a student’s gender identity as the student’s sex for purposes of Title IX and its implementing regulations. This means a school must not treat a transgender student differently from the way it treats other students of the same gender identity.

- The Departments interpret Title IX to require that when a student or the student’s parent or guardian, as appropriate, notifies the school administration that the student will assert a gender identity that differs from previous representations or records, the school will begin treating the student consistent with the student’s gender identity. Under Title IX, there is no medical diagnosis or treatment requirements that students must meet as a prerequisite to being treated consistent with their gender identity. Because transgender students often are unable to obtain identification documents that reflect their gender identity (e.g., due to restrictions imposed by state and local law in their place of birth or residence), requiring students to produce such identification documents in order to treat them consistent with their gender identity may violate Title IX when doing so has the practical effect of limiting or denying students equal access to an educational program or activity.

- A school’s Title IX obligation to ensure nondiscrimination on the basis of sex requires schools to provide transgender students equal access to educational programs and activities even in circumstances in which other students, parents, or community members raise objections or concerns. As is consistently recognized in civil rights cases, the desire to accommodate others’ discomfort cannot justify a policy that singles out and disadvantages a particular class of students.

- Schools must take reasonable steps to protect students’ privacy related to their transgender status, including their birth name or sex assigned at birth. Nonconsensual disclosure of personally identifiable information (PII), such as a student birth name or sex assigned at birth, could be harmful to or invade the privacy of transgender students and may also violate the Family Educational Rights and Privacy Act (FERPA). A school may maintain records with this information, but such records should be kept confidential.

The “Dear Colleague” Letter also addresses the following topics:

1. **Schools’ Responsibility to Provide a Safe and Nondiscriminatory Environment**

2. **Treating Students Consistent with their Gender Identity Regardless of Identification Documents; Using Gender-Identity Appropriate Names, and Pronouns**

3. **Sex-Segregated Activities and Facilities Must Accommodate Transgender Students According to their Gender Identity** – In this context the letter addresses Restroom and Locker Rooms, Athletics, Single Sex Classes, Single-Sex Schools, Social Fraternities and Sororities, Housing and Overnight Accommodations, and Other Sex-Specific Activities and Rules.

**Drones**

**FAA Clarifies Educational Use of Drones**

_Frost Brown Todd, LLC - May 9, 2016_

Until recently, schools could not allow their students to fly drones for educational purposes without going through the costly and time-consuming process of obtaining specific Federal Aviation Administration (FAA) approval. On May 4, the FAA released a memorandum clarifying the educational use of Unmanned Aircraft Systems.
The bottom line is that the following activities are now permitted under hobby or recreational guidelines (that is, no commercial use exemption, no pilot’s certificate, and no need to obtain a certificate of authorization or waiver):

1. Flights at educational institutions and community sponsored events as long as the operator is not compensated.
2. Flight by students in furtherance of aviation related education at an accredited educational institution.
3. Assistance of students by faculty teaching aviation related courses at accredited educational institutions, provided the student maintains operational control.

Bear in mind that the above operations require compliance with the existing model or recreational guidelines. That is, they must operate in accordance with community guidelines, not interfere with manned aircraft, and operators must give prior notice when within five miles of an airport.

Human Resources

What Obama’s Overtime Rule Could Mean for Colleges


This week the Obama administration released a final rule that will extend overtime pay to millions more American workers, including hundreds of thousands of lower-level salaried employees on college campuses. Much of the attention has focused on the impact on postdoctoral fellows, the overworked, underpaid backbone of the academic research enterprise.

But it’s not just postdocs who will benefit from the rule, which will double the annual salary cutoff below which workers are generally eligible for overtime pay, raising it to $47,476. Many entry-level and midlevel professionals — from admissions officers to athletic trainers to student-aid administrators — will qualify too.

That means the rule will be expensive for colleges, many of which already struggle with high labor costs. And that’s where the downside comes in: Already college groups are warning of consequences when the rule kicks in, at the start of December.

"Requiring such a dramatic and costly change to be implemented so quickly will leave many colleges with no choice but to respond to this regulation with a combination of tuition increases, service reductions, and, possibly, layoffs," Molly Corbett Broad, president of the American Council on Education, said in a written statement.

Peter McPherson, president of the Association of Public and Land-Grant Universities, wrote in a blog post published on Thursday that "there is simply no way for universities to absorb costs of this magnitude without an impact on our academic, research, and outreach missions."

Here’s what the new overtime-pay rule means for your campus:

**It’s a boon to postdocs — but not all of them.**

Postdoctoral fellows have been agitating for higher pay for years, and the National Academy of Sciences has recommended that colleges pay postdocs a starting salary of at least $50,000. This rule will compel colleges to increase their pay to at least $47,477, to avoid having to pay them overtime. (The National Institutes of Health has already announced that it will raise its own research stipend for postdocs above that threshold.)

On Thursday the National Postdoctoral Association, which represents 79,000 postdoctoral scholars, issued a statement calling the rule "a positive step towards achieving our goal of increasing compensation for postdoctoral researchers nationwide."

Yet the association also expressed disappointment that the overtime expansion leaves out researchers who primarily teach, including some in the humanities. Most salaried teachers — including adjunct instructors and graduate teaching assistants — aren’t eligible for overtime pay, under a longstanding policy that exempts them from the benefit. The postdoc association says that exception creates an unfair distinction between scientific and humanities postdoctoral studies. The group has called for a "uniform application" of the rule.
This doesn’t affect just research universities and large public institutions.

While such institutions are more likely to have large numbers of scientific postdocs, the rule’s reach extends well beyond the laboratory. In fact, the new salary threshold applies to many administrative employees, including those in admissions, financial aid, academic affairs, and athletics.

David S. Baime, senior vice president for government relations and policy analysis at the American Association of Community Colleges, said his organization’s members include 386 colleges whose business and financial-operations staff members each earn less than $47,000, on average. They employ, on average, 12 staff members each. The association includes 364 institutions where the average computer, engineering, and science salary is below the threshold, with an average staff of 10.

Private colleges, meanwhile, said the rule would undermine their efforts to rein in tuition growth. In a statement, the National Association of Independent Colleges and Universities said that "the rule will have a significant impact on campus budgets — most of which have already been set for the next fiscal year, if not the next two fiscal years."

Darron Collins, president of the tiny College of the Atlantic, in Maine, said he feared the rule could spell a "potential reduction in autonomy for employees who up until now have viewed their work as a vocation more than a job."

There’s more than one way to comply with the rule.

When President Obama first proposed raising the overtime-pay threshold to just over $50,000, last July, the College and University Professional Association for Human Resources sent a letter that warned that the new rule would force colleges to reclassify many workers to hourly status, “to the detriment of employees, institutions, and students.”

But the Labor Department, in guidance issued with the rule this week, said colleges have “numerous options for compliance.” They can raise the salaries of newly eligible employees so those salaries are above the threshold; they can pay such employees overtime, on top of their salaries; they can “reorganize workloads, adjust schedules, or spread work hours” to limit overtime pay; or they can reduce employees’ base pay so the amount they are paid, with overtime, "remains largely the same."

The guidance also notes that public colleges that qualify as "public agencies" under federal labor law may provide employees with compensatory time off in lieu of cash overtime premiums. Private colleges do not have that option.

Information Security

DoD Issues Final Rule on ‘Basic’ Safeguards for Information Systems


With an apparent nod to widespread concerns from universities and others, the Department of Defense (DoD), NASA, and the General Services Administration have issued a final rule that imposes “basic” safeguards for systems holding federal information, rather than requiring protections for certain types of the information. But universities and others should prepare for additional and perhaps stricter regulations, as the agencies said the final rule was “just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems.”

Published May 16, the rule finalized a proposed rule issued on Aug. 24, 2012, and an advance notice of proposed rulemaking released in December 2010. Under the proposed rule, contractors would have had to implement protections to safeguard systems that contain information termed “other-than-public” that was generated by or for the federal contracting agencies (RRC 10/12, p. 1).

These safeguards would include physical and electronic barriers, intrusion protections and other measures called for in a related 2011 DoD proposed rule, and would have been applied to that rule’s seven categories: “public computers or websites; transmitting electronic information; transmitting voice and fax information; physical and electronic barriers; sanitization; intrusion protection and transfer limitations” (RRC 8/11, p. 9).

Keep an Eye Out

Among the concerns expressed about the proposed rule was the lack of an exception for basic research.

With an effective date of June 15, the final regulation stems from Federal Acquisition Regulation case 2009-030 and FAR case 2011-020, Basic Safeguarding of Contractor Information Systems, which were merged in 2011.
The new regulation deletes the definition of public information and “does not focus on the protection of any specific type of information, but requires basic elements for safeguarding an information system,” according to the preamble. “These requirements should not have any chilling effect on fundamental research,” it states.

The rule, “which focuses on ensuring a basic level of safeguarding for any contractor system with Federal information, reflective of actions a prudent business person would employ, is just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems.”

Under the regulation, a “contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.”

Contractors are required to “apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:”

- “Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).”
- “Limit information system access to the types of transactions and functions that authorized users are permitted to execute.”
- “Verify and control/limit connections to and use of external information systems.”
- “Control information posted or processed on publicly accessible information systems.”
- “Identify information system users, processes acting on behalf of users, or devices.”
- “Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.”
- “Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.”
- “Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.”
- “Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.”
- “Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.”
- “Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.”
- “Identify, report, and correct information and information system flaws in a timely manner.”
- “Provide protection from malicious code at appropriate locations within organizational information systems.”
- “Update malicious code protection mechanisms when new releases are available.”
- “Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.”

The rule may have calmed some fears about expensive and complicated safeguards. But that anxiety may return as the agencies take further steps in the future, as noted.

The rule points out that in summer 2015, the Office of Management and Budget “issued proposed guidance to enhance and clarify cybersecurity protections in Federal acquisitions related to CUI [controlled unclassified information] in systems that contractors operate on behalf of the Government as well as in systems that are not operated on behalf of an agency but are used incidental to providing a product or service for an agency with particular focus on security controls, incident reporting, information system assessments, and information security continuous monitoring.”

The agencies “will be developing FAR changes to implement the OMB guidance when it is finalized,” the rule states. “In addition, we plan to develop regulatory changes for the FAR in coordination with National Archives and Records Administration (NARA) which is separately finalizing a rule to implement” Executive Order (E.O.) 13556, which deals with CUI.
“The E.O. established the CUI program to standardize the way the executive branch handles information (other than classified information) that requires safeguarding or dissemination controls,” the rule explains. The agencies offered no timeline as to when final guidance and the other rules would be forthcoming.

DoJ Issues Supplemental Advance Notice of Proposed Rulemaking on Accessibility of Web Information and Services of State and Local Government Entities

Supplemental advance notice of proposed rulemaking on the accessibility of web in formation and services of state and local government entities was published by the U.S. Department of Justice. The Department is considering revising the regulations implementing Title II of the Americans with Disabilities Act (ADA) to establish specific technical requirements that would make the services, programs, and activities that state and local governments offer to the public via the internet accessible to those with disabilities. The Department is considering proposing WCAG 2.0 Level AA as the accessibility standard that would apply to Web sites and Web content of title II entities. This supplemental advance notice was released to solicit additional public comments on various issues relating to the potential application of such technical requirements to the websites sites of Title II entities and to gather information for preparing a regulatory impact analysis. The Department also issued a statement announcing the supplemental notice. Comments must be submitted on or before ninety days after the date of publication.
SUMMARY

Following are excerpts from news articles having a risk management or compliance impact. The full article may be seen at the referenced source (some may require subscription to access). Topics for this month include the following:

- CMS Regulations
- Connecticut Law
- Discrimination
- Human Resources
- Information Security
- Information Technology
- MACRA

Connecticut Law

Connecticut Legislature Passes Non-Compete Act Concerning Contracts with Physicians

Shipman & Goodwin – May 24, 2016

On May 18, 2016, the Connecticut legislature transmitted Public Act No. 16-95 (the “Act”) to the Governor for his signature. The Governor is expected to sign the bill into law in the coming weeks. Once he does, it will become effective as of July 1, 2016. The Act, among other things, codifies rules relating to non-competition agreements with physicians, which differ from the rule of reason analysis applicable to such agreements in the past. Hospitals and physician practices should take note of these new standards, which affect non-competition agreements entered into both before and after the Act’s July 1 effective date.

The Act defines a “covenant not to compete” as “any provision of an employment or other contract or agreement that creates or establishes a professional relationship with a physician and restricts the right of a physician to practice medicine in any geographic area of the state for any period of time after the termination or cessation of such partnership, employment or other professional relationship.” The Act thus applies to any non-compete entered into with a physician, whether the physician is a partner, owner, employee or independent contractor.

Currently, there are no statutory rules applicable to non-competition agreements in Connecticut. Generally, the enforceability of such an agreement in Connecticut is determined under a reasonableness analysis, by which a reviewing Court assesses whether the agreement is reasonably limited in time, geographic scope, the fairness of the protection it affords the employer, the extent of the restraint on the employee’s opportunity to pursue his or her occupation and the extent to which the agreement interferes with the public’s interest. There are no hard and fast rules concerning the length of time or geographic radius within which a covenant not to compete will be considered “reasonable” and therefore enforceable. Moreover, traditionally, in a proceeding to challenge the enforceability of a covenant not to compete, the employee bears the burden of establishing that such an agreement is not reasonable.

While covenants not to compete with a physician have traditionally been considered under this rule of reason analysis, the Act alters this standard for such agreements, both currently in existence and executed after the effective date of the Act.

The Act Flips the Burden of Establishing Enforceability of a Physician Non-Compete

The Act affirms the application of a reasonableness analysis to such agreements, but states that “[t]he party seeking to enforce a covenant not to compete shall have the burden of proof in any proceeding.” The Act thus flips the burden of proof to the hospital, employer or practice to affirmatively prove that the covenant not to compete is reasonable -- even where a suit is brought by a physician to challenge the enforceability of a non-competition agreement. This shifting of the burden of proof is applicable to all physician non-competes, not just those executed after the effective date of the Act.
The Act Restricts the Geographic and Temporal Scope of Physician Non-Competes

For agreements executed after July 1, 2016, the Act restricts both the geographic and temporal scope of any non-compete agreement with a physician. In particular, such a non-compete may not restrict a physician from competing for longer than one year and cannot extend to any more than 20 miles from the primary site where the physician practices. The “primary site where [the] physician practices” is defined in the Act as the “office, facility or location where a majority of the revenue derived from such physician’s services is generated” or “any other office, facility or location where such physician practices and mutually agreed to by the parties and identified in the covenant not to compete.”

The Act Invalidates Certain Non-Compete Agreements

Lastly, the Act states that a non-competition agreement cannot be enforced against a physician under the following two circumstances: (1) where the non-compete agreement was not made as part of or in anticipation of a partnership or ownership agreement and the professional services or employment agreement containing the non-compete expires and is not renewed; or (2) the employment or professional services agreement is terminated without cause. Again, the Act significantly alters the rules applicable to physician non-competition agreements by rendering certain classes of those agreements unenforceable, regardless of the reasonableness of the restrictions.

Recommendations

We strongly encourage hospitals and physician groups to familiarize themselves with the changes to the law governing physician non-competes and review standard or template non-competition covenants contained in employment, professional services, partnership or ownership agreements to ensure compliance with Public Act No. 16-95, including without limitation a review of the temporal and geographic scope of such non-competition covenants. Hospitals and physician groups are also encouraged to consider expressly identifying office facilities or locations in which a physician practices in physician non-competes going forward and to consider the consequences of terminating any physician who is subject to a non-competition agreement without cause.

Discrimination

EEOC Enters Transgender Bathroom Debate With New Guide

Corporate Counsel— May 3, 2016

The Equal Employment Opportunity Commission has entered the fray in the transgender bathroom access debate that has sprung up in North Carolina and along the presidential campaign trail.

On Monday, the commission issued a new guide for employers on how Title VII of the Civil Rights Act applies to transgender people in the workplace. The document affirms the commission’s previously held views supporting transgender workers’ rights to use whichever bathroom they choose.

Citing previous EEOC rulings on transgender employees, the guide emphasizes that failing to provide transgender employees with equal access to the bathroom corresponding with their gender identity constitutes sex discrimination.

It provides clarity on two key related issues as well. One is that an employer cannot condition a worker’s right to use the bathroom they prefer on proof that they have had surgery or other medical procedures. The other is that employers cannot force a transgender worker to use a single-user bathroom, although the employer can certainly make one available to any employee, transgender or not, who wants to use it.

And according to the guidance, “gender-based stereotypes, perceptions, or comfort level” must not interfere with the ability of transgender people to be free from discrimination and harassment in the workplace.

Notably, the EEOC calls out states that have tried and succeeded in passing legislation to restrict the bathroom choices of the transgendered. “Contrary state law is not a defense under Title VII,” the guide says.

Some states have passed laws or tried to pass laws restricting transgender rights when it comes to bathroom usage and other aspects of life at work. But other states, as well as cities and other municipalities, have actually echoed the EEOC’s stance by adopting gender identity as a protected characteristic.
They may even expand on the EEOC’s coverage, says Dori Stibolt, a partner at Fox Rothschild, because while the commission only covers companies with 15 or more employees, other more local laws may apply to smaller businesses too. “There has been a real push by various human rights organizations to change laws via local activity and they’ve been very successful at it,” Stibolt says.

Experts say ensuring compliance with the EEOC guidance on restrooms shouldn’t be burdensome for companies. Anti-discrimination and anti-harassment policies should now cite the rights of transgender people, including their restroom access, says Cynthia Augello, a partner at Cullen and Dykman. “People who haven’t updated their policies in a few years probably should to include [these protections],” she says. “They should engage in training their employees so they make sure they know that this is now covered.”

Companies concerned about giving workers privacy can also add a new single-use bathroom to their facility, Augello adds. As long as transgender people aren’t forced to use this bathroom as their only option, it shouldn’t raise the ire of the EEOC.

Gender Identity & Sexual Orientation Discrimination; Title IX


Dear Colleague:

Schools across the country strive to create and sustain inclusive, supportive, safe, and nondiscriminatory communities for all students. In recent years, we have received an increasing number of questions from parents, teachers, principals, and school superintendents about civil rights protections for transgender students. Title IX of the Education Amendments of 1972 (Title IX) and its implementing regulations prohibit sex discrimination in educational programs and activities operated by recipients of Federal financial assistance. This prohibition encompasses discrimination based on a student’s gender identity, including discrimination based on a student’s transgender status. This letter summarizes a school’s Title IX obligation regarding transgender students and explains how the U.S. Department of Education (ED) and the U.S. Department of Justice (DOJ) evaluate a school’s compliance with these obligations.

ED and DOJ (the Departments) have determined that this letter is significant guidance. This guidance does not add requirements to applicable law, but provides information and examples to inform recipients about how the Departments evaluate whether covered entities are complying with their legal obligations. If you have questions or are interested in commenting on this guidance, please contact ED at ocr@ed.gov or 800-421-3481 (TDD 800-877-8339); or DOJ at education@usdoj.gov or 877-292-3804 (TTY: 800-514-0383).

Accompanying this letter is a separate document from ED’s Office of Elementary and Secondary Education, Examples of Policies and Emerging Practices for Supporting Transgender Students. The examples in that document are taken from policies that school districts, state education agencies, and high school athletics associations around the country have adopted to help ensure that transgender students enjoy a supportive and nondiscriminatory school environment. Schools are encouraged to consult that document for practical ways to meet Title IX’s requirements.

Terminology

- Gender identity refers to an individual’s internal sense of gender. A person’s gender identity may be different from or the same as the person’s sex assigned at birth.

- Sex assigned at birth refers to the sex designation recorded on an infant’s birth certificate should such a record be provided at birth.

- Transgender describes those individuals whose gender identity is different from the sex they were assigned at birth. A transgender male is someone who identifies as male but was assigned the sex of female at birth; a transgender female is someone who identifies as female but was assigned the sex of male at birth.

- Gender transition refers to the process in which transgender individuals begin asserting the sex that corresponds to their gender identity instead of the sex they were assigned at birth. During gender transition, individuals begin to live and identify as the sex consistent with their gender identity and may dress differently, adopt a new name, and use pronouns consistent with their gender identity. Transgender individuals may undergo gender transition at any stage of their lives, and gender transition can happen swiftly or over a longer duration of time.
Compliance with Title IX

As a condition of receiving Federal funds, a school agrees that it will not exclude, separate, deny benefits to, or otherwise treat differently on the basis of sex any person in its educational programs or activities unless expressly authorized to do so under Title IX or its implementing regulations. The Departments treat a student’s gender identity as the student’s sex for purposes of Title IX and its implementing regulations. This means a school must not treat a transgender student differently from the way it treats other students of the same gender identity. The Departments’ interpretation is consistent with courts’ and other agencies’ interpretations of Federal laws prohibiting sex discrimination.

The Department interpret Title IX to require that when a student or the student’s parent or guardian, as appropriate, notifies the school administration that the student will assert a gender identity that differs from previous representations or records, the school will begin treating the student consistent with the student’s gender identity. Under Title IX, there is no medical diagnosis or treatment requirements that students must meet as a prerequisite to being treated consistent with their gender identity. Because transgender students often are unable to obtain identification documents that reflect their gender identity (e.g., due to restrictions imposed by state and local law in their place of birth or residence), requiring students to produce such identification documents in order to treat them consistent with their gender identity may violate Title IX when doing so has the practical effect of limiting or denying students equal access to an educational program or activity.

A school’s Title IX obligation to ensure nondiscrimination on the basis of sex requires schools to provide transgender students equal access to educational programs and activities even in circumstances in which other students, parents, or community members raise objections or concerns. As is consistently recognized in civil rights cases, the desire to accommodate others’ discomfort cannot justify a policy that singles out and disadvantages a particular class of students.

1. Safe and Nondiscriminatory Environment

Schools have a responsibility to provide a safe and nondiscriminatory environment for all students, including transgender students. Harassment that targets a student based on gender identity, transgender status, or gender transition is harassment based on sex, and the Departments enforce Title IX accordingly. If sex-based harassment creates a hostile environment, the school must take prompt and effective steps to end the harassment, prevent its recurrence, and, as appropriate, remedy its effects. A school’s failure to treat students consistent with their gender identity may create or contribute to a hostile environment in violation of Title IX. For a more detailed discussion of Title IX requirements related to sex-based harassment, see guidance documents from ED’s Office of Civil Rights (OCR) that are specific to this topic.

2. Identification Documents, Names, and Pronouns

Under Title IX, a school must treat students consistent with their gender identity even if their education records or identification documents indicate a different sex. The Departments have resolved Title IX investigations with agreements committing that school staff and contractors will use pronouns and names consistent with a transgender student’s gender identity.

3. Sex-Segregated Activities and Facilities

Title IX’s implementing regulations permit a school to provide sex-segregated restrooms, locker rooms, shower facilities, housing, and athletic teams, as well as single-sex classes under certain circumstances. When school provides sex-segregated activities and facilities, transgender students must be allowed to participate in such activities and access such facilities consistent with their gender identity.

- **Restroom and Locker Rooms.** A school may provide separate facilities on the basis of sex, but must allow transgender students access to such facilities consistent with their gender identity. A school may not require transgender students to use facilities inconsistent with their gender identity or to use individual-user facilities when other students are not required to do so. A school may, however, make individual-user options available to all students who voluntarily seek additional privacy.

- **Athletics.** Title IX regulations permit a school to operate or sponsor sex-segregated athletics teams when selection for such teams is based on competitive skill or when the activity involved is a contact sport. A school may not, however, adopt or adhere to requirements that rely on overly broad generalizations or
stereotypes about the differences between transgender students and other students of the same sex (i.e., the same gender identity) or others’ discomfort with transgender students. Title IX does not prohibit age-appropriate, tailored requirements based on sound, current, and research-based medical knowledge about the impact of the students’ participation on the competitive fairness or physical safety of the sport.

- **Single Sex Classes.** Although separating students by sex in classes and activities is generally prohibited, nonvocational elementary and secondary schools may offer nonvocational single-sex classes and extracurricular activities under certain circumstances. When offering such classes and activities, a school must allow transgender students to participate consistent with their gender identity.

- **Single-Sex Schools.** Title IX does not apply to the admissions policies of certain educational institutions, including nonvocational elementary and secondary schools, and private undergraduate colleges. Those schools are therefore permitted under Title IX to set their own sex-based admissions policies. Nothing in Title IX prohibits a private undergraduate women’s college from admitting transgender women it is so chooses.

- **Social Fraternities and Sororities.** Title IX does not apply to the membership practices of social fraternities and sororities. Those organizations are therefore permitted under Title IX to set their own policies regarding the sex, including gender identity, of their members. Nothing in Title IX prohibits a fraternity from admitting transgender men or a sorority from admitting transgender women if it so chooses.

- **Housing and Overnight Accommodations.** Title IX allows a school to provide separate housing on the basis of sex. But a school must allow transgender students to access housing consistent with their gender identity and may not require transgender student to stay in single-occupancy accommodations or to disclose personal information when not required of their students. Nothing in Title IX prohibits a school from honoring a student’s voluntary request for single occupancy accommodations if it so chooses.

- **Other Sex-Specific Activities and Rules.** Unless authorized by Title IX or its implementing regulations, a school may not segregate or otherwise distinguish students on the basis of their sex, including gender identity, in any school activities or the application of any school rule. Likewise, a school may not discipline students or exclude them from participating in activities for appearing or behaving in a manner that is consistent with their gender identity or that does not conform to stereotypical notions of masculinity or femininity (e.g., in yearbook photographs, at school dances, or at graduation ceremonies).

4. **Privacy and Education Records**

Protecting transgender students’ privacy is critical to ensuring they are treated consistent with their gender identity. The Departments may find a Title IX violation when a school limits students’ educational rights or opportunities by failing to take reasonable steps to protect students’ privacy related to their transgender status, including their birth name or sex assigned at birth. Nonconsensual disclosure of personally identifiable information (PII), such as a student birth name or sex assigned at birth, could be harmful to or invade the privacy of transgender students and may also violate the Family Educational Rights and Privacy Act (FERPA). A school may maintain records with this information, but such records should be kept confidential.

- **Disclosure of Personally Identifiable Information from Education Records.** FERPA generally prevents the nonconsensual disclosure of PII from a student’s education record; one exception is that records may be disclosed to individual school personnel who have been determined to have a legitimate educational interest in information. Even when a student has disclosed the student’s transgender status to some members of the school community, schools may not rely on this FERPA exception to disclose PII from education records to other school personnel who do not have a legitimate educational interest in the information. Inappropriately disclosing (or requiring students or their parents to disclose) PII from education records to the school community may violate FERPA and interfere with transgender students’ right under Title IX to be treated consistent with their gender identity.

- **Amendment or Correction of Education Records.** A school may receive requests to correct a student’s education records to make them consistent with the student’s gender identity. Updating a transgender student’s education records to reflect the student’s gender identity and new name will help protect privacy and ensure personnel consistently use appropriate names and pronouns.
Under FERPA, a school must consider the request of an eligible student or parent to amend information in the student's education records that is inaccurate, misleading, or in violation of the student’s privacy rights. If the school does not amend the record, it must inform the requestor of its decision and of the right to a hearing. If, after the hearing, the school does not amend the record, it must inform the requester of the right to insert a statement in the record with the requestor’s comments on the contested information, a statement that the requestor disagrees with the hearing decision, or both. That statement must be disclosed whenever the record to which the statement relates is disclosed.

Under Title IX, a school must respond to a request to amend information related to a student’s transgender status consistent with its general practices for amending other students’ records. If a student or parent complains about the school’s handling of such a request, the school must promptly and equitably resolve the complaint under the school’s Title IX grievance procedures.

We appreciate the work that many schools, state agencies, and other organizations have undertaken to make educational programs and activities welcoming, safe, and inclusive for all students.

CMS Regulations

CMS Releases Proposed Rule for MACRA Implementation – Overview and Merit-Based Incentive Payment Systems (MIPS)


On April 27, 2016, the Centers for Medicare and Medicaid Services (CMS) released a proposed rule that would put in place key parts of the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA). MACRA impacts a number of laws and government initiatives that have been implemented over the past two decades affecting physician reimbursement, and in doing so, will fundamentally change the way that Medicare reimburses physicians.

The MACRA Proposed Rule contains two key initiatives: Merit-Based Incentive Payment Systems (MIPS), which partially repeals the meaningful use program for electronic health records, and alternative payment models (APMs).

BACKGROUND AND OVERVIEW

Elimination of the Sustainable Growth Rate

One of MACRA’s most notable features is its elimination of the Sustainable Growth Rate (SGR) formula which was introduced in 1997 in an attempt to rein in the skyrocketing costs of physician services. Under the SGR, Medicare payments for physician services were supposed to be adjusted annually based in part on changes in the United States gross domestic product. Over the past several years, application of the SGR formula would have resulted in annual decreases to physician payments were it not for recurring legislative “patches” that implemented temporary delays in the application of the SGR formula. MACRA permanently repeals the SGR formula and replaces it with modest increases in Medicare physician fees. The additional cost to Medicare resulting from the repeal of the SGR is to be offset in part by the increased reliance on APMs and on the implementation of other cost-saving measures.

The Current Physician Reimbursement System

Physician services furnished to Medicare beneficiaries are generally reimbursed on the basis of the lesser of actual charges or the amount determined under the Medicare Physician Fee Schedule. Currently and through 2018, physician reimbursement under this system depends on the physician’s participation in, and performance under, three separate programs: (1) the Physician Quality Reporting System (PQRS), under which eligible physicians who do not satisfactorily report required quality measure data are subject to a reduction in their Medicare fees; (2) the Medicare Electronic Health Record (EHR) Incentive Program (also known as the “meaningful use” program), under which physicians who fail to achieve meaningful use of EHR systems will incur a reduction in their Medicare fees and (3) the Value-based Modifier Program, which provides incentive payments to physicians based on the quality of care they furnish compared to their cost of care during a performance period.
CHANGES UNDER MACRA — MIPS

Under MACRA, starting in 2019, CMS will replace the three programs mentioned above with a two track system under which physicians will be reimbursed either: (1) on a fee-for-service basis with enhanced incentives under the Merit-Based Incentive Payment Systems (MIPS); or (2) through participation in APMs.

Under MIPS, eligible physicians will be rewarded or penalized based on the quality of the care they provide during a performance year. The amount of the reward or penalty will be based on a composite score using the physician’s performance in the following four categories:

1. Clinical quality (50% of total score in year 1)
2. Resource utilization (10% of total score in year 1)
3. Clinical practice improvement activity (15% of total score in year 1)
4. Advanced care information (formally known as “meaningful use”) (25% of total score in year 1). (Because of the importance of the changes to the meaningful use program, we will discuss these changes in a subsequent blog post.)

The MIPS program will involve positive or negative payment adjustments to the Medicare Physician Fee Schedule (“PFS”) payments. MIPS payments under this program are a zero sum game because of MACRA’s required budget neutrality. This means that the money CMS saves from the negative adjustments will be used to fund the positive adjustments. Additionally, from 2019 through 2024, the best performing physicians will be eligible for an additional bonus payment of up to 10% allocated from a $500 million pool.

Physicians scoring below a certain threshold will incur a negative adjustment in their payments starting with a maximum penalty of 4% in 2019 and increasing to a maximum penalty of 9% in 2022 and beyond. Physicians scoring above the threshold in a given year will incur a positive adjustment on a sliding scale, with the maximum bonus payment equal to three times the aggregate penalty cap for that year. Those physicians who meet the threshold will receive no payment adjustment.

The proposal provides for a MIPS performance period of 1 calendar year for all measures and activities applicable to the four performance categories discussed above. CMS proposes to use 2017, i.e., next year, as the performance period for the 2019 payment adjustments, meaning that payments in 2019 would be based on the clinician’s performance in 2017. The quality measures would be selected annually through a call for quality measures process, with a final list of quality measures published in the Federal Register by November 1st of each year.

As an alternative, physicians who have a significant Medicare population can opt-out of MIPS and instead participate in what the proposed rule refers to as “Advanced APMs,” such as accountable care organizations (ACOs) and patient-centered medical homes (PCMHs). The APM portion of the MACRA proposed rule will be discussed in an upcoming blog post.

Human Resources

New Federal Overtime Rule Could Have Significant Impact on Higher Education

American Council on Education — May 18, 2016

The Department of Labor (DOL) released its final rule on overtime pay today, establishing a new threshold of $47,476 a year for those working more than 40 hours a week to be eligible for overtime compensation, roughly double the current threshold of $23,660.

The rule goes into effect Dec. 1.

According to DOL, the higher income limit will make 4.2 million salaried workers newly eligible for overtime pay. The new level will be adjusted every three years to reflect changes in the cost of living.
DOL released its proposed rule in July 2015, after being charged by President Obama in 2014 with revising the regulations governing exemptions to the Fair Labor Standards Act’s overtime pay requirements for executive, administrative and professional employees.

ACE and a number of higher education associations submitted comments on the proposal, outlining a range of problems the higher education community had with the draft. None of these problems appear to have been addressed in the final rule.

ACE President Molly Corbett Broad expressed concern about how the rule will impact colleges and universities, which are among the primary employers in many communities.

“While in principle we support raising the wage threshold, today’s move by the Department of Labor will harm many higher education institutions, employees and students . . . requiring such a dramatic and costly change to be implemented so quickly will leave many colleges with no choice but to respond to this regulation with a combination of tuition increases, service reductions and, possibly, layoffs,” Broad said in a statement.

“We appreciate the department’s willingness to reconsider slightly its initial proposal to raise the threshold even higher. But negatively impacted by the new regulations are a wide array of non-faculty employees—from athletics coaches and trainers to admissions recruiters and student affairs officers—whose work is not well suited to hourly wage status and who will face diminished workplace autonomy and fewer opportunities for flexible work arrangements and career development.”

The Obama administration has issued both an overview and more detailed guidance for colleges and universities on how to implement the new rule. However, these documents merely collect information about current law that was not changed by the new rule. ACE had hoped the final rule would provide some relief related to postdoctoral researchers because their salaries, set by federal grant making agencies, are often below the new threshold. Unfortunately, the new rule will treat these researchers like other employees with salaries below the new threshold.

As the guidance reiterates, many college employees are exempt from the new rule because they are considered teachers. As Inside Higher Ed (IHE) outlined this morning, the teaching exemption applies to 1. Anyone whose primary job duty is instruction; 2. Students in research jobs under the supervision of a faculty member while in the course of a degree program; 3. Coaches and assistant coaches whose primary duty is teaching; and 4. Some academic personnel involved in advising or helping students.

“Many other groups of employees—including those in admissions, student affairs and many other divisions—would be covered by the new rules,” according to IHE.

For a further discussion of the rule, the College and University Professional Association for Human Resources (CUPA-HR) has scheduled a webinar for May 25 on “FLSA Overtime Final Rule: What You Need to Know and Do Now.”

ACE also will be convening a panel of experts for a June 17 live webcast to further explore the complexities and challenges campuses will face in implementing these new regulations. More information on how to register will be provided soon.

What Obama’s Overtime Rule Could Mean for Colleges

This week the Obama administration released a final rule that will extend overtime pay to millions more American workers, including hundreds of thousands of lower-level salaried employees on college campuses. Much of the attention has focused on the impact on postdoctoral fellows, the overworked, underpaid backbone of the academic research enterprise.

But it’s not just postdocs who will benefit from the rule, which will double the annual salary cutoff below which workers are generally eligible for overtime pay, raising it to $47,476. Many entry-level and midlevel professionals — from admissions officers to athletic trainers to student-aid administrators — will qualify too.

That means the rule will be expensive for colleges, many of which already struggle with high labor costs. And that’s where the downside comes in: Already college groups are warning of consequences when the rule kicks in, at the start of December.
"Requiring such a dramatic and costly change to be implemented so quickly will leave many colleges with no choice but to respond to this regulation with a combination of tuition increases, service reductions, and, possibly, layoffs," Molly Corbett Broad, president of the American Council on Education, said in a written statement.

Peter McPherson, president of the Association of Public and Land-Grant Universities, wrote in a blog post published on Thursday that "there is simply no way for universities to absorb costs of this magnitude without an impact on our academic, research, and outreach missions."

Here's what the new overtime-pay rule means for your campus:

**It's a boon to postdocs — but not all of them.**

Postdoctoral fellows have been agitating for higher pay for years, and the National Academy of Sciences has recommended that colleges pay postdocs a starting salary of at least $50,000. This rule will compel colleges to increase their pay to at least $47,477, to avoid having to pay them overtime. (The National Institutes of Health has already announced that it will raise its own research stipend for postdocs above that threshold.)

On Thursday the National Postdoctoral Association, which represents 79,000 postdoctoral scholars, issued a statement calling the rule "a positive step towards achieving our goal of increasing compensation for postdoctoral researchers nationwide."

Yet the association also expressed disappointment that the overtime expansion leaves out researchers who primarily teach, including some in the humanities. Most salaried teachers — including adjunct instructors and graduate teaching assistants — aren't eligible for overtime pay, under a longstanding policy that exempts them from the benefit. The postdoc association says that exception creates an unfair distinction between scientific and humanities postdoctoral studies. The group has called for a "uniform application" of the rule.

**This doesn't affect just research universities and large public institutions.**

While such institutions are more likely to have large numbers of scientific postdocs, the rule's reach extends well beyond the laboratory. In fact, the new salary threshold applies to many administrative employees, including those in admissions, financial aid, academic affairs, and athletics.

David S. Baime, senior vice president for government relations and policy analysis at the American Association of Community Colleges, said his organization’s members include 386 colleges whose business and financial-operations staff members each earn less than $47,000, on average. They employ, on average, 12 staff members each. The association includes 364 institutions where the average computer, engineering, and science salary is below the threshold, with an average staff of 10.

Private colleges, meanwhile, said the rule would undermine their efforts to rein in tuition growth. In a statement, the National Association of Independent Colleges and Universities said that "the rule will have a significant impact on campus budgets — most of which have already been set for the next fiscal year, if not the next two fiscal years."

Darron Collins, president of the tiny College of the Atlantic, in Maine, said he feared the rule could spell a "potential reduction in autonomy for employees who up until now have viewed their work as a vocation more than a job."

**There's more than one way to comply with the rule.**

When President Obama first proposed raising the overtime-pay threshold to just over $50,000, last July, the College and University Professional Association for Human Resources sent a letter that warned that the new rule would force colleges to reclassify many workers to hourly status, "to the detriment of employees, institutions, and students."

But the Labor Department, in guidance issued with the rule this week, said colleges have "numerous options for compliance." They can raise the salaries of newly eligible employees so those salaries are above the threshold; they can pay such employees overtime, on top of their salaries; they can "reorganize workloads, adjust schedules, or spread work hours" to limit overtime pay; or they can reduce employees’ base pay so the amount they are paid, with overtime, "remains largely the same."

The guidance also notes that public colleges that qualify as "public agencies" under federal labor law may provide employees with compensatory time off in lieu of cash overtime premiums. Private colleges do not have that option.
Information Security
DoD Issues Final Rule on ‘Basic’ Safeguards for Information Systems

With an apparent nod to widespread concerns from universities and others, the Department of Defense (DoD), NASA, and the General Services Administration have issued a final rule that imposes “basic” safeguards for systems holding federal information, rather than requiring protections for certain types of the information. But universities and others should prepare for additional and perhaps stricter regulations, as the agencies said the final rule was “just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems.”

Published May 16, the rule finalized a proposed rule issued on Aug. 24, 2012, and an advance notice of proposed rulemaking released in December 2010. Under the proposed rule, contractors would have had to implement protections to safeguard systems that contain information termed “other-than-public” that was generated by or for the federal contracting agencies (RRC 10/12, p. 1).

These safeguards would include physical and electronic barriers, intrusion protections and other measures called for in a related 2011 DoD proposed rule, and would have been applied to that rule’s seven categories: “public computers or websites; transmitting electronic information; transmitting voice and fax information; physical and electronic barriers; sanitization; intrusion protection and transfer limitations” (RRC 8/11, p. 9).

Keep an Eye Out

Among the concerns expressed about the proposed rule was the lack of an exception for basic research.

With an effective date of June 15, the final regulation stems from Federal Acquisition Regulation case 2009-030 and FAR case 2011-020, Basic Safeguarding of Contractor Information Systems, which were merged in 2011.

The new regulation deletes the definition of public information and “does not focus on the protection of any specific type of information, but requires basic elements for safeguarding an information system,” according to the preamble. “These requirements should not have any chilling effect on fundamental research,” it states.

The rule, “which focuses on ensuring a basic level of safeguarding for any contractor system with Federal information, reflective of actions a prudent business person would employ, is just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems.”

Under the regulation, a “contracting officer shall insert the clause at 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, in solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.”

Contractors are required to “apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:”

- “Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).”
- “Limit information system access to the types of transactions and functions that authorized users are permitted to execute.”
- “Verify and control/limit connections to and use of external information systems.”
- “Control information posted or processed on publicly accessible information systems.”
- “Identify information system users, processes acting on behalf of users, or devices.”
- “Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.”
- “Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.”
- “Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.”
- “Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.”
• “Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.”

• “Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.”

• “Identify, report, and correct information and information system flaws in a timely manner.”

• “Provide protection from malicious code at appropriate locations within organizational information systems.”

• “Update malicious code protection mechanisms when new releases are available.”

• “Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.”

The rule may have calmed some fears about expensive and complicated safeguards. But that anxiety may return as the agencies take further steps in the future, as noted.

The rule points out that in summer 2015, the Office of Management and Budget “issued proposed guidance to enhance and clarify cybersecurity protections in Federal acquisitions related to CUI [controlled unclassified information] in systems that contractors operate on behalf of the Government as well as in systems that are not operated on behalf of an agency but are used incidental to providing a product or service for an agency with particular focus on security controls, incident reporting, information system assessments, and information security continuous monitoring.”

The agencies “will be developing FAR changes to implement the OMB guidance when it is finalized,” the rule states. “In addition, we plan to develop regulatory changes for the FAR in coordination with National Archives and Records Administration (NARA) which is separately finalizing a rule to implement” Executive Order (E.O.) 13556, which deals with CUI.

“The E.O. established the CUI program to standardize the way the executive branch handles information (other than classified information) that requires safeguarding or dissemination controls,” the rule explains. The agencies offered no timeline as to when final guidance and the other rules would be forthcoming.

MedStar Health forced to turn patients away after virus attack

Healthcare IT News– March 30, 2016

Despite saying that it responded quickly to the malware that locked users out of IT systems, the health network had to deny some patients access while it continues recovering from the malicious code.

MedStar Health was forced to turn some patients away on Tuesday as it recovered from a computer virus.

The healthcare provider said Tuesday that it was making progress toward restoring functionality of its computers, which were taken down after being hit by malware early Monday morning. MedStar then took those IT systems offline to avoid further corrupting its network infrastructure.

“With a few unique exceptions, all of our doors remain open,” MedStar explained in a statement, while several reports said patients were denies access to the hospital and sent elsewhere. “The safety of patients and associates and the privacy of their information is our utmost concern.”

Officials said they have not encountered evidence that patient data has been either stolen or compromised and that MedStar employees will refrain from adding any new data to systems without first determining that those computers are clean.

The attack, currently under investigation by the FBI, forced MedStar’s 10 hospitals and more than 250 outpatient centers to shut down their computers and email on Monday.

The provider said staffers were working Tuesday to restore the majority of IT machines. They are using backup systems, including paper documentation, where necessary, and as an additional layer of support to clinical operations.

Several reports described the attack as ransomware, malicious code deployed to hold systems hostage until victims pay for a key to regain access. While neither the FBI nor MedStar have confirmed that the code is in fact ransomware, that style of attack has spiked in recent weeks with instances at Chino Valley Medical Center and its sister site Desert
Valley Medical Center in California, Methodist Hospital in Kentucky and, prior to those, Hollywood Presbyterian was forced to pay cybercriminals $17,000 in Bitcoin in mid-February.

Information Technology

DoJ Issues Supplemental Advance Notice of Proposed Rulemaking on Accessibility of Web Information and Services of State and Local Government Entities

Supplemental advance notice of proposed rulemaking on the accessibility of web in formation and services of state and local government entities was published by the U.S. Department of Justice. The Department is considering revising the regulations implementing Title II of the Americans with Disabilities Act (ADA) to establish specific technical requirements that would make the services, programs, and activities that state and local governments offer to the public via the internet accessible to those with disabilities. The Department is considering proposing WCAG 2.0 Level AA as the accessibility standard that would apply to Web sites and Web content of title II entities. This supplemental advance notice was released to solicit additional public comments on various issues relating to the potential application of such technical requirements to the websites sites of Title II entities and to gather information for preparing a regulatory impact analysis. The Department also issued a statement announcing the supplemental notice. Comments must be submitted on or before ninety days after the date of publication.

MACRA

MACRA Proposed Physician Payment Rule Is Out

On May 9, CMS released the much-anticipated proposed rule on MACRA that will implement the two physician payment options: the Merit-Based Incentive Payment System (MIPS) and Alternative Payment Models (APMS) beginning in 2019. The rule is available at: https://www.federalregister.gov/articles/2016/05/09/2016-10032/medicare-program-merit-based-incentive-payment-system-and-alternative-payment-model-incentive-under.

CMS says that it will closely examine the recommendations made by the HHS office of Assistant Secretary for Planning and Evaluation (ASPE) regarding the issue of risk adjustment for socioeconomic status on quality and resource use and will incorporate recommendations, as feasible and appropriate, in future rulemaking. The ASPE report is expected to be out by October 2016.

The new payment system begins January 1, 2019 but the performance period that will determine payment in that year is 2017. The proposed rule also will replace the current Meaningful Use program for EPs with a new program, Advancing Care Information that CMS describes as focusing on patient care and connectivity goals.
SUMMARY

Following are excerpts from news articles having a risk management or compliance impact. The full article may be seen at the referenced source (some may require subscription to access). Only one topic was noted for this month:

• Campus Safety

Campus Safety

How Colleges Train for Active Shooters on Campus


Shootings and other incidents of violence often raise alarm among students and faculty members about what they should do when a worst-case scenario becomes a reality. So more colleges are taking extra steps to prepare themselves for one of the most-feared situations in academe: an active shooter on the campus.

Campuses are embracing active-shooter training as a way to keep fear at a minimum and raise confidence in moments when chaos might otherwise reign.

How colleges go about that depends on an institution’s needs and how much they want to commit to the training. While some seek guidance from in-house safety experts, others hire companies to lead drills, demonstrations, and simulations. And some make it mandatory for students to watch active-shooter response videos and take e-training courses, while others do not.

Reality-Based Training

An active-shooter-response training exercise was underway last week at Temple University, in Philadelphia, just one day after the deadly shooting at the University of California at Los Angeles.

Raymond L. Betzner, an associate vice president for communications at Temple, said the exercise wasn’t a reaction to the UCLA incident, and had been planned months earlier.

Mr. Betzner said it wasn’t the first time Temple’s emergency responders had undergone active-shooter training. But he said it was the first time the university had held such training on a broad scale.

As part of the safety drill, officers with Temple’s police and security divisions, in full riot gear, searched its residence halls for two mock gunmen played by actors. The officers eventually cornered the shooters, but not before they simulated killing one person and injuring others. The victims, also played by actors, were drenched in fake blood, as medical students and professionals examined their wounds. Meanwhile, Temple’s media-relations team fielded phone calls, simulating the conditions of an actual emergency.

Temple also tested what Mr. Betzner called a "light web page," which he described as able to withstand heavy traffic and to be used to post basic information in a crisis, just in case the normal site crashed. After the training ended, the participants took part in what’s known as a "hotwash," in which they talked about their experiences.

Mr. Betzner said the people involved in the training were glad they had participated but hoped they never had to use what they had learned. He strongly encouraged other campuses to stage active-shooter trainings.

"You need to get a feel for this," Mr. Betzner said. "You need to get the sensations for it. Even though we knew that it was not a real scenario, that there weren’t real people hurt, there is pressure, a real tension that comes, and under that pressure people respond differently."

Cerritos College, in Norwalk, Calif., held a similar drill last week. Members of the college’s track-and-field team played the role of victims as its campus police department and local law-enforcement agencies combined forces to test their ability to work together in a crisis.

It was the college’s first time conducting multi-agency training, said Tom H. Gallivan, chief of the campus police, and each agency learned about the importance of communication.

Customized Training Services

Randy Spivey is chief executive of the Center for Personal Protection and Safety, a company that trains campus police officers and others to become active-shooter training instructors. The organization has taught many higher-education
institutions since 2007, when a gunman shot and killed 32 people at Virginia Tech and wounded 17 others before killing himself. The tragedy at Virginia Tech was a watershed moment for campus safety, Mr. Spivey said.

In recent years, Mr. Spivey said, campuses have been changing how they want to be trained. In the past, some institutions had asked students to be trained differently than employees, he said, but a majority don’t anymore. He said institutions had feared that students would use the training, somehow, as active shooters themselves. His company offers a range of services, from videos that cost about $200 to fully customized trainings that could cost $70,000 to $150,000, he said.

Greg J. Crane, founder of the Alice Training Institute, which also specializes in active-shooter trainings, said his company had trained hundreds of higher-education institutions.

Mr. Crane said there have been eight instances in which his training system was used in real active-shooter situations. And in those cases, he said, there have been no fatalities.

It is essential for safety officers and other people on campuses, Mr. Crane said, to be trained in how to respond in an active-shooter situation, especially now. The sound of gunshots should elicit a second-nature reaction, similar to muscle memory, he said.

"If the room was on fire," he said, "I don’t think anybody would say, I didn’t know what to do."
SUMMARY

Following are excerpts from news articles having a risk management or compliance impact. The full article may be seen at the referenced source (some may require subscription to access). Topics for this month include the following:

- Campus Safety
- HIPAA
- Information Security
- OSHA Reports

Campus Safety

How Colleges Train for Active Shooters on Campus


Shootings and other incidents of violence often raise alarm among students and faculty members about what they should do when a worst-case scenario becomes a reality. So more colleges are taking extra steps to prepare themselves for one of the most-feared situations in academe: an active shooter on the campus.

Campuses are embracing active-shooter training as a way to keep fear at a minimum and raise confidence in moments when chaos might otherwise reign.

How colleges go about that depends on an institution’s needs and how much they want to commit to the training. While some seek guidance from in-house safety experts, others hire companies to lead drills, demonstrations, and simulations. And some make it mandatory for students to watch active-shooter response videos and take e-training courses, while others do not.

Reality-Based Training

An active-shooter-response training exercise was underway last week at Temple University, in Philadelphia, just one day after the deadly shooting at the University of California at Los Angeles.

Mr. Betzner said it wasn’t the first time Temple’s emergency responders had undergone active-shooter training. But he said it was the first time the university had held such training on a broad scale.

As part of the safety drill, officers with Temple’s police and security divisions, in full riot gear, searched its residence halls for two mock gunmen played by actors. The officers eventually cornered the shooters, but not before they simulated killing one person and injuring others. The victims, also played by actors, were drenched in fake blood, as medical students and professionals examined their wounds. Meanwhile, Temple’s media-relations team fielded phone calls, simulating the conditions of an actual emergency.

Temple also tested what Mr. Betzner called a "light web page," which he described as able to withstand heavy traffic and to be used to post basic information in a crisis, just in case the normal site crashed. After the training ended, the participants took part in what’s known as a "hotwash," in which they talked about their experiences.

Mr. Betzner said the people involved in the training were glad they had participated but hoped they never had to use what they had learned. He strongly encouraged other campuses to stage active-shooter trainings.

"You need to get a feel for this," Mr. Betzner said. "You need to get the sensations for it. Even though we knew that it was not a real scenario, that there weren’t real people hurt, there is pressure, a real tension that comes, and under that pressure people respond differently."

Cerritos College, in Norwalk, Calif., held a similar drill last week. Members of the college’s track-and-field team played the role of victims as its campus police department and local law-enforcement agencies combined forces to test their ability to work together in a crisis.
It was the college’s first time conducting multi-agency training, said Tom H. Gallivan, chief of the campus police, and each agency learned about the importance of communication.

**Customized Training Services**

Randy Spivey is chief executive of the Center for Personal Protection and Safety, a company that trains campus police officers and others to become active-shooter training instructors. The organization has taught many higher-education institutions since 2007, when a gunman shot and killed 32 people at Virginia Tech and wounded 17 others before killing himself. The tragedy at Virginia Tech was a watershed moment for campus safety, Mr. Spivey said.

In recent years, Mr. Spivey said, campuses have been changing how they want to be trained. In the past, some institutions had asked students to be trained differently than employees, he said, but a majority don’t anymore. He said institutions had feared that students would use the training, somehow, as active shooters themselves. His company offers a range of services, from videos that cost about $200 to fully customized trainings that could cost $70,000 to $150,000, he said.

Greg J. Crane, founder of the Alice Training Institute, which also specializes in active-shooter trainings, said his company had trained hundreds of higher-education institutions.

Mr. Crane said there have been eight instances in which his training system was used in real active-shooter situations. And in those cases, he said, there have been no fatalities.

It is essential for safety officers and other people on campuses, Mr. Crane said, to be trained in how to respond in an active-shooter situation, especially now. The sound of gunshots should elicit a second-nature reaction, similar to muscle memory, he said.

"If the room was on fire," he said, "I don’t think anybody would say, I didn’t know what to do."

**HIPAA**

**Weekend Tragedy Sheds Light on HIPAA Rules**


The federal privacy rule in the Health Insurance Portability and Accountability Act establishes a set of national standards for the protection of certain health information.

The privacy rule provides guidance to organizations subject to the privacy rule for the use and disclosure of certain health information — referred to as protected health information. The goal of the rule is to achieve a proper balance that protects the privacy interests of individuals seeking medical care, yet permits the use and disclosure of such protected health information for limited reasons deemed important by the law.

In the aftermath of the terror attack at a gay nightclub in Orlando, the federal government acted swiftly to waive certain provisions of the privacy rule under Section 1135(b)(7) of the Social Security Act in order to limit the additional agony family members would suffer by waiting for news of their loved one.

**In Wake of Oregon Shooting, Don't Expect Gun Makers to Pay**

Specifically, to satisfy the preconditions for issuing the waiver, President Barack Obama declared the Orlando shooting a national emergency and Health and Human Services Secretary Sylvia Mathews Burwell declared the situation a public health emergency. These two actions enabled the HHS secretary to then waive sanctions and penalties against Orlando-area hospitals providing care to the wounded should they fail to comply with certain requirements of the privacy rule, including for example failing to obtain a patient's consent before speaking with family members or friends involved in the patient's care.

The waiver invoked by the HHS secretary in this situation is very narrow. The rule itself was not suspended; rather the waiver acted only to insulate those hospitals providing care to the individuals wounded in the attack from certain sanctions and penalties that the rule would otherwise impose.
Compliance is still required with the privacy rule except for that very narrow set of disclosures permitted by the waiver. For example, while the waiver permits disclosure of general information as to a patient, it does not extend to the actual posting or disclosure of medical records.

Additionally, the waiver applies only in the emergency area and for the emergency period identified by the HHS secretary not to exceed 72 hours or until the emergency declaration is lifted if earlier, and only to those care-providing hospitals that instituted a disaster protocol.

When the emergency declaration terminates, the waiver will no longer be in effect, and hospitals must then comply with all aspects of the privacy rule for all of its patients, even if 72 hours has not elapsed since the date when the hospital's disaster protocol was first instituted.

The Orlando shooting presented a unique situation where family and friends were desperately seeking protected health information regarding the dozens of individuals wounded.

With the waiver of the privacy rule's sanctions and penalties, those hospitals providing care were able to disclose certain information for a limited period of time. By invoking the waiver, the federal government effectively determined that — for not longer than a 72-hour period — the interests of family and friends in obtaining certain information outweighed some of the privacy interests of those receiving medical care.

Fortunately, the federal government has only infrequently had to make these kinds of value judgments.

Information Security

Congress ponders health care cybersecurity

BenefitsPRO – May 26, 2016

Hospitals are panicked, and Congress doesn’t know what to do to make them feel better about cyberattacks.

A number of recent high profile hackings have raised alarms about the vulnerabilities of the nation’s health care system to hackers.

A report by PBS at the end of March estimated that 113 million health records had been compromised in 2015. The nation’s performance had improved during the first three months of 2016; only 3.5 million had been accessed.

What is particularly troublesome is “ransomware,” a type of virus that can infiltrate a computer system and demand a ransom to give the owner control of the system again. The ransom is often demanded in bitcoins, the cyber currency.

Those who have health care records hacked are in worse shape than those whose credit card numbers are swipe.

Earlier this year, officials of Hollywood Presbyterian Hospital paid hackers a roughly $17,000 ransom. While many saw the hospital’s decision as rational, the precedent it set scares health care leaders who believe it may embolden hackers to target others.

According to Politico, hospitals across the country face nearly weekly threats from similar actors. Part of the problem, explain some experts, is the pressure the Obama administration has put on health care providers to implement electronic health records.

The administration’s push for EHRs “thrust tens of thousands of health care providers into the digital age before they were ready,” David Brailer, chief of health IT in the administration of George W. Bush told Politico. “One area where they were woefully unprepared is security.”

Lawmakers are seeking solutions, including through a bipartisan bill introduced last month that would require the Department of Health and Human Services to appoint a point person on cybersecurity.

On Wednesday, however, Rep. Joseph Pitts, R-PA, the chair of the Energy and Commerce Subcommittee on Health, said that he was unsure of whether the proposed legislation would go far enough in addressing the issues revealed in a study of the agency’s security measures conducted by the committee.

"The committee’s investigation uncovered problems that were much more persistent and pervasive than previously thought,” he said in a statement.
OSHA Reports

OSHA’s New Rule Impacts the Health Care Industry  
*JDSUPRA Business Advisor* – July 26, 2016

The U.S. Occupational Safety and Health Administration (OSHA) recently issued a final rule that becomes effective January 1, 2017 requiring healthcare industry employers to electronically submit to OSHA injury and illness data from their OSHA logs. This information will then become publicly available on the OSHA website.

As a corollary, and “to ensure the completeness and accuracy of injury and illness data,” the final rule also:

- Creates an explicit requirement that employees must be informed of their right to report work-related injuries and illnesses free from retaliation;
- Specifically requires that an employer's procedure for reporting work-related injuries and illnesses must be reasonable and not deter or discourage employees from reporting; and
- Explicitly prohibits retaliation against employees for reporting work-related injuries or illnesses.

The requirement to report data applies to: (1) work locations with 250 or more employees, and (2) work locations with 20 to 249 employees in specific “high-risk industries” identified in the rule. The rule includes several types of healthcare industries in its definition of high-risk industries. Specific healthcare industries that must comply with this rule if they have 20 or more employees at a particular work location are:

- Ambulatory healthcare services;
- General medical and surgical hospitals;
- Psychiatric and substance abuse hospitals;
- Specialty (except psychiatric and substance abuse) hospitals;
- Nursing care facilities;
- Residential mental retardation, mental health, and substance abuse facilities;
- Community care facilities for the elderly; and
- Other residential care facilities.

Businesses with 250 or more employees at a work location in industries covered by the new recordkeeping regulation must submit information from their 2016 Form 300A by July 1, 2017. These employers will also be required to submit information from all 2017 forms (300A, 300, and 301) by July 1, 2018. Starting in 2019, the information must be submitted by March 2 each year. Businesses with 20-249 employees in high-risk industries, including those healthcare industries mentioned above, must submit information from their 2016 Form 300A by July 1, 2017, and their 2017 Form 300A by July 1, 2018. Starting in 2019, the information must be submitted by March 2 each year.

OSHA will make the injury and illness data public. After removing any Personally Identifiable Information that could be used to identify individual employees, OSHA will post the data on its website, and anyone will be able to download it. Employers in the above-referenced high-risk industries (and those with 250 or more employees) should begin planning now to ensure compliance with the January 1, 2017 reporting deadlines.

The new rule also emphasizes that employees who report workplace related injuries and illnesses may not be discriminated against or retaliated against because they have reported such injuries or illnesses. It provides OSHA with the authority to cite an employer for retaliation even in the absence of any employee complaint. The commentary to the rule says:

- Employers must have a reasonable procedure for employees to report work-related injuries and illnesses.
- Employers’ reporting procedures cannot deter or discourage reasonable employees from accurately reporting a workplace injury or illness.
Blanket or automatic post-accident testing policies are prohibited and will be viewed as taking an adverse action against, retaliating against, or discouraging employees from reporting accidents.

Employers need not specifically suspect drug use before testing, but there should be a reasonable possibility that drug use by a reporting employee was a contributing factor to the reported injury or illness in order for an employer to require testing, and, even then, the testing should be limited to only the employee who caused the accident rather than everyone involved.

Although the new rule does not prohibit all post-accident/post-injury drug testing policies, OSHA’s position is that the circumstances of some accidents make it unlikely that drug use was a contributing factor, and therefore testing employees in these situations would be viewed as retaliation. OSHA provides these examples of circumstances where required drug testing would be suspect:

- After an employee reports a bee sting;
- When an employee has a repetitive strain injury;
- After an injury caused by a lack of machine guarding; or
- When a machine or tool malfunctions.

The rule acknowledges many employers implement post-accident/post-injury drug testing policies because they are located in states that offer workers’ compensation premium reductions for enacting Drug Free Workplace Policies. Compliance with these workers’ compensation programs or other state or federal laws or regulations requiring post-accident/post-injury or reasonable suspicion testing are still permitted.

Employers must also specifically inform employees: (i) they have the right to report work-related injuries and illnesses; and (ii) the employer is prohibited from retaliating against employees for reporting work-related injuries or illnesses. Employers also must establish a reporting procedure that does not deter or discourage an employee from reporting work-related injuries and illnesses. These posting and reporting requirements are effective as of November 1, 2016.

In light of OSHA’s new rule, employers in the health care industry should review drug testing policies as well as accident/injury reporting policies to ensure they do not violate OSHA’s new rules.
SUMMARY

Following are excerpts from news articles having a risk management or compliance impact. The full article may be seen at the referenced source (some may require subscription to access).

- Athletics
- Campus Safety
- HIPAA
- Information Security
- On-Line Education

Athletics

Georgia Southern U. Staff Members Helped Athletes Cheat, NCAA Rules


Two staff members at Georgia Southern University breached ethical-conduct rules by providing forbidden academic assistance to three athletes, the National Collegiate Athletic Association announced on Thursday, citing a decision by its Division I Committee on Infractions.

In one instance, an assistant director of compliance gave a football player a thumb drive containing coursework from a previous semester that the player then used for a class he was enrolled in, the NCAA said. The student eventually turned in an assignment taken from the thumb drive and claimed it as his own. A professor, noticing the deceit, questioned the student, who then collaborated with the assistant director on a response, wherein the student assumed full responsibility for the academic dishonesty. Later, under questioning, the student acknowledged that the staff member had provided him with the thumb drive and instructed him to lie.

The assistant director also did not cooperate with NCAA investigators, the association said.

In another case, a director of student-athlete services was found to have submitted numerous extra-credit assignments for two athletes without their knowledge. She did so by obtaining their login and password information, the NCAA said. Neither staff member still works at Georgia Southern, *NBC Sports* reported.

The NCAA, which did not disclose the names of the staff members or the athletes, also announced various penalties and corrective measures, including a public reprimand, a reduction of two scholarships for the football program in the next academic year, and a fine of $5,000 plus 1 percent of the football program’s operating budget, to be paid by the university.

Campus Safety

10 Ways to Bolster Crisis Communications Planning


There is never downtime in higher education—there’s simply a shift in priorities. The summer months provide an opportunity for strategic planning, reporting, advancing new initiatives and connecting more deeply with colleagues. It’s also a valuable time to reflect on crisis communications. We know crises can occur at any time, but the summer months may provide a reprieve as the campus activity slows down during this period.

The last step of any crisis communications plan should be to review the work of the team and make adjustments to improve communications in the future. The following 10 recommendations for crisis communications are the result of this review process and could be useful for PR professionals and communications offices at higher education institutions.

1. **Update your crisis communications plan, and review it. Repeat.**

Ask yourself who knows the plan and who has reviewed it recently. Oftentimes this work gets put on the backburner because there are other actionable and immediate priorities being worked on—commencements, recruitment events and overall managed chaos throughout the semester. Take the time to read through your plan and make revisions that
are relevant to your environment (e.g., are there new staff on the institution’s crisis response team or has your institution implemented a new text messaging platform that needs to be incorporated into the plan?).

2. Be prepared.
Think about crisis communications and management often, so when the inevitable happens on your campus or shows up in your inbox, you aren’t wasting time thinking about what needs to happen and how to respond effectively. A crisis will never go as planned, but doing as much proactive planning in advance of a crisis will go a long way. Consider different scenarios, such as sexual assault, student behavior issues, town/gown relations and litigation, and then map out how to best respond.

3. Assess the situation thoroughly and quickly.
The crisis response team needs to act with a sense of urgency. Make sure communications has a seat at the table when issues are being assessed. It’s important to review the issue/crisis from all angles and understand the opportunities to address it. Input from the entire crisis team is invaluable as it provides a more comprehensive perspective and can elevate anticipated reactions and possible new challenges, as well as opportunities.

4. Communicate in a timely manner and with purpose.
What’s the message, who needs to know and when? Being proactive, open and transparent can help build good will. Recognize what information stakeholders need to hear and want to hear as part of message development. Remember faculty, staff and students first. Alumni and donors are a close second and will likely have a strong reaction based on the institution’s response and what is reported in the news. Be responsive to media and communicate key messages to better manage reputation and risk.

5. Show compassion.
Make sure your communications are genuine and empathetic, not cold and corporate. Reflect your institution’s culture and have an authentic voice. You will gain increased support and it may help move your organization away from the issue at hand.

6. Understand the broader context.
Obviously, the issue at hand is the focus, but knowledge of the surrounding environment is important. It’s helpful to know if the issue is one of several, a standalone, first in the region or a national issue. Knowing about other issues taking place on campus and any upcoming events (e.g., admissions and alumni) are factors to consider.

7. Partner with legal.
It’s critical that legal counsel weigh in on all communications and is included in strategy and planning meetings. They bring sound guidance and perspective around current and future litigation concerns and have deep knowledge around the issue, and potentially others, to help shape messaging. It’s also important to maintain confidentiality and privileged communications. A strong relationship will elevate thinking around other considerations to factor into what can and cannot be said.

8. Listen to the dialogue taking place around you.
Be mindful and attentive to what’s being said about the crisis, the concerns being raised and any rumors, especially as they can snowball quickly. On a college campus, the buzz can happen almost immediately. Monitor social media channels and the media, including comments to stories. This understanding will help head off any growing concerns and misinformation and put the institution in better control of the narrative that will be communicated through holding statements, talking points, audience-specific communications, Q&As and other materials.

9. Activate a social media plan.
Social media can add to the 24/7 frenzy. It’s important to listen to the conversations taking place and design an appropriate engagement strategy. It could run the gamut from posting all communications and responding to posts, to going quiet and communicating directly with a follower. Know all of your channels—from the Dean’s Office to athletics—and which matter most. Make sure there is clear communication with these groups in advance of a crisis, about strategy, how they can support efforts and what actions are acceptable. Finally, make sure any current content being posted does not come across as insensitive in the context of the current issue.

10. Identify and train your media spokesperson.
Put yourself in the shoes of the stakeholder to determine the optics of a message being delivered by different people. This exercise will help identify the most appropriate spokesperson. Also, college presidents can benefit from training just as much as deans and other divisional leaders. The time to do it is now.
Five Myths About Patient Privacy


Shortly after the recent massacre at an Orlando nightclub, the city’s mayor declared that the White House had agreed to waive federal privacy rules to allow doctors to update victims’ families. News of the waiver was widely reported, but as the Obama administration later clarified, both the mayor and the media were “simply mistaken.” No waiver was granted because none was needed. The confusion amid the tragedy in Orlando underscores widespread misconceptions about the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Here we shed light on a handful of myths that bedevil doctors and patients alike.

Myth No. 1 - HIPAA prohibits communicating with patients’ loved ones.

HIPAA sets national standards to safeguard the privacy of individuals’ health information. As in Orlando, it is often perceived as a barrier to effective communication between doctors and patients’ loved ones. Virginia state Sen. Creigh Deeds — whose mentally ill son attacked him before committing suicide in 2013 — recently testified before Congress that “HIPAA prevented me from accessing the information I needed to keep him safe and help him towards recovery.”

Such stories are heart-wrenching but misattributed to HIPAA. In most cases, the privacy regulation permits doctors and nurses to communicate with a patient’s family, friends or caretakers. The rules were crafted to account for the realities of health care, including the integral role often played by those closest to the patient.

As the former head of HIPAA enforcement told Congress, “HIPAA is meant to be a valve, not a blockage.” When the patient is present and clearheaded, the law allows hospitals to share relevant information with loved ones so long as the patient does not protest. This can be accomplished through the patient’s agreement or acquiescence, or based on a doctor’s professional judgment that the patient does not object. If a person accompanies the patient to an appointment, for example, doctors can reasonably infer that discussing the patient’s treatment in front of that individual is appropriate.

When the patient is unavailable or incapacitated, doctors can also exercise professional judgment to determine whether disclosure is in the patient’s best interests. A clear example is when the patient is unconscious, but this provision can also apply if the patient is suffering from temporary psychosis and lacks the ability to make health-care decisions.

Still, studies have shown that confusion and fear over privacy laws often lead hospitals to unnecessarily withhold information and reflexively cite HIPAA as justification — an approach that can make families feel locked out of care.

But overall, HIPAA affords doctors significant flexibility to communicate with patients’ loved ones, whether about routine or time-sensitive matters. The only time the law truly forecloses the sharing of such information is when the patient is present, lucid and tells doctors not to — and even then, patients’ wishes can be overridden in the event that they pose a serious and imminent threat to health or safety.

Myth No. 2 - Same-sex marriage rights are critical to equality under HIPAA.

Before the rumors of a HIPAA waiver in Orlando were quelled, various news outlets reported that it marked a “victory for gay rights.” Waiving medical privacy laws was portrayed as a prerequisite for sharing information with same-sex partners.

In reality, HIPAA enables discussions with relatives, friends or anyone else identified by the patient, meaning that the impact of the Supreme Court’s marriage-equality rulings on permissible communication was marginal at best. HIPAA does not require doctors to obtain proof of identity when inquirers say they are a patient’s friends or relatives. Providing information to family and friends under HIPAA is linked to their involvement in the patient’s medical affairs, not the legal status of their relationship. Patients’ sexual preferences were irrelevant long before same-sex marriage became the law of the land.

Early in his administration, President Obama emphasized the importance of hospital visitation rights for same-sex partners and sought to enforce this policy through Medicare rules. However, spouses — unlike parents vis-a-vis their minor children — are not automatically presumed to have access to patient records. It is up to the patient to designate them or doctors to involve them as clinically appropriate.
Myth No. 3 - HIPAA provides extra protections for mental health information.

Rep. Tim Murphy, also a psychologist from Pennsylvania, believes that amending HIPAA is crucial to mental health reform. Rep. Eddie Bernice Johnson, a registered nurse from Texas, says that “individuals with mental illness and substance use disorders often face obstacles to treatment because of the Privacy Rule within HIPAA.” New York’s chief psychiatrist has described HIPAA as “the tragedy of mental health law.”

Yet HIPAA does not distinguish between physical and mental health information, nor does it provide extra protections for the latter. Indeed, HIPAA is generally agnostic as to the type of health information being protected. The drafters of the privacy regulation acknowledged that many states had laws specifically guarding records related to mental illness and “other stigmatized conditions” but declined to follow their lead. While the HIPAA rules in no way erode these additional state protections, they do not confer any special status on mental health information.

The rare instance in which HIPAA affords greater protection to sensitive information involves “psychotherapy notes.” However, this exception is much narrower than is commonly understood. Psychotherapy notes are therapists’ private, desk-drawer notes reflecting on conversations during counseling sessions. They exist for therapists’ personal use as memory joggers and must be kept separate and apart from patient charts in order to retain their designation. Any information of wider utility — such as treatment or diagnosis — is excluded from the definition and associated protections. In fact, a main reason psychotherapy notes are shielded from disclosure is because they would have so little relevance or use to anyone other than the doctor who created them.

Myth No. 4 - HIPAA stops doctors from reporting threats.

Mass shootings involving mentally ill suspects often prompt discussion about what warning signs doctors should have reported. These questions persist even in cases when doctors had alerted authorities, as happened before the 2012 movie theater tragedy in Aurora, Colo.

After the Sandy Hook Elementary School shooting, one of Obama’s 23 executive actions was to clarify that “no federal law” prohibits health-care professionals from reporting threats of violence to the police. This mandate was accomplished via an open letter to the health-care community explaining that HIPAA allows doctors to issue appropriate warnings when they believe that patients present a serious and imminent threat to themselves or someone else. In such cases, doctors can disclose necessary information to law enforcement, school officials, family members, the target of a credible threat, or anyone else in a position to avert the danger. Under the HIPAA rules, doctors who take these steps are generally presumed to have acted in good faith.

When patients make threats or pose a high suicide risk, doctors often have a “duty to warn” emanating from state laws, court decisions or professional ethics rules. HIPAA does not in itself impose such a duty, but it explicitly permits health-care professionals to take action “consistent with” these standards.

Myth No. 5 - HIPAA is the reason for medical privacy.

HIPAA is often singled out as the basis of patient confidentiality. Yet privacy was a core value in health care long before the HIPAA rules were promulgated in the early 2000s. The Hippocratic Oath admonishes doctors to keep secret what they “see or hear” from patients. The American Medical Association’s first code of ethics, adopted in 1847, emphasized the “obligation of secrecy” at the heart of the doctor-patient relationship.

In practice, HIPAA provides a federal floor of privacy protections, not a ceiling. It defers to state laws that are “more stringent” or protective of patient rights. State laws that create additional safeguards for conditions deemed especially sensitive — whether HIV/AIDS, communicable diseases, cancer or mental illness — remain in full force. Neither does HIPAA override other federal laws. Thus, for example, substance-abuse programs subject to 1970s-era federal confidentiality requirements continue to follow those stricter standards in the vast majority of cases.

Even where HIPAA allows health information to be shared, it almost never requires it. Doctors and hospitals must still be cognizant of other applicable laws or professional ethics guidelines that impose stricter limitations. HIPAA is designed to align with these obligations as often as possible, but those instances where gaps arise tend to be the most complex and emotionally fraught.

HIPAA established a procedural framework for doctors, hospitals and other health-care players to exchange information without compromising patient privacy. Even if the law disappeared tomorrow, the legal precepts and ethical norms that long preceded it would remain in place — as would many of the frustrations cited by HIPAA’s most ardent detractors. This month, the House of Representatives proclaimed that “there exists confusion in the health care community around what is currently permissible under HIPAA rules.” Alas, that just may be the most accurate statement about HIPAA ever uttered.
Information Security

Is Your Company Prepared for a Ransomware Attack?

This year already appears to be the Year of Ransomware, with the healthcare industry most acutely feeling the pain inflicted by this malware species. April saw a record number of ransomware attacks in the United States.

Ransomware is a type of malware that locks a device or renders its data unusable until the victim pays the attacker a ransom, often in an alternative currency known as bitcoin. According to Symantec, there are two primary categories of the malware: locker ransomware (which locks the device until the ransom is paid) and crypto ransomware (which generally encrypts individual files without locking the user out of the device entirely). Both types of ransomware ultimately deny the victim access to the data stored on the device.

Ransomware can be delivered as a malicious payload in a manner similar to any other malware, including through phishing, social engineering, malicious advertising or an existing remote-access Trojan. Once downloaded on a device, the malware generally either locks the device or quietly begins encrypting data stored on it. Many types of ransomware also seek to traverse the victim’s network in an effort to move to other systems, including storage devices and critical servers. Only once the ransom is paid does the attacker unlock the device or provide the key to decrypt data, although in some cases attackers have reportedly not carried out their end of the bargain even after being paid.

The risks posed by ransomware extend well beyond the encryption of data or locking of a device. As more and more businesses embrace data-driven processes and increase their reliance on Big Data, a ransomware infection means not only that data or systems become unavailable – it means that the business may not be able to function. Entities in nearly all sectors, including financial services, e-commerce, cloud services, and more, depend on the availability of data and systems to function and provide core services. Critical infrastructure, which is often required to provide essential services (e.g., electricity, telecommunications), also depends heavily on data and system availability. As we have seen this year, hospitals appear to be particularly vulnerable.

Indeed, 2016 kicked off with a string of ransomware attacks targeting the health care industry. In early February, Hollywood Presbyterian Medical Center in Los Angeles had to operate using paper and fax machines after a ransomware attack prevented personnel from accessing patient records and communicating electronically. Reports indicated that patients bound for the emergency room had to be diverted to other hospitals. After 10 days of functioning largely in the pre-Internet era, the hospital elected to pay a $17,000 ransom, with its president and CEO noting that paying the hackers was the “quickest and most efficient way to restore our systems and administrative functions.”

Over the next several weeks similar attacks were perpetrated against a separate California hospital group, Kentucky’s Methodist Hospital, and most recently MedStar, which operates 10 Maryland hospitals. In those attacks, the requested ransoms ranged from $1,600 to $18,500, but all entities reported that they were able to resolve the attacks without paying the hackers. Health care ransomware attacks were not limited to the United States, as the U.S. Computer Emergency Readiness Team (US-CERT) noted in an alert that healthcare entities in Germany and New Zealand faced similar attacks in early 2016.

The FBI recently advised that individuals and organizations “should not pay the ransom” and highlighted that the “best way to protect yourself and your organization is to have a backup of your data, maintain it, and disconnect it from your computer.” US-CERT recently issued a ransomware alert recommending that entities take several added protective measures in addition to backing up data, including the use of application whitelisting, avoiding enabling macros from email attachments and ensuring that software patches are downloaded and antivirus programs are kept up-to-date. Additionally, both the FBI and US-CERT recommend that all instances of ransomware, whether affecting individuals or businesses, should be reported to the FBI’s Internet Crime Complaint Center (IC3), and victims should consider reaching out to reputable security vendors for assistance.

Responding quickly and effectively to ransomware is essential to minimize its operational impact, which can often be a highly complex undertaking if multiple systems are impacted. Unlike most security incidents involving a compromise of data, such as payment card breaches or data breaches involving personal information disclosure, ransomware attacks can leave victims with little time to decide how to respond before their operations are halted. A key reason to have a breach response plan – one that can help companies respond not only to data breaches but also
One commonality among (reported) ransomware attacks is that the monetary demands are generally not excessive, which encourages victims to pay the ransom and move on. As law enforcement guidance has noted, paying a ransom is no guarantee that the locked data or systems will be released, nor does it provide assurance that the current hackers (or, more likely, other hackers) will not come back to the well with new ransomware demanding additional payment. When facing a ransomware attack, the seemingly low cost of remediating the issue mixed with the added stress of having a suddenly nonoperational business makes it a worthy consideration to have, and test, a ransomware response plan before an attack occurs.

The operational risks associated with ransomware (as well as other types of malware that impact data and system availability, such as wiper malware) have not gone unnoticed by regulators. The European Union, for instance, will soon finalize the Network and Information Security Directive, which will require certain operators of “essential services” and “digital service providers” (e.g., online marketplaces, search engines and cloud computing services), among others, to implement “appropriate and proportionate technical and organizational measures to manage the risks posed to the security of networks and information systems,” including ensuring the “continuity of those services.” This would likely include managing risks posed by attacks similar to ransomware, which often impacts continuity of services. (Germany passed a similar law last year.) In the United States, the National Institute of Standards and Technology released a voluntary Cybersecurity Framework in 2014 that encourages entities to ensure that “information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.”

By threatening the availability of core business operations, ransomware fits neatly within the set of concerns addressed through the idea of “security resilience,” which is of particular importance to critical infrastructure and other entities that require highly available operations. Resilience is based on the ability to withstand or quickly recover from incidents with severe operational impacts, including malware attacks, and encompasses functions related to business continuity and disaster recovery. Traditional elements of resilience include infrastructure redundancy and robust backup and backup testing processes. These tools – particularly performing regular backups of critical data – are often recommended by security experts as a backstop measure against ransomware.

Organizations that are highly dependent on the availability of data and electronic systems should treat ransomware as a real and serious risk to their operational viability, and consider it within their enterprise and cyberrisk management processes. Ransomware and other malware with potentially severe operational impacts are becoming increasingly widespread and – as the hospital attacks show – dangerous and costly. If 2016 is the Year of Ransomware, it should also be the year that entities take steps to prepare against attacks that impact the availability of data and system operability – not only in the face of a ransomware attack, but also to face whatever 2017 has in store.

Recent U.S. Department of Education Dear Colleague Letter Raises the Bar on Standards for Protecting Federal Financial Aid Data


On July 1, 2016, the U.S. Department of Education issued a follow-up Dear Colleague Letter to the Dear Colleague Letter of July 29, 2015. This most recent letter reminds institutions of their legal obligation to protect student data under Title IV and sets forth the new standards and methods the DOE will use when evaluating data security compliance.

An institution’s Title IV Program Participation Agreement (PPA) requires that they must protect all student financial aid data. The Student Aid Internet Gateway (SAIG) Enrollment Agreement, the system used by educational institutions and third-party servicers to exchange data electronically with the U.S. Department of Education, contains similar requirements.

In addition, the letter reminds institutions that the specific requirements of the Gramm-Leach-Bliley Act (GLBA) governing data security at financial services organizations apply to post-secondary institutions. These include implementing a written information security program, designating an individual to coordinate information security, performing ongoing risk assessments, and properly vetting third-party service providers. It is also noted that compliance with the GLBA will be incorporated into the DOE’s annual student aid compliance audit requirements.
Most significantly, the letter “strongly encourages institutions to review and understand the standards defined in NIST SP 800-171.” These standards were developed by the National Institute of Standards and Technology (NIST) to protect sensitive federal information that is used and stored in non-federal information systems and organizations. NIST SP 800-171 sets forth a significant expansion of the data security requirements and controls expected in the handling of student financial aid data and other types of federal data and information. In citing these standards, the DOE acknowledges “the investment and effort by institutions to meet and maintain the standards set forth in NIST SP 800-171” but “strongly encourages those institutions that fall short of NIST standards to assess their current gaps and immediately begin to design and implement plans to close those gaps using NIST standards as a model.”

The message from the US DOE is clear – institutions of higher education that use student financial aid data, and other forms of federal data are expected to “immediately” begin to integrate the specific requirements of NIST SP-171.

OnLine Education

Education Department Proposes Rules to Clarify State Oversight of Online Courses


The U.S. Department of Education is proposing further regulations for online-education programs at colleges and universities, the department said in a news release on Friday.

The department’s new regulations, which follow rules that took effect last summer, would make state-authorization requirements, which vary by state, more clear for institutions that offer online courses.

Among the most notable changes, colleges that offer online courses would have to be authorized by each state in which they enroll students, if the states require such authorization. The new regulations would close what’s been described as a loophole in which distance-education providers enroll students in states where the institutions are not located, the agency said.

States would also be required to document how they process and resolve student complaints about distance-education classes.

The agency will accept public comment on the proposed regulations until August 24, and it expects to issue a final version before the end of the year.
SUMMARY

Following are excerpts from news articles having a risk management or compliance impact. The full article may be seen at the referenced source (some may require subscription to access). Topics for this month include the following:

- ADA Compliance
- Campus Safety
- False Claims Act
- HIPAA
- Information Security
- Stark Law Compliance

ADA Compliance

10 Ways to Bolster Crisis Communications Planning

*University Business* – July 2016

At one university, a garbage can blocked access to the paper towels, a table was placed in front of the automatic door button, students in wheelchairs couldn’t access the accessible sink in a science lab because of a trash can’s placement, and staff sometimes plowed snow into disabled parking spaces or access lanes.

At another institution, a professor banned all laptops, except those used by students with disabilities to take notes in class. When other students asked for an explanation, the professor violated privacy by revealing that the laptops were an accommodation for disabled students.

These common oversights can occur even on campuses where leaders believe they have complied with the Americans with Disabilities Act and Section 504 of the Rehabilitation Act. To avoid running afoul of the law, constant vigilance and ongoing review are essential because there are so many factors to consider—from what the law covers to how to best put accommodations into practice.

Nuts and bolts of ADA

The ADA requires U.S. colleges that receive federal funds to provide the accommodations students need to live and learn on campus. Some 11 percent of undergraduates report disabilities, and an unknown number never declare them. “We believe there are a lot more students with disabilities who probably could identify,” says Michael Hudson, director of the Resource Center for Persons with Disabilities at Michigan State University. “They’re still facing stigma. They don’t want to be different.”

Hudson estimates that 75 percent of the students he works with have invisible disabilities, such as anxiety, attention deficit hyperactivity disorder, dyslexia, autism spectrum disorder and food or environmental allergies.

The law defines a disability as a physical or mental impairment that lasts longer than six months and substantially limits one or more major life activity, including learning, eating, sleeping, seeing, hearing, walking, standing, communicating or concentrating.

Unlike in K12 education, where school districts must provide accommodations for all students with disabilities, higher ed institutions are required to support only students who report a disability and request help.

The ADA mandate applies to college-sponsored activities on and off campus, including internships.

Universal design’s time

The best institutions believe in the spirit of the law—not only accepting it but being happy it’s there, says Bea Awoniyi, board chairman of the Association on Higher Education and Disability (AHEAD) and assistant vice president of student affairs at Santa Fe College in Florida.
In other words, they think big and broad when it comes to the ADA.

“Universal design” involves putting measures in place to serve all kinds of students, adds Claire Hall, a higher education attorney and principal of UECAT Compliance Solutions, a Rhode Island-based consulting firm.

One example of universal design is when a campus dining facility provides gluten-free and nut-free options at every meal, so those with celiac disease and nut allergies don’t have to take extra steps just to eat.

Implementation requires educating your entire campus community (via the disabilities services office)—and it works best when there’s buy-in from the top.

While experts say there’s no data to quantify what percentage of higher ed institutions practice universal design, its principles are certainly getting attention.

“We do see a significant upswing in the interest and the application,” says David Gordon, spokesman for the Center for Applied Special Technology, a nonprofit focused on universal design for learning. “Increasingly, institutions from PK-20 are understanding that their assessments, materials and even their learning goals need to be flexible enough to recognize the great human variability that the neurosciences and other learning sciences are revealing every day.”

It takes a campus

Besides the disabilities office, the list of campus departments that may be involved in providing accommodations is long—including facilities, athletics, academics, information technology, residence life, dining, student affairs, campus safety, admissions, the bursar’s office, study abroad and career services.

Marist College in New York has a behavioral intervention team with 16 people from multiple departments to help prevent students from falling off the radar. Recently, a student was distraught because of academic troubles and a computer problem that caused registration delays, resulting in him being blocked out of a class he needed.

Two staff members who saw he was upset called the special services office for guidance, says Patricia Cordner, assistant dean for student affairs and interim director for special services. Staff in the counseling office helped him put things in perspective, and a conversation helped work things out with a professor.

At institutions that are regarded as ADA compliance models, disability services directors don’t just preach to the choir. They ensure that part of new hire orientations across campus include an overview of ADA and related staff responsibilities.

Sue Ackerman, disabilities services director at Rochester Institute of Technology in New York, routinely meets with faculty to support the notion that accommodating students with disabilities doesn’t mean giving them an unfair advantage.

At most colleges, new students discuss past accommodations with the disabilities services or health services office, which then creates a plan in collaboration with other departments. For example, a student with allergies and asthma may need to be housed in an air-conditioned room without carpeting.

The faculty has some discretion as to how needs are met; for example, if a student needs extra time on a test, the professor could stay in the classroom with the student for the extra time or have the student take the test at the disabilities services office.

Creative problem-solving

A vast majority of students need only routine accommodations, such as extra time for test-taking, assistance from note-takers or moving a class to an accessible building. Yet requests for accommodations must be considered individually.

Emerging challenges for universities include grappling with accommodations for students with severe allergies or chemical sensitivities, says Deborah Demille-Wagman, director of Academic and Disability Support at American University in Washington, D.C. “Such requests often include asking that we control the behavior of others.”

The aim is to respect all students’ rights. For example, when a student has a severe chemical sensitivity to fragrances, it’s impossible to require all people on campus to avoid scented products, says Demille-Wagman.
But the university can work with the student to ensure that classrooms are well ventilated, classmates and faculty are asked to refrain from using fragrance, and the student can take a break from the classroom or miss class, if necessary.

A growing number of students with documented anxiety disorder or other mental illness are requesting—and getting approval for—an emotional-support animal (typically a dog or cat) in the dorm. Aaron Spector, director of Disability Resources and Services at Temple University in Philadelphia, suggests that institutions develop policies and procedures to guard against complaints of discrimination or favoritism, as Temple has.

Since there are also students allergic to dogs and cats, schools are obligated to find a way to accommodate both groups, notes Hall of UECAT Compliance Solutions.

And the law requires that accommodations be made regardless of cost.

A few years ago, a blind student at Michigan State approached Hudson, who is also blind, to say she wanted to major in computer science, even though she knew the heavy amount of math required would necessitate extensive accommodations.

“It involved a lot of hard work on her part and ours,” he says.

Disability services worked with the physics and engineering departments to create 3D models that she could touch in order to learn the physics concepts. Using existing equipment, the university made textbooks in braille, adding 2D graphs, line drawings and diagrams that she could touch. They used an adaptive device that looks like a clip board covered with a thin piece of plastic; when she drew on it with a special pen, the line became raised.

As she advanced through her courses, the university brought in consultants as needed, Hudson says. The school also trained students in the honors program to help devise creative tools. One low-tech solution involved sticking pins into a board and connecting the pins with string.

The student wound up graduating with a computer science degree in four years and is now working at Apple, helping with product accessibility.

What’s not required

Colleges and universities must try to level the playing field for those with disabilities. But they don’t have to give these students an academic advantage or extra perks.

A student in a wheelchair, for instance, may reasonably receive a room on the first floor to ensure safe exit in the event of a fire, but the university need not honor a student’s request to get into a particular high-demand dorm if needs can be met elsewhere.

Less expensive remedies are also allowed. For a hearing-impaired student, for example, a college can install a bed-shaker, rather than the costlier flashing lights a student might request, to alert that the fire alarm has gone off.

Rather than looking at serving disabled students as a burden, the situation can be approached as an opportunity to prepare all students for the diverse world of work, says Awoniyi. “Many people want diverse populations,” she says. “The best universities and colleges think of disability as an aspect of diversity.”

Technological challenges and tools

As technology evolves, it poses new challenges to ADA compliance. For example, more than 90 percent of 20 top college websites studied by Perkins Solutions, a digital accessibility consulting firm, failed to meet some or all of the guidelines that make websites accessible to users with disabilities.

People with disabilities use assistive technology such as screen readers, text enlargement or voice-command programs. But behind-the-scenes coding can block these applications, says Bill Oates, vice president of Perkins Solutions, a subsidiary of Perkins School for the Blind in Massachusetts.

On a website, all users should be able to play and stop a video, stop screens in a slideshow from changing before the user has finished reading the text, and turn captions on or off. To comply with ADA, institutions need to ensure that online courses as well as websites used by prospective and existing students and staff are accessible to all.
Campus Safety

10 Ways to Bolster Crisis Communications Planning


There is never downtime in higher education—there’s simply a shift in priorities. The summer months provide an opportunity for strategic planning, reporting, advancing new initiatives and connecting more deeply with colleagues. It’s also a valuable time to reflect on crisis communications. We know crises can occur at any time, but the summer months may provide a reprieve as the campus activity slows down during this period.

The last step of any crisis communications plan should be to review the work of the team and make adjustments to improve communications in the future. The following 10 recommendations for crisis communications are the result of this review process and could be useful for PR professionals and communications offices at higher education institutions.

1. **Update your crisis communications plan, and review it. Repeat.**
   Ask yourself who knows the plan and who has reviewed it recently. Oftentimes this work gets put on the backburner because there are other actionable and immediate priorities being worked on—commencements, recruitment events and overall managed chaos throughout the semester. Take the time to read through your plan and make revisions that are relevant to your environment (e.g., are there new staff on the institution’s crisis response team or has your institution implemented a new text messaging platform that needs to be incorporated into the plan?).

2. **Be prepared.**
   Think about crisis communications and management often, so when the inevitable happens on your campus or shows up in your inbox, you aren’t wasting time thinking about what needs to happen and how to respond effectively. A crisis will never go as planned, but doing as much proactive planning in advance of a crisis will go a long way. Consider different scenarios, such as sexual assault, student behavior issues, town/gown relations and litigation, and then map out how to best respond.

3. **Assess the situation thoroughly and quickly.**
   The crisis response team needs to act with a sense of urgency. Make sure communications has a seat at the table when issues are being assessed. It’s important to review the issue/crisis from all angles and understand the opportunities to address it. Input from the entire crisis team is invaluable as it provides a more comprehensive perspective and can elevate anticipated reactions and possible new challenges, as well as opportunities.

4. **Communicate in a timely manner and with purpose.**
   What’s the message, who needs to know and when? Being proactive, open and transparent can help build good will. Recognize what information stakeholders need to hear and want to hear as part of message development. Remember faculty, staff and students first. Alumni and donors are a close second and will likely have a strong reaction based on the institution’s response and what is reported in the news. Be responsive to media and communicate key messages to better manage reputation and risk.

5. **Show compassion.**
   Make sure your communications are genuine and empathetic, not cold and corporate. Reflect your institution’s culture and have an authentic voice. You will gain increased support and it may help move your organization away from the issue at hand.

6. **Understand the broader context.**
   Obviously, the issue at hand is the focus, but knowledge of the surrounding environment is important. It’s helpful to know if the issue is one of several, a standalone, first in the region or a national issue. Knowing about other issues taking place on campus and any upcoming events (e.g., admissions and alumni) are factors to consider.

7. **Partner with legal.**
   It’s critical that legal counsel weigh in on all communications and is included in strategy and planning meetings. They bring sound guidance and perspective around current and future litigation concerns and have deep knowledge around the issue, and potentially others, to help shape messaging. It’s also important to maintain confidentiality and privileged communications. A strong relationship will elevate thinking around other considerations to factor into what can and cannot be said.
8. Listen to the dialogue taking place around you.
Be mindful and attentive to what’s being said about the crisis, the concerns being raised and any rumors, especially as they can snowball quickly. On a college campus, the buzz can happen almost immediately. Monitor social media channels and the media, including comments to stories. This understanding will help head off any growing concerns and misinformation and put the institution in better control of the narrative that will be communicated through holding statements, talking points, audience-specific communications, Q&As and other materials.

9. Activate a social media plan.
Social media can add to the 24/7 frenzy. It’s important to listen to the conversations taking place and design an appropriate engagement strategy. It could run the gamut from posting all communications and responding to posts, to going quiet and communicating directly with a follower. Know all of your channels—from the Dean’s Office to athletics—and which matter most. Make sure there is clear communication with these groups in advance of a crisis, about strategy, how they can support efforts and what actions are acceptable. Finally, make sure any current content being posted does not come across as insensitive in the context of the current issue.

10. Identify and train your media spokesperson.
Put yourself in the shoes of the stakeholder to determine the optics of a message being delivered by different people. This exercise will help identify the most appropriate spokesperson. Also, college presidents can benefit from training just as much as deans and other divisional leaders. The time to do it is now.

False Claims Act

Hospital Network Paying $2.5M to Settle Overbilling Claims


The University of Pittsburgh Medical Center has paid $2.5 million to settle some claims in a federal whistleblower lawsuit accusing the hospital network of overbilling government insurance programs for neurosurgery.

UPMC, Pennsylvania's largest private employer with 60,000 workers, didn't acknowledge wrongdoing in the settlement announced Wednesday by the U.S. Attorney's Office in Pittsburgh. The nonprofit reported $12 billion in revenue last year.

The federal government sued last year after two doctors and another whistleblower sued in 2012 alleging various kinds of inflated billing. Some of the whistleblower claims remain and will be pursued privately, and UPMC said it would defend those claims "vigorously."

The claims settled primarily involve the way UPMC billed for surgeries in which some of its doctors acted as first assistants or teaching assistants on surgical procedures. Under regulations governing Medicare, Medicaid, Tricare/Champus and other federal programs, those assisting physicians must spend a certain amount of time or perform specific roles during surgery, otherwise UPMC cannot bill for their services.

The lawsuit claimed UPMC billed for the assistant services when those doctors didn't meet the criteria and sometimes even when they weren't present at all.

UPMC "created a culture where money — not medicine — drove the decision-making process," the lawsuit said.

The lawsuit didn't say how much money the overbilling allegedly cost the government programs or how the feds arrived at the $2.5 million settlement figure. UPMC didn't address that issue in its statement.

But the lawsuit also alleged UPMC was a "repeat offender" with regard to billing for surgeries performed by residents, fellows or physician assistants when no teaching physician oversaw the procedures.

UPMC paid the government $17 million in 1998 after an audit by the U.S. Department of Health and Human Services uncovered that specific type of overbilling, but this earlier settlement "obviously did not constitute a sufficient deterrent to forego its clearly fraudulent billing practices," the lawsuit said.

UPMC issued a statement saying Wednesday's settlement "wraps up" the government's investigation of billing to Medicare, Medicaid and Tricare.
"UPMC learned that some of the billing these entities submitted did not accurately reflect the services performed, and resulted in more reimbursement than was due. The physicians themselves did not submit these bills," the statement said. "UPMC discovered the billing discrepancies, disclosed the errors to the United States Attorney's office, conducted an internal review, and fully cooperated with the government's review."

UPMC has since taken steps to fix its billing process and practices.

The remaining claims to be pursued in non-government lawsuits largely concern something known as Relative Value Units. Those are numerical units that the government uses to "score" the complexity of a surgical procedure and the amount of time it requires.

Relative Value Units are also used to calculate bills for surgical procedures, and the lawsuit contends UPMC inflated or over-reported those scores to drive up its revenue and to overpay some surgeons, giving those doctors an incentive to over-report their surgical work.

**HIPAA**

**Almost 30 percent of hospitals out of compliance with HIPAA requirements for contingency plans for their EHRs**


*Testing and revision plans lacking, as well as staff training on how to deal with EHR system downtime, Office of the Inspector General report says.*

While most hospitals have contingency plans in place in case something happens to their electronic health records, less than three-quarters of those surveyed by the Department of Health and Human Services' Office of the Inspector General have plans that address testing and revision procedures -- a requirement under the Health Insurance Portability and Accountability Act.

About 68 percent of hospitals had contingency plans that complied with all four HIPAA requirements: testing and revision procedures, an emergency mode operations plan, a disaster recovery plan and a data backup plan. Ninety-five percent of hospitals had plans addressing disaster recovery and emergency mode operations; 83 percent had a data backup plan.

Findings in the OIG report underscore the importance of more hospitals adopting testing and revision procedures. The government, healthcare and information technology sectors have raised concerns about vulnerabilities in networked medical devices that have the potential to put hospital networks and EHR systems at risk, the OIG found.

For instance, in January, a California hospital reported that it suffered a ransomware attack that disabled its network and EHR system for about a week, leading to delayed patient care and the need to divert patients to other facilities. And in March, MedStar Health reported a suspected ransomware attack that forced it to take computer systems offline throughout its entire system, including 10 hospitals.

In fact, over half of hospitals reported an unplanned EHR disruption, and about a quarter of those experienced delays in patient care as a result.

Of the 73 percent of hospitals who reported having testing and revision procedures in place, only 45 percent of them said they trained staff through recommended drills on how to deal with EHR system downtime. One hospital reported it avoided drills because of the risk to patient safety from unnecessarily shutting down EHR systems.

The Office for Civil Rights enforces HIPAA's security rule, but the OIG report found that the OCR considers HIPAA compliance broadly, and doesn't target EHRs when reviewing a covered entity's contingency plans. Oversight of HIPAA compliance is generally triggered when the OCR becomes aware of specific problems, such as breached and complaints.

Based on those findings, the OIG repeated its previous recommendation that the OCR fully implement a permanent audit program to assess compliance with HIPAA requirements.
Five myths about patient privacy


Shortly after the recent massacre at an Orlando nightclub, the city’s mayor declared that the White House had agreed to waive federal privacy rules to allow doctors to update victims’ families. News of the waiver was widely reported, but as the Obama administration later clarified, both the mayor and the media were “simply mistaken.” No waiver was granted because none was needed. The confusion amid the tragedy in Orlando underscores widespread misconceptions about the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Here we shed light on a handful of myths that bedevil doctors and patients alike.

**Myth No. 1 - HIPAA prohibits communicating with patients’ loved ones.**

HIPAA sets national standards to safeguard the privacy of individuals’ health information. As in Orlando, it is often perceived as a barrier to effective communication between doctors and patients’ loved ones. Virginia state Sen. Creigh Deeds — whose mentally ill son attacked him before committing suicide in 2013 — recently testified before Congress that “HIPAA prevented me from accessing the information I needed to keep him safe and help him towards recovery.” Such stories are heart-wrenching but misattributed to HIPAA. In most cases, the privacy regulation permits doctors and nurses to communicate with a patient’s family, friends or caretakers. The rules were crafted to account for the realities of health care, including the integral role often played by those closest to the patient.

As the former head of HIPAA enforcement told Congress, “HIPAA is meant to be a valve, not a blockage.” When the patient is present and clearheaded, the law allows hospitals to share relevant information with loved ones so long as the patient does not protest. This can be accomplished through the patient’s agreement or acquiescence, or based on a doctor’s professional judgment that the patient does not object. If a person accompanies the patient to an appointment, for example, doctors can reasonably infer that discussing the patient’s treatment in front of that individual is appropriate.

When the patient is unavailable or incapacitated, doctors can also exercise professional judgment to determine whether disclosure is in the patient’s best interests. A clear example is when the patient is unconscious, but this provision can also apply if the patient is suffering from temporary psychosis and lacks the ability to make health-care decisions.

Still, studies have shown that confusion and fear over privacy laws often lead hospitals to unnecessarily withhold information and reflexively cite HIPAA as justification — an approach that can make families feel locked out of care. But overall, HIPAA affords doctors significant flexibility to communicate with patients’ loved ones, whether about routine or time-sensitive matters. The only time the law truly forecloses the sharing of such information is when the patient is present, lucid and tells doctors not to — and even then, patients’ wishes can be overridden in the event that they pose a serious and imminent threat to health or safety.

**Myth No. 2 - Same-sex marriage rights are critical to equality under HIPAA.**

Before the rumors of a HIPAA waiver in Orlando were quelled, various news outlets reported that it marked a “victory for gay rights.” Waiving medical privacy laws was portrayed as a prerequisite for sharing information with same-sex partners.

In reality, HIPAA enables discussions with relatives, friends or anyone else identified by the patient, meaning that the impact of the Supreme Court’s marriage-equality rulings on permissible communication was marginal at best. HIPAA does not require doctors to obtain proof of identity when inquirers say they are a patient’s friends or relatives. Providing information to family and friends under HIPAA is linked to their involvement in the patient’s medical affairs, not the legal status of their relationship. Patients’ sexual preferences were irrelevant long before same-sex marriage became the law of the land.

Early in his administration, President Obama emphasized the importance of hospital visitation rights for same-sex partners and sought to enforce this policy through Medicare rules. However, spouses — unlike parents vis-a-vis their minor children — are not automatically presumed to have access to patient records. It is up to the patient to designate them or doctors to involve them as clinically appropriate.
Myth No. 3 - HIPAA provides extra protections for mental health information.

Rep. Tim Murphy, also a psychologist from Pennsylvania, believes that amending HIPAA is crucial to mental health reform. Rep. Eddie Bernice Johnson, a registered nurse from Texas, says that “individuals with mental illness and substance use disorders often face obstacles to treatment because of the Privacy Rule within HIPAA.” New York’s chief psychiatrist has described HIPAA as “the tragedy of mental health law.”

Yet HIPAA does not distinguish between physical and mental health information, nor does it provide extra protections for the latter. Indeed, HIPAA is generally agnostic as to the type of health information being protected. The drafters of the privacy regulation acknowledged that many states had laws specifically guarding records related to mental illness and “other stigmatized conditions” but declined to follow their lead. While the HIPAA rules in no way erode these additional state protections, they do not confer any special status on mental health information.

The rare instance in which HIPAA affords greater protection to sensitive information involves “psychotherapy notes.” However, this exception is much narrower than is commonly understood. Psychotherapy notes are therapists’ private, desk-drawer notes reflecting on conversations during counseling sessions. They exist for therapists’ personal use as memory joggers and must be kept separate and apart from patient charts in order to retain their designation. Any information of wider utility — such as treatment or diagnosis — is excluded from the definition and associated protections. In fact, a main reason psychotherapy notes are shielded from disclosure is because they would have so little relevance or use to anyone other than the doctor who created them.

Myth No. 4 - HIPAA stops doctors from reporting threats.

Mass shootings involving mentally ill suspects often prompt discussion about what warning signs doctors should have reported. These questions persist even in cases when doctors had alerted authorities, as happened before the 2012 movie theater tragedy in Aurora, Colo.

After the Sandy Hook Elementary School shooting, one of Obama’s 23 executive actions was to clarify that “no federal law” prohibits health-care professionals from reporting threats of violence to the police. This mandate was accomplished via an open letter to the health-care community explaining that HIPAA allows doctors to issue appropriate warnings when they believe that patients present a serious and imminent threat to themselves or someone else. In such cases, doctors can disclose necessary information to law enforcement, school officials, family members, the target of a credible threat or anyone else in a position to avert the danger. Under the HIPAA rules, doctors who take these steps are generally presumed to have acted in good faith.

When patients make threats or pose a high suicide risk, doctors often have a “duty to warn” emanating from state laws, court decisions or professional ethics rules. HIPAA does not in itself impose such a duty, but it explicitly permits health-care professionals to take action “consistent with” these standards.

Myth No. 5 - HIPAA is the reason for medical privacy.

HIPAA is often singled out as the basis of patient confidentiality. Yet privacy was a core value in health care long before the HIPAA rules were promulgated in the early 2000s. The Hippocratic Oath admonishes doctors to keep secret what they “see or hear” from patients. The American Medical Association’s first code of ethics, adopted in 1847, emphasized the “obligation of secrecy” at the heart of the doctor-patient relationship.

In practice, HIPAA provides a federal floor of privacy protections, not a ceiling. It defers to state laws that are “more stringent” or protective of patient rights. State laws that create additional safeguards for conditions deemed especially sensitive — whether HIV/AIDS, communicable diseases, cancer or mental illness — remain in full force. Neither does HIPAA override other federal laws. Thus, for example, substance-abuse programs subject to 1970s-era federal confidentiality requirements continue to follow those stricter standards in the vast majority of cases.

Even where HIPAA allows health information to be shared, it almost never requires it. Doctors and hospitals must still be cognizant of other applicable laws or professional ethics guidelines that impose stricter limitations. HIPAA is designed to align with these obligations as often as possible, but those instances where gaps arise tend to be the most complex and emotionally fraught.

HIPAA established a procedural framework for doctors, hospitals and other health-care players to exchange information without compromising patient privacy. Even if the law disappeared tomorrow, the legal precepts and ethical norms that long preceded it would remain in place — as would many of the frustrations cited by HIPAA’s
most ardent detractors. This month, the House of Representatives proclaimed that “there exists confusion in the health care community around what is currently permissible under HIPAA rules.” Alas, that just may be the most accurate statement about HIPAA ever uttered.

Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center


The University of Mississippi (UM) Medical Center (UMMC) has agreed to settle multiple alleged violations of the Health Insurance Portability and Accountability Act (HIPAA) with the U.S. Department of Health and Human Services Office for Civil Rights (OCR). During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach, due largely to organizational deficiencies and insufficient institutional oversight. UMMC will pay a penalty of $2,750,000 and adopt a corrective action plan to help assure future compliance with HIPAA Privacy, Security, and Breach Notification Rules.

On March 21, 2013, OCR was notified of a breach, after UMMC’s privacy officer discovered that a password-protected laptop was missing from UMMC’s Medical Intensive Care Unit (MICU). UMMC’s investigation concluded that it had likely been stolen by a visitor to the MICU who had inquired about borrowing one of the laptops. OCR’s investigation revealed that ePHI stored on a UMMC network drive was vulnerable to unauthorized access via UMMC’s wireless network, because users could access an active directory containing 67,000 files after entering a generic username and password. The directory included 328 files containing the ePHI of an estimated 10,000 patients dating back to 2008.

Further, OCR’s investigation revealed that UMMC failed to:

- implement appropriate policies and procedures to prevent, detect, contain, and correct security violations;
- implement physical safeguards for all workstations that access ePHI to restrict access to authorized users;
- assign a unique user name and/or number for identifying and tracking user identity in information systems containing ePHI;
- and notify each individual whose unsecured ePHI was reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach.

UM is Mississippi’s sole public academic health science center, with education and research functions in addition to providing patient care in four specialized hospitals on the Jackson campus and at clinics throughout Jackson and the State. Its designated health care component, UMMC, includes University Hospital, the site of the breach in this case, located on the main UMMC campus in Jackson.

OCR audits involve 180 new protocols

On the Front Lines - Wolters Kluwer Health News Update

The HHS Office for Civil Rights (OCR) could be auditing Health Information Portability and Accountability Act (HIPAA) (P.L. 104-191) covered entities (CEs) and business associates (BAs) based on 180 new areas of inquiry by the end of summer 2016. Kelly McLendon, RHIA, CHPS, Managing Director of CompliancePro Solutions, told an audience at a Health Care Compliance Association (HCCA) webinar titled, "OCR Phase 2 Audit Program Update: 180 New Audit Protocols," that the protocols could have more than 1,000 questions associated with them. He urged CEs and BAs to prepare for deep audits and be ready to submit significant documentation demonstrating compliance with the HIPAA Privacy, Security, and Breach Notification rules.

Initial questionnaires. In March 2016, the OCR announced its intention to conduct 200 Phase 2 audits by the end of the year (see HIPAA Phase 2 audits are here: be prepared, March 24, 2016). It has begun sending identifying questionnaires to CEs to make sure that it has accurate contact information for the entities. These questionnaires issued as a series of emails, with one identifying the correct point of contact, another asking for pertinent information about the CE, and a third asking for information about the CE’s BAs; the questionnaire related to BAs, alone, asks for 27 fields of information per BA. The agency is rumored to plan to send audit notification letters at the end of the summer,
McLendon emphasized the need to respond to all questionnaires in a timely manner, but suggested that organizations respond later in the allowable timeframe to possibly allow themselves additional time to prepare for potential audits.

**New protocols.** The OCR updated its audit protocols and categorized each area of inquiry as focused on privacy (89), security (72), or breach (19). The agency has indicated that it will not audit any CE or BA on all 180 protocols, but has made no indication as to how many protocols may be involved in each audit. McLendon suspects that audits will focus on no more than 10 to 20 protocols, since each one may have five to 20 questions associated with it. He hazarded a guess that all organizations will be audited on hot topics, including breach, patients’ access to their own protected health information (PHI), and mobile devices; however, the OCR has not provided an indication as to other areas of focus.

**Documentation.** McLendon noted that all protocols will require organizations to obtain and review policies and procedures regarding the area of inquiry, such as a privacy inquiry regarding a patient’s right to access his or her own protected health information (PHI). Every policy must have written procedures attached to it in order to satisfy the OCR. In addition, CEs and BAs must evaluate compliance with performance criteria and determine whether policies and procedures adequately address the area of inquiry. Documentation is paramount in these "deep" audits. With respect to patient’s right access, for example, the OCR will want to review documentation regarding the handling of requests that were both granted and denied, requests that were granted in part and denied in part, and ensuring that information was provided in the requested form and format.

While the OCR considers privacy extremely important, "Security is a bear," McLendon said. "The amount of documentation you have to produce on the security side is massive." In discussing an area of inquiry involving mobile devices, for example, he emphasized the documentation involved in demonstrating that a CE or BA has tracked all hardware and electronic media containing PHI. Many protocols also have language listing "elements to review" and suggesting that they "may include but are not limited to" the items suggested, allowing for the possibility of even more documentation.

McLendon discussed a breach area of inquiry involving risk assessments. To emphasize how deep the audits will go, he noted that the OCR may wish to sample the organization’s methodology for determining whether a breach has occurred that requires notification and suggested that the agency may wish to review 10 out of 100 examples.

McLendon also emphasized the need to respond to documentation requests in any area. If the OCR asks for information on events that occurred in a two-year time period, for example, and the CE or BA does not believe that any such events occurred, it should go back further in time until it is able to provide information about how it handled the events at that time.

**Impending audits.** The OCR plans to complete 200 audits by the end of 2016. The majority will be desk audits, but it is unclear how many onsite audits will occur. Furthermore, the OCR has not stated whether BA audits will be counted in that number or whether they will be completed in 2016. Since this is the first time the agency is auditing BAs, it is unclear how those audits will proceed. McLendon stressed the need for all organizations to be prepared for audits. He reminded listeners that entities responding to OCR complaints will need to provide the same type of information requested in an audit. It is also possible that information provided by organizations responding to initial questionnaires in 2016 may be used to select them for audits in 2017 and beyond. Entities should prepare right away. As McLendon said, "Phase 2 is here."

---

**Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University**

*HHS Office for Civil rights in Action – July 18, 2016*

Oregon Health & Science University (OHSU) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules following an investigation by the U.S. Department of Health and Human Services Office for Civil Rights (OCR) that found widespread and diverse problems at OHSU, which will be addressed through a comprehensive three-year corrective action plan. The settlement includes a monetary payment by OHSU to the Department for $2,700,000.
OCR’s investigation began after OHSU submitted multiple breach reports affecting thousands of individuals, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive. These incidents each garnered significant local and national press coverage. OCR’s investigation uncovered evidence of widespread vulnerabilities within OHSU’s HIPAA compliance program, including the storage of the electronic protected health information (ePHI) of over 3,000 individuals on a cloud-based server without a business associate agreement. OCR found significant risk of harm to 1,361 of these individuals due to the sensitive nature of their diagnoses. The server stored a variety of ePHI including credit card and payment information, diagnoses, procedures, photos, driver’s license numbers and Social Security numbers.

OHSU performed risk analyses in 2003, 2005, 2006, 2008, 2010, and 2013, but OCR’s investigation found that these analyses did not cover all ePHI in OHSU’s enterprise, as required by the Security Rule. While the analyses identified vulnerabilities and risks to ePHI located in many areas of the organization, OHSU did not act in a timely manner to implement measures to address these documented risks and vulnerabilities to a reasonable and appropriate level. OHSU also lacked policies and procedures to prevent, detect, contain, and correct security violations and failed to implement a mechanism to encrypt and decrypt ePHI or an equivalent alternative measure for ePHI maintained on its workstations, despite having identified this lack of encryption as a risk.

OHSU is a large public academic health center and research university centered in Portland, Oregon, comprising two hospitals, and multiple general and specialty clinics throughout Portland and throughout the State of Oregon.

Information Security

Is Your Company Prepared for a Ransomware Attack?

Corporate Counsel – July 11, 2016

This year already appears to be the Year of Ransomware, with the healthcare industry most acutely feeling the pain inflicted by this malware species. April saw a record number of ransomware attacks in the United States.

Until recently, a layperson might understandably believe ransomware affects only individuals, not corporations, with stories circulating for several years of encrypted desktop computers being unlocked only after the unsuspecting consumer pays anonymous hackers several hundred dollars. Recent news stories indicate, however, that ransomware is now a corporate problem, too. While this might ordinarily be viewed merely as a nuisance for some entities, those that rely on the availability of data or electronic systems to perform key functions (and who doesn’t?) are faced with a grave reality: Ransomware can grind operations to a halt.

Ransomware is a type of malware that locks a device or renders its data unusable until the victim pays the attacker a ransom, often in an alternative currency known as bitcoin. According to Symantec, there are two primary categories of the malware: locker ransomware (which locks the device until the ransom is paid) and crypto ransomware (which generally encrypts individual files without locking the user out of the device entirely). Both types of ransomware ultimately deny the victim access to the data stored on the device.

Ransomware can be delivered as a malicious payload in a manner similar to any other malware, including through phishing, social engineering, malicious advertising or an existing remote-access Trojan. Once downloaded on a device, the malware generally either locks the device or quietly begins encrypting data stored on it. Many types of ransomware also seek to traverse the victim’s network in an effort to move to other systems, including storage devices and critical servers. Only once the ransom is paid does the attacker unlock the device or provide the key to decrypt data, although in some cases attackers have reportedly not carried out their end of the bargain even after being paid.

The risks posed by ransomware extend well beyond the encryption of data or locking of a device. As more and more businesses embrace data-driven processes and increase their reliance on Big Data, a ransomware infection means not only that data or systems become unavailable – it means that the business may not be able to function. Entities in nearly all sectors, including financial services, e-commerce, cloud services, and more, depend on the availability of data and systems to function and provide core services. Critical infrastructure, which is often required to provide essential services (e.g., electricity, telecommunications), also depends heavily on data and system availability. As we have seen this year, hospitals appear to be particularly vulnerable.
Indeed, 2016 kicked off with a string of ransomware attacks targeting the health care industry. In early February, Hollywood Presbyterian Medical Center in Los Angeles had to operate using paper and fax machines after a ransomware attack prevented personnel from accessing patient records and communicating electronically. Reports indicated that patients bound for the emergency room had to be diverted to other hospitals. After 10 days of functioning largely in the pre-Internet era, the hospital elected to pay a $17,000 ransom, with its president and CEO noting that paying the hackers was the “quickest and most efficient way to restore our systems and administrative functions.”

Over the next several weeks similar attacks were perpetrated against a separate California hospital group, Kentucky’s Methodist Hospital, and most recently MedStar, which operates 10 Maryland hospitals. In those attacks, the requested ransoms ranged from $1,600 to $18,500, but all entities reported that they were able to resolve the attacks without paying the hackers. Health care ransomware attacks were not limited to the United States, as the U.S. Computer Emergency Readiness Team (US-CERT) noted in an alert that healthcare entities in Germany and New Zealand faced similar attacks in early 2016.

While health care has been hit particularly hard this year, the issue pervades a broad range of industries. The U.S. House of Representatives was the target of ransomware attacks in May that required the House to lockdown parts of its network and restrict access to certain email and cloud services programs. The Federal Financial Institutions Examination Council (FFIEC) recently issued a statement warning of an “increasing frequency and severity of cyber-attacks involving extortion,” including the use of ransomware. In March, security experts notified Apple that they had discovered a ransomware program embedded in an app related to BitTorrent (the peer-to-peer data sharing system) that encrypted certain files and demanded that users send one bitcoin (valued at ~$400) to unlock the data. Before Apple was able to implement a fix, an estimated 6,500 systems were infected.

Ransomware has hit less likely targets as well, such as the Horry County school system in South Carolina, which paid an $8,500 ransom to unlock its computers. Federal agencies have been the frequent target of ransomware. According to the Department of Homeland Security (DHS), between June and December 2015 alone, 321 incidents of ransomware targeted 29 different federal agencies.

The FBI recently advised that individuals and organizations “should not pay the ransom” and highlighted that the “best way to protect yourself and your organization is to have a backup of your data, maintain it, and disconnect it from your computer.” US-CERT recently issued a ransomware alert recommending that entities take several added protective measures in addition to backing up data, including the use of application whitelisting, avoiding enabling macros from email attachments and ensuring that software patches are downloaded and antivirus programs are kept up-to-date. Additionally, both the FBI and US-CERT recommend that all instances of ransomware, whether affecting individuals or businesses, should be reported to the FBI’s Internet Crime Complaint Center (IC3), and victims should consider reaching out to reputable security vendors for assistance.

Responding quickly and effectively to ransomware is essential to minimize its operational impact, which can often be a highly complex undertaking if multiple systems are impacted. Unlike most security incidents involving a compromise of data, such as payment card breaches or data breaches involving personal information disclosure, ransomware attacks can leave victims with little time to decide how to respond before their operations are halted. A key reason to have a breach response plan – one that can help companies respond not only to data breaches but also to cyber incidents having an operational impact on data or systems – is the heightened stress company personnel face in responding to a breach. This is only exacerbated by ransomware attacks.

One commonality among (reported) ransomware attacks is that the monetary demands are generally not excessive, which encourages victims to pay the ransom and move on. As law enforcement guidance has noted, paying a ransom is no guarantee that the locked data or systems will be released, nor does it provide assurance that the current hackers (or, more likely, other hackers) will not come back to the well with new ransomware demanding additional payment. When facing a ransomware attack, the seemingly low cost of remediating the issue mixed with the added stress of having a suddenly nonoperational business makes it a worthy consideration to have, and test, a ransomware response plan before an attack occurs.

The operational risks associated with ransomware (as well as other types of malware that impact data and system availability, such as wiper malware) have not gone unnoticed by regulators. The European Union, for instance, will soon finalize the Network and Information Security Directive, which will require certain operators of “essential services” and “digital service providers” (e.g., online marketplaces, search engines and cloud computing services),
among others, to implement “appropriate and proportionate technical and organizational measures to manage the risks posed to the security of networks and information systems,” including ensuring the “continuity of those services.” This would likely include managing risks posed by attacks similar to ransomware, which often impacts continuity of services. (Germany passed a similar law last year.) In the United States, the National Institute of Standards and Technology released a voluntary Cybersecurity Framework in 2014 that encourages entities to ensure that “information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.”

By threatening the availability of core business operations, ransomware fits neatly within the set of concerns addressed through the idea of “security resilience,” which is of particular importance to critical infrastructure and other entities that require highly available operations. Resilience is based on the ability to withstand or quickly recover from incidents with severe operational impacts, including malware attacks, and encompasses functions related to business continuity and disaster recovery. Traditional elements of resilience include infrastructure redundancy and robust backup and backup testing processes. These tools – particularly performing regular backups of critical data – are often recommended by security experts as a backstop measure against ransomware.

Organizations that are highly dependent on the availability of data and electronic systems should treat ransomware as a real and serious risk to their operational viability, and consider it within their enterprise and cybersecurity management processes. Ransomware and other malware with potentially severe operational impacts are becoming increasingly widespread and – as the hospital attacks show – dangerous and costly. If 2016 is the Year of Ransomware, it should also be the year that entities take steps to prepare against attacks that impact the availability of data and system operability – not only in the face of a ransomware attack, but also to face whatever 2017 has in store.

Is your Covered Entity or Business Associate Capable of Responding to a CyberSecurity Incident?
HHS Office for Civil Rights in Action – July 2016

Computer security incident response is an important element of an information technology program. It can assist Covered Entities and Business Associates in promptly detecting breaches, decreasing loss and damage, mitigating the weaknesses that were exploited, protecting the confidentiality, integrity, and availability of data, and restoring IT services back to normal.

HIPAA defines security incidents as attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (See the definition of security incident at 45 CFR 164.304). HIPAA also identifies breaches as, generally, an impermissible acquisition, access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information. (See the definition of breach at 45 CFR 164.402).

According to a survey recently conducted, 43% of the survey respondents lack formal incident response plans and procedures, and 55% percent of them lack formal incident response teams. Also, 61% of these respondents have experienced a data breach in over the past two years, which included unauthorized access, denial of service, or malware infection. Cybersecurity-related attacks have continued to rise and become more destructive and disruptive. According to a different study, in 2014 the average cost to a company suffering a data breach affecting personally identifiable information (PII) was $3.5 million, with an average cost of $145 per individual.

With the constant upsurge of security breaches that involve cyberattacks and as required by the HIPAA Security Rule, Covered Entities and Business Associates should have security incident response capabilities established. Although effective incident response planning can be a complex task, it should be one of Covered Entities’ and Business Associates’ priorities.

When establishing incident response capabilities, Covered Entities and Business Associates should consider:

- **Developing incident response policies, plans, and procedures**
  
  An incident response policy assists Covered Entities and Business Associates in having a proper, concentrated, and coordinated approach to responding to incidents. The incident response plan should provide a roadmap for implementing the entity’s incident response capabilities. The plan should also meet the Covered Entities’ and
Business Associates’ distinctive requirements that relate to their mission, sizes, structures, and functions, and identify the necessary resources and management support. Incident response policies and plans should be approved by management and reviewed on an annual basis.

The incident response procedures should be based on the incident response policy and plan. Incident response procedures are outlines of the specific technical processes, tools, techniques, and forms that are utilized not only by the incident response team, but also by staff who need to report an incident. These procedures should include the entity’s processes for:

- preparing for incidents;
- detecting and analyzing incidents;
- containing, eradicating and recovering from incidents; and
- conducting post-incident activities and reviews.

**Building relationships and setting up plans for communicating with internal and external parties regarding incidents**

Building relationships and lines of communication between the incident response team and other groups, both internal and external can be challenging. Covered Entities and Business Associates should plan the communication with these groups before an incident occurs.

Before establishing incident response policies and procedures, the incident response team should first develop relationships and lines of communication with internal groups within its organization, such as the IT department, public affairs office, legal department, internal law enforcement, and management.

Also, the incident response team should discuss with its entity’s public affairs office, legal department, and management about sharing information with external groups. Covered Entities and Business Associates are often required to communicate with external parties regarding an incident and should comply whenever applicable. External parties could consist of federal agencies, law enforcement, media, internet service providers (ISPs), vendors, or other incident response teams.

**Staffing and training**

Covered Entities and Business Associates should staff their incident response team with people who have the appropriate skillsets. These skills could include network administration, programming, technical support, intrusion detection, and CyberSecurity forensic analysis; team members should also possess teamwork and communication skills.

Furthermore, incident response team and staff members should be provided with the necessary training to be effective in their roles, and to carry out their responsibilities during an incident or when an incident is suspected.

**Recent U.S. Department of Education Dear Colleague Letter Raises the Bar on Standards for Protecting Federal Financial Aid Data**

On July 1, 2016 the U.S. Department of Education issued a follow-up Dear Colleague Letter to the Dear Colleague Letter of July 29, 2015. This most recent letter reminds institutions of their legal obligation to protect student data under Title IV and sets forth the new standards and methods the DOE will use when evaluating data security compliance.

An institution’s Title IV Program Participation Agreement (PPA) requires that they must protect all student financial aid data. The Student Aid Internet Gateway (SAIG) Enrollment Agreement, the system used by educational institutions and third-party servicers to exchange data electronically with the U.S. Department of Education, contains similar requirements.

In addition, the letter reminds institutions that the specific requirements of the Gramm-Leach-Bliley Act (GLBA) governing data security at financial services organizations apply to post-secondary institutions. These include implementing a written information security program, designating an individual to coordinate information security,
performing ongoing risk assessments, and properly vetting third-party service providers. It is also noted that compliance with the GLBA will be incorporated into the DOE’s annual student aid compliance audit requirements.

Most significantly, the letter “strongly encourages institutions to review and understand the standards defined in NIST SP 800-171.” These standards were developed by the National Institute of Standards and Technology (NIST) to protect sensitive federal information that is used and stored in non-federal information systems and organizations. NIST SP 800-171 sets forth a significant expansion of the data security requirements and controls expected in the handling of student financial aid data and other types of federal data and information. In citing these standards, the DOE acknowledges “the investment and effort by institutions to meet and maintain the standards set forth in NIST SP 800-171” but “strongly encourages those institutions that fall short of NIST standards to assess their current gaps and immediately begin to design and implement plans to close those gaps using NIST standards as a model.”

The message from the US DOE is clear – institutions of higher education that use student financial aid data, and other forms of federal data are expected to “immediately” begin to integrate the specific requirements of NIST SP-171.

Your Money or Your PHI: New Guidance on Ransomware

HHS.gov – July 11, 2016

One of the biggest current threats to health information privacy is the serious compromise of the integrity and availability of data caused by malicious cyber-attacks on electronic health information systems, such as through ransomware. The FBI has reported an increase in ransomware attacks and media have reported a number of ransomware attacks on hospitals.

To help health care entities better understand and respond to the threat of ransomware, the HHS Office for Civil Rights has released new Health Insurance Portability and Accountability Act (HIPAA) guidance on ransomware. The new guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats, including:

- Conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and establishing a plan to mitigate or remediate those identified risks;
- Implementing procedures to safeguard against malicious software;
- Training authorized users on detecting malicious software and report such detections;
- Limiting access to ePHI to only those persons or software programs requiring access; and
- Maintaining an overall contingency plan that includes disaster recovery, emergency operations, frequent data backups, and test restorations.

Some of the other topics covered in the guidance include: understanding ransomware and how it works; spotting the signs of ransomware; implementing security incident responses; mitigating the consequences of ransomware; and the importance of contingency planning and data backup. The guidance makes clear that a ransomware attack usually results in a “breach” of healthcare information under the HIPAA Breach Notification Rule. Under the Rule, and as noted in the guidance, entities experiencing a breach of unsecure PHI must notify individuals whose information is involved in the breach, HHS, and, in some cases, the media, unless the entity can demonstrate (and document) that there is a “low probability” that the information was compromised.

Ransomware is a type of malware (malicious software) that encrypts data with a key known only to the hacker and makes the data inaccessible to authorized users. After the data is encrypted, the hacker demands that authorized users pay a ransom (usually in a cryptocurrency such as Bitcoin to maintain anonymity) in order to obtain a key to decrypt the data. Ransomware frequently infects devices and systems through spam, phishing messages, websites, and email attachments and enters the computer when a user clicks on the malicious link or opens the attachment.

Organizations need to take steps to safeguard their data from ransomware attacks. HIPAA covered entities and business associates are required to develop and implement security incident procedures and response and reporting processes that are reasonable and appropriate to respond to malware and other security incidents.
Stark Law Compliance

South Carolina Hospital to Pay $17 Million to Resolve False Claims Act and Stark Law Allegations

US Department of Justice – July 28, 2016

The Lexington County Health Services District Inc. d/b/a Lexington Medical Center located in West Columbia, South Carolina, has agreed to pay $17 million to resolve allegations that it violated the Physician Self-Referral Law (the Stark Law) and the False Claims Act by maintaining improper financial arrangements with 28 physicians, the Department of Justice announced today.

The Stark Law is intended to ensure that physician referrals are made based on the medical needs of the patients and are not tainted by certain financial arrangements. Thus, the Stark Law generally forbids a hospital from billing Medicare for certain services referred by physicians who have a financial relationship with the hospital unless that relationship falls within enumerated exceptions. The exceptions generally require, among other things, that the financial arrangements do not exceed fair market value, do not take into account the volume or value of any referrals and are commercially reasonable. In addition, arrangements with physicians who are not hospital employees must be set out in writing and satisfy a number of other requirements intended to insulate the referrals from financial considerations.

“This case demonstrates the United States’ commitment to ensuring that doctors who refer Medicare beneficiaries to hospitals for procedures, tests and other health services do so only because they believe the service is in the patient’s best interest, and not because the physician stands to gain financially from the referral,” said Principal Deputy Assistant Attorney General Benjamin C. Mizer, head of the Justice Department’s Civil Division.

The United States alleged that Lexington Medical Center entered into asset purchase agreements for the acquisition of physician practices or employment agreements with 28 physicians that violated the Stark Law because they took into account the volume or value of physician referrals, were not commercially reasonable or provided compensation in excess of fair market value.

Also as part of the settlement, Lexington Medical Center will enter into a Corporate Integrity Agreement (CIA) with the Department of Health and Human Services-Office of the Inspector General (HHS-OIG) that requires Lexington Medical Center to implement measures designed to avoid or promptly detect future conduct similar to that which gave rise to this settlement.

The settlement resolves allegations filed in a lawsuit by Dr. David Hammett, a former physician employed by Lexington Medical Center, in federal court in Columbia, South Carolina. The lawsuit was filed under the qui tam, or whistleblower, provisions of the False Claims Act, which permit private individuals to sue on behalf of the government for false claims and to share in any recovery. Dr. Hammett will receive approximately $4.5 million of the recovered funds.

This civil settlement illustrates the government’s emphasis on combating health care fraud and marks another achievement for the Health Care Fraud Prevention and Enforcement Action Team (HEAT) initiative, which was announced in May 2009 by the Attorney General and the Secretary of Health and Human Services. The partnership between the two departments has focused efforts to reduce and prevent Medicare and Medicaid financial fraud through enhanced cooperation. One of the most powerful tools in this effort is the False Claims Act. Since January 2009, the Justice Department has recovered a total of more than $30 billion through False Claims Act cases, with more than $18.3 billion of that amount recovered in cases involving fraud against federal health care programs.”

The case was handled by the U.S. Attorney’s Office for the District of South Carolina, the Civil Division’s Commercial Litigation Branch and HHS-OIG.

The lawsuit is captioned United States ex rel. Hammett v. Lexington County Health Services District, Case No. 3:14-cv-03653 (D. S.C.). The claims settled by this agreement are allegations only; there has been no determination of liability.
Current Issues in Compliance
August 2016

SUMMARY

Following are excerpts from news articles having a risk management or compliance impact. The full article may be seen at the referenced source (some may require subscription to access).

- ADA Compliance
- Distance Education Regulations
- Human Resources
- Campus Safety

ADA Compliance

Justice Department Revises Regulations to Implement Requirements of ADA Amendments Act of 2008

Department of Justice, Office of Public Affairs, August 10, 2016

A final rule revising the Justice Department’s Americans with Disabilities Act (ADA) Title II and Title III regulations to implement the requirements of the ADA Amendments Act of 2008 (ADAAA) was made available for public inspection by the Federal Register today. The final rule will take effect Oct. 11, 2016.

Although the ADAAA is already in effect and applies to entities covered under Title II and III of the ADA, the department’s changes to its Title II and III regulations will help clarify the interpretation and application of the ADAAA. These changes also satisfy the Attorney General’s responsibility to publish regulations that are consistent with any congressional changes to the ADA.

The ADAAA’s provisions addressing the definition of disability also apply to Title I of the ADA, for which the Equal Employment Opportunity Commission issued regulations in 2011. The publication of the Title II and Title III rule will ensure that the definition of disability is interpreted consistently for these three titles of the ADA.

The revisions to the Department's title II and title III regulations are based on the broad purposes and specific requirements of the ADA Amendments Act. Consistent with the ADA Amendments Act, the regulations establish the following:

- The definition of "disability" should be interpreted broadly. The question of whether an individual’s impairment is a disability under the ADA should not demand extensive analysis.
- Major life activities now include the operation of major bodily functions, such as functions of the neurological, digestive, or respiratory systems. Also, the ADA Amendments Act provides a more extensive, non-exhaustive list of examples of major life activities, which includes major bodily functions.
- Due to uncertainty about the meaning of "physical and mental impairments," the term is now illustrated with the additional examples of dyslexia and Attention-Deficit/Hyperactivity Disorder (ADHD).
- Specific rules of construction apply when determining whether an individual has a disability. These rules of construction include the following:
  1. The primary issue in a case brought under the ADA should be whether the covered entity has complied with its obligations and whether discrimination has occurred, not the extent to which the individual’s impairment substantially limits a major life activity;
  2. The term "substantially limits" shall be construed broadly in favor of expansive coverage, to the maximum extent permitted by the terms of the ADA;
  3. In making the individualized assessment required by the ADA, the term “substantially limits” shall be interpreted to require a degree of functional limitation that is lower than the standard for substantially limits applied prior to the ADA Amendments Act;
  4. The comparison of the extent to which an impairment substantially limits the ability of an individual to perform a major life activity should be to most people in the general population;
5. Comparing an individual’s performance of a major life activity to the performance of the same major life activity by most people in the general population usually will not require scientific, medical, or statistical evidence;

6. The ameliorative effects of mitigating measures, such as medication or hearing aids (but excepting ordinary eyeglasses and contact lenses), shall not be considered in assessing whether an individual has a disability;

7. An impairment that is episodic or in remission is a disability if it would substantially limit a major life activity when active; and

8. An impairment that substantially limits one major life activity need not substantially limit other major life activities in order to be considered a substantially limiting impairment.

Distance Education Regulations

Education Department Proposes Rule on State Authorization of Postsecondary Distance Education, Foreign Locations


The U.S. Department of Education today proposed regulations that seek to improve oversight and protect more than 5.5 million distance education students at degree-granting institutions, including nearly 3 million exclusively online students by clarifying the state authorization requirements for postsecondary distance education.

To ensure that institutions offering distance education are legally authorized and monitored by states, as required by the Higher Education Act, the proposed regulations clarify state authorization requirements for institutions to participate in the Department's federal student aid programs. The proposed regulations also address state and federal oversight of American colleges operating in foreign locations worldwide.

"These proposed regulations achieve an important balance between accountability and flexibility, and in so doing create better protections for students and taxpayers," said U.S. Under Secretary of Education Ted Mitchell. "Additionally, these regulations promote and clarify state authorization procedures, further strengthening the integrity of federal financial aid programs."

In 2006, Congress abolished a rule restricting access to federal student aid for distance education programs. Since then, the number of students enrolled in online degree programs has significantly increased. By 2014, more than half of students at for-profit institutions were enrolled in exclusively distance education courses, compared with an estimated 9 percent of students in public institutions and 15 percent of students in private nonprofit institutions.

State authorization is a longstanding requirement in the Higher Education Act that requires institutions to be authorized in the state in which they are located as a condition for eligibility to receive Title IV Federal student aid. While all higher education institutions must have state authorization in the states in which they are physically located, there are no federal requirements for distance education providers in states where the institutions are not located.

The proposed regulations close this loophole by:

- Requiring institutions offering distance education or correspondence courses to be authorized by each state in which the institution enrolls students, if such authorization is required by the state. The proposed regulation recognizes authorization through participation in a state authorization reciprocity agreement, as long as the agreement does not prevent a state from enforcing its own consumer laws.

- Requiring institutions to document the state process for resolving student complaints regarding distance education programs.

- Requiring public and individualized disclosures to enrolled and prospective students in distance education programs, including adverse actions taken against the school, the school's refund policies, and whether each program meets applicable state licensure or certification requirements.

- Requiring that foreign branch campuses or locations be authorized by the appropriate foreign government agency and, if at least half of a program can be completed at the foreign location or branch campus, be approved by the accrediting agency and reported to the state where the main campus is located.
The Department previously regulated on state authorization of both physical locations and distance education in 2010, but a federal court vacated the distance education portion of the rule on procedural grounds in 2011. The other portions of the 2010 state authorization rule relating to physical locations were implemented last year. Similar to the proposed rule, the 2010 physical locations rule also required institutions to be authorized by states having a state-based consumer complaint system.

The Department held three sessions of negotiated rulemaking on this issue in 2014, but the negotiating committee did not reach consensus. These proposed regulations are a result of that process and further a longstanding regulatory effort by the Department to support state oversight of schools that offer distance or correspondence education and protect students in those programs.

The proposed regulations will be published in the Federal Register on July 25, and the public comment period will end August 24. The Department expects to publish a final regulation before the end of the year.

Human Resources

NLRB Rules that Graduate (and Undergraduate!) Students are Employees and May Unionize


The National Labor Relations Board (Board), in Columbia University, has issued a 3-1 decision holding that graduate, and undergraduate, student assistants are common law employees within the meaning of the National Labor Relations Act and therefore are eligible to organize and bargain collectively under federal labor law. In so doing, the Board overruled its 2004 determination in Brown University. Board Member Miscimarra wrote a lengthy dissent, arguing that the educational nature of the relationship between student and educational institution should dictate that student assistants are not employees and therefore they should not be eligible to organize and bargain collectively.

After much speculation, and following an invitation for briefing in December 2015, the NLRB rejected the Brown holding that graduate assistants cannot be statutory employees because they are “primarily students and have a primarily educational, not economic, relationship with their university.” The Board first noted that it has the statutory authority to treat student assistants as statutory employees. The Board applied a common law test and indicated that when student assistants perform “work,” at the direction of a college or university, for which they are compensated, a common law employment relationship will be deemed to exist and the students will be eligible to organize and bargain collectively.

The Board indicated that the new test will apply to all student assistants, including graduate assistants engaged in research funded by external grants (and subject to the conditions of those grants). The Board also determined that the petitioned for bargaining unit at Columbia — which included graduate students, terminal Master’s degree students, and undergraduate students — constituted an appropriate unit and that none of the petitioned for classifications consisted of temporary employees who should be excluded from the unit. Finally, the Board remanded the case to the Regional Director for consideration of whether student assistants not currently performing their assistant duties should be eligible to vote based upon a continuing expectation of future common law employment.

The Board’s decision was long the subject of speculation and has been anticipated by many commentators. In the wake of the decision, colleges and universities should anticipate increased organizing activity on their campuses and will have the obligation to bargain with units comprised of student assistants if they are recognized after an NLRB election. Given the breadth of the Board’s decision, and the potential units that could be petitioned for by unions, this decision has the potential to represent a significant challenge if broad units of student assistants are voted in and certified under NLRB procedures.
Campus Safety

Best Practices for Assessing and Enhancing Compliance Prior to an Incident

In today’s litigation and regulatory climate, companies involved in an incident causing injuries or environmental damage can expect intense scrutiny from litigants, regulators and prosecutors. While initial questions may focus on the immediate causes of the incident, inquiries quickly broaden. Soon all aspects of a company’s operations may be under the microscope, including its pre-incident compliance record and culture.

Often, the intense post-incident scrutiny brings to light negative evidence that helps opponents portray companies as being callously indifferent to safety regulations, potentially exposing them to findings of gross negligence, enhanced fines and penalties and even criminal charges. For example, in the ongoing trial of PG&E for alleged knowing and willful violations of federal pipeline safety regulations and obstruction in connection with the September 2010 explosion that killed eight people and destroyed 38 homes in San Bruno, California, jurors have seen emails suggesting the company ignored safety concerns in the months leading up to the incident and describing pre-incident cuts in safety spending as “near-criminal.” Similarly, parties to the liability trial following BP’s Gulf of Mexico oil spill focused on documents and actions in the days preceding the blowout as reflective of a corporate culture that put “profits over safety.” In his decision finding BP grossly negligent, U.S. District Judge Carl Barbier cited various “profit-driven” decisions as reflecting a “conscious disregard of known risks” by BP.

In addition to potentially helping to avoid an incident in the first place, proactively assessing and enhancing compliance prior to an incident will leave companies in a much better position should the unthinkable occur. While evidence of pre-incident compliance problems, particularly knowing or reckless non-compliance with safety regulations, can certainly make things easier for opponents, the opposite is also true—a robust and effective compliance program makes it harder for opposing parties to demonstrate the extreme departure from standards of care typically required to establish gross negligence or support a finding of punitive damages. It can also lead to fewer or lesser criminal charges and even help companies avoid such charges altogether.

Where to Begin?

Undertaking a comprehensive search for every undotted “i” and uncrossed “t” could be prohibitively expensive, if not entirely impossible, for most companies. Fortunately, lessons from prior incidents highlight common problems and can help identify priorities.

A review of investigation reports following incidents involving multiple fatalities and environmental damage in North America over the past several years indicates the following issues are repeatedly cited as contributing causes of such incidents:

- Poor safety culture or an emphasis on putting profits ahead of safety;
- Insufficient, or incomplete implementation of, safety management systems;
- Gaps between corporate policies and day-to-day operations;
- Deficiencies in employee training and supervision;
- Confusion in lines of responsibility or accountability;
- Failure to close out audit findings or implement lessons learned from prior incidents.

Due to their apparent prevalence preceding major incidents, these issues provide a good initial list of high priority items against which to consider your track record and the effectiveness of your policies and procedures before you have an incident.

What to do?

While there is no one size-fits-all approach to assessing and enhancing compliance, the goals are clear: (1) identify gaps where current activities fall short (or appear to fall short) of regulatory requirements or company procedures and (2) work to close those gaps. Experience with prior incidents suggests the following actions can be effective:
• Assess safety culture, including through employee surveys and interviews, and continually emphasize safety over profits such as by empowering all employees and contractors to exercise stop-work authority whenever they feel conditions are unsafe and ensure they will not face reprisal for doing so;

• Conduct a privileged review of your safety management system and health, safety and environmental policies and procedures to confirm they are sufficient to ensure compliance and that they have been implemented everywhere intended;

• Periodically audit operations to confirm day-to-day activities meet or exceed regulatory requirements and comply with company policies and procedures;

• Regularly review and refresh training materials and seek to identify and remediate any potential deficiencies;

• Take steps to identify any confusion in lines of responsibility or accountability, for example through employee interviews and annual reviews, and clarify any identified issues;

• Confirm that recommendations from prior investigations have been implemented or reasons for non-implementation have been appropriately documented.

In undertaking the foregoing steps, involve your legal department and/or outside counsel where appropriate to maximize available privilege protections. Doing so can dramatically lessen the likelihood of self-inflicted wounds that can lead to increased liability.

Conclusion

While it may not be possible to prevent every incident, companies that proactively assess and enhance compliance prior to an incident will be much better positioned to manage the intense scrutiny that follows should an incident occur. Taking steps such as those identified above may serve companies well in the inevitable investigations and litigation that follow incidents as evidence of corporate responsibility and adherence to standards of care. Companies that do so will be less likely to be found to have engaged in conduct rising to the level of gross negligence or subject to enhanced fines and penalties and may face fewer or lesser criminal charges, or even avoid them altogether.

United States District Court Enjoins Enforcement of Dear Colleague Letter on Transgender Students; Decision May Impact OCR Guidance on Sexual Violence


On August 21, 2016, in a case entitled *State of Texas et al. v. United States of America et al.*, Judge Reed O’Connor of the United States District Court for the Northern District of Texas issued a nationwide preliminary injunction prohibiting the United States government (specifically, the Office for Civil Rights of the Department of Education (“OCR”), the Department of Justice (“DOJ”), the Department of Labor and the Equal Employment Opportunity Commission) from enforcing the terms of the May 13, 2016 Dear Colleague Letter issued by OCR and DOJ. As institutions are aware, the Dear Colleague Letter articulated OCR’s and DOJ’s interpretation of Title IX and its implementing regulations as requiring K-12 schools, colleges and universities to treat a student’s gender identity as the student’s “sex” for purposes of Title IX’s prohibition against discrimination based on sex, and described several areas where schools and institutions must provide transgender students with equal access to education programs and activities “even in circumstances in which other students, parents and community members raise objections or concerns.”

In reaching its decision, the Court found that there was a likelihood that the plaintiffs (13 states and two school districts) would prevail on their claim that the Departments’ interpretation of Title IX is contrary to the plain language of the statute and its implementing regulations, and is therefore incorrect as a matter of law. Specifically, the Court determined that the term “sex,” as understood at the time that the statute and regulations were initially adopted, was understood to refer to an individual’s biological sex, rather than the individual’s gender identity.

Perhaps more significantly, in an aspect of the decision that could impact OCR’s enforcement strategy in other areas, the Court also determined that OCR and DOJ were required to comply with the federal Administrative Procedure Act (the “APA”) prior to issuing the Dear Colleague Letter, and that their failure to do so rendered the Dear Colleague Letter invalid. By way of background, the APA requires federal agencies to publish proposed rules in the Federal Register, and to provide the public a period of time to comment on them (this is commonly referred to as the “notice
and comment” process). The purpose of this requirement is to enable an agency to consider the perspectives of persons or entities that would be impacted by proposed rules before they are finalized. However, not every action an agency takes is required to go through the notice and comment process, and the APA specifically excludes from its ambit agency pronouncements that amount merely to interpretations of existing rules (rather than the imposition of new substantive requirements).

In concluding that OCR and DOJ were required (and failed) to comply with the APA prior to issuing the Dear Colleague Letter, the Court noted that OCR and DOJ have applied the guidance contained in the Dear Colleague Letter as if it were binding law in a manner different than the underlying regulation had previously been applied, and that the guidance is “compulsory in nature” in that schools must comply with the guidance or be deemed in breach of their Title IX obligations.

This decision is obviously significant insofar as it impacts the enforceability of the May 13, 2016 Dear Colleague Letter. However, colleges and universities that have voluntarily implemented measures consistent with the Dear Colleague Letter may certainly continue to do so, unless they are located in states that have adopted legislation prohibiting such action. Where the decision (or, at a minimum, the reasoning underlying the decision) may have a greater impact is in its potential effect on OCR’s subregulatory guidance with respect to institutions’ obligations to prevent and address sexual violence (e.g., OCR’s April 3, 2011 Dear Colleague Letter and its April 29, 2014 Questions and Answers on Title IX and Sexual Violence). Although the arguments for and against the validity of OCR’s substantive interpretation of Title IX are different as between these two subject areas, there are certainly parallels between OCR’s use of purported subregulatory guidance on both issues. Indeed, the District Court noted the impact of the May 13, 2016 Dear Colleague Letter on institutions, as evidenced by the government’s efforts to enforce its requirements, as a significant factor in characterizing it as legislative (and thus subject to the APA) rather than interpretive in nature, and OCR’s enforcement of its guidance on sexual violence is undeniable, with over 250 active investigations at more than 200 institutions currently pending.

It is certainly possible, and perhaps even likely, that the federal government will appeal the Court’s decision in State of Texas, and in any event OCR can be expected to assert that the Court’s rationale does not apply to its guidance on sexual violence. However, the Court’s decision will certainly be used in support of pending litigation challenging the validity of OCR’s guidance on sexual violence, and in connection with congressional efforts to overturn that guidance. Needless to say, the situation merits further watching.
SUMMARY

Following are excerpts from news articles having a risk management or compliance impact. The full article may be seen at the referenced source (some may require subscription to access). Topics for this month include the following:

- ADA Compliance
- False Claims Act
- HIPAA
- Human Resources
- Information Security
- Stark Law Compliance

ADA Compliance

Justice Department Revises Regulations to Implement Requirements of ADA Amendments Act of 2008

*Department of Justice, Office of Public Affairs* - August 10, 2016

A final rule revising the Justice Department’s Americans with Disabilities Act (ADA) Title II and Title III regulations to implement the requirements of the ADA Amendments Act of 2008 (ADAAA) was made available for public inspection by the Federal Register today. The final rule will take effect Oct. 11, 2016.

Although the ADAAA is already in effect and applies to entities covered under Title II and III of the ADA, the department’s changes to its Title II and III regulations will help clarify the interpretation and application of the ADAAA. These changes also satisfy the Attorney General’s responsibility to publish regulations that are consistent with any congressional changes to the ADA.

The ADAAA’s provisions addressing the definition of disability also apply to Title I of the ADA, for which the Equal Employment Opportunity Commission issued regulations in 2011. The publication of the Title II and Title III rule will ensure that the definition of disability is interpreted consistently for these three titles of the ADA.

The revisions to the Department's title II and title III regulations are based on the broad purposes and specific requirements of the ADA Amendments Act. Consistent with the ADA Amendments Act, the regulations establish the following:

- The definition of "disability" should be interpreted broadly. The question of whether an individual’s impairment is a disability under the ADA should not demand extensive analysis.

- Major life activities now include the operation of major bodily functions, such as functions of the neurological, digestive, or respiratory systems. Also, the ADA Amendments Act provides a more extensive, non-exhaustive list of examples of major life activities, which includes major bodily functions.

- Due to uncertainty about the meaning of "physical and mental impairments," the term is now illustrated with the additional examples of dyslexia and Attention-Deficit/Hyperactivity Disorder (ADHD).

- Specific rules of construction apply when determining whether an individual has a disability. These rules of construction include the following:

  1. The primary issue in a case brought under the ADA should be whether the covered entity has complied with its obligations and whether discrimination has occurred, not the extent to which the individual’s impairment substantially limits a major life activity;

  2. The term "substantially limits" shall be construed broadly in favor of expansive coverage, to the maximum extent permitted by the terms of the ADA;

  3. In making the individualized assessment required by the ADA, the term “substantially limits” shall be interpreted to require a degree of functional limitation that is lower than the standard for substantially limits applied prior to the ADA Amendments Act;
4. The comparison of the extent to which an impairment substantially limits the ability of an individual to perform a major life activity should be to most people in the general population;

5. Comparing an individual’s performance of a major life activity to the performance of the same major life activity by most people in the general population usually will not require scientific, medical, or statistical evidence;

6. The ameliorative effects of mitigating measures, such as medication or hearing aids (but excepting ordinary eyeglasses and contact lenses), shall not be considered in assessing whether an individual has a disability;

7. An impairment that is episodic or in remission is a disability if it would substantially limit a major life activity when active; and

8. An impairment that substantially limits one major life activity need not substantially limit other major life activities in order to be considered a substantially limiting impairment.

False Claims Act

False Claims Act penalties double
SCCE - The Compliance and Ethics Blog - June 30, 2016

On June 30, the Department of Justice passed an interim final rule that gave False Claims Act penalties a big raise. Here’s what you need to know:

- The False Claims Act prohibits submitting false or fraudulent claims to the Federal government (e.g. Medicare or Medicaid) for payment.
- Health care providers who submit false claims face penalties.
- The current False Claims Act penalties are: $5,500 (minimum) and $11,000 (maximum) per claim.
- Starting August 1, 2016, these penalties increase to $10,781.40 (minimum) and $21,562.80 (maximum).
- The new amounts apply to false claims submitted after November 2, 2015.
- Because the penalty amounts are “per claim,” providers facing lawsuits or investigations involving multiple claims need to multiple these penalty amounts by the number of claims involved to estimate their exposure.

When False Claims Act penalties double, so do whistleblower rewards. This means that employees, former employers and competitors have twice the motivation to report providers’ claims inaccuracies to the government.

When False Claims Act penalties double, so does the importance of your compliance program. The best way to avoid the financial exposure of a False Claims Act lawsuit or settlement is to put ample resources into your compliance program effort:

- Prevent non-compliance with policies, procedures, and employee education.
- Detect non-compliance with an anonymous way to report non-compliance internally, and routine audits.
- Correct non-compliance before it grows into a bigger problem.
- Self-Report non-compliance to receive mitigated penalties.

Government sends a $2.95 million warning to health care providers with announcement of settlement in 60-day overpayment rule case
Bricker & Eckler - Health Care Law – August 29, 2016

The first federal lawsuit involving interpretation and application of the 60-day overpayment refund rule, which was discussed in previous Bricker & Eckler publications (see “Department of Justice wins federal court ruling on 60-day overpayment rule” from August 2015 and “DOJ intervenes in False Claims Act suit over ACA’s 60-day overpayment rule” from July 2014), has been settled. On August 24, 2016, the government sent a powerful message when the New York Attorney General announced that Mount Sinai Health System agreed to pay $2.95 million to settle allegations that three of its hospitals held onto approximately $844,000 in Medicaid overpayments beyond the 60-day deadline.
for reporting and returning identified overpayments. The overpayments stemmed from the hospitals’ incorrect billing of Medicaid as a secondary payor for claims for services rendered to Medicaid managed care patients. According to the New York Attorney General’s press release announcing the settlement, the hospitals became aware of the overpayments in 2009 and 2010 but “avoided fully reimbursing Medicaid for those patients until March 2013.” The government’s investigation was initiated by a whistleblower who filed a qui tam lawsuit after his employment was terminated days after he brought the errors to the attention of management at the hospitals. The whistleblower will receive $354,000 as his share of the settlement proceeds for bringing this case on behalf of the government.

The Centers for Medicare & Medicaid Services (CMS) final rule on Medicare Part A and Part B overpayments was published in the Federal Register on February 11, 2016, and requires health care providers to report and return overpayments within 60 days of “identifying” the overpayment. In the final rule, CMS clarified what “identifying” an overpayment means, explaining that the 60-day clock for reporting and returning overpayments begins when the person “has or should have, through the exercise of reasonable diligence, determined that the person has received an overpayment and quantified the amount of the overpayment.” However, in the final rule, CMS cautioned that providers and suppliers cannot avoid liability by failing to investigate possible overpayments. According to the final rule, CMS will deem a provider or supplier to “have determined that [it] received an overpayment and quantified the amount of the overpayment if the person fails to exercise reasonable diligence and the person in fact received an overpayment.” The 60-day clock for reporting and returning the overpayment begins when the reasonable diligence is completed “…or on the day the person received credible information of a potential overpayment if the person failed to conduct reasonable diligence and the person in fact received an overpayment.” CMS explains that reasonable diligence includes both good faith proactive compliance activities to monitor the receipt of overpayments and timely investigations in response to obtaining credible information of a potential overpayment.

This settlement should serve as a warning to health care providers that once a possible overpayment situation is reported or discovered, they must investigate the matter and not bury their heads in the sand. In this case, the failure of the hospitals to promptly investigate and report/return the $844,000 overpayment to the Medicaid agency resulted in costing them over three times the original overpayment amount.

HIPAA

HIPAA Update

AHC Media – August 8, 2016

Health System Agrees to Largest Settlement to Date

In the largest settlement of its kind, Illinois healthcare system Advocate Health agreed to pay $5.5 million and develop a corrective action plan to settle HIPAA violations due to data breaches. The violations include data protection violations related to electronic protected health information (ePHI) that have occurred over the past three years.

According to the U.S. Department of Health and Human Services’ Office of Civil Rights (OCR), the massive settlement was due to the extent and duration of the hospital system’s noncompliance with data security laws, and the number of patients affected. The security lapses affected four million patients and included patient names, insurance information, credit card numbers, addresses, clinical information, and dates of birth.

The investigations began in 2013 when Advocate Health submitted three breach notifications to OCR, including a breach that involved unauthorized access to 2,000 patient records by a third-party billing partner, and another that included theft of desktop computers containing four million patient records from an Advocate administrative office. The OCR investigation revealed Advocate Health did not conduct a thorough assessment of risks and vulnerabilities in the system; did not implement policies and procedures; failed to implement reasonable safeguards involving an unencrypted, stolen laptop; and did not ensure that third-party business associates would provide safeguards for ePHI.

“We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals’ ePHI is secure,” said OCR Director Jocelyn Samuels in a statement. “This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level.”
OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals

HHS Office for Civil Rights in Action – August 18, 2016

Since the passage of the Health Information Technology for Economic and Clinical Health Act of 2009 and the subsequent implementation of the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule, OCR has prioritized investigation of reported breaches of protected health information (PHI). The root causes of breaches may indicate entity-wide and industry-wide noncompliance with HIPAA’s regulations, and investigation of breaches provides OCR with an opportunity to evaluate an entity’s compliance programs, obtain correction of any deficiencies, and better understand compliance issues in HIPAA-regulated entities more broadly. OCR’s Regional Offices investigate all reported breaches involving the PHI of 500 or more individuals. Regional Offices also investigate reports of smaller breaches (involving the PHI of fewer 500 individuals), as resources permit.

Beginning this month, OCR, through the continuing hard work of its Regional Offices, has begun an initiative to more widely investigate the root causes of breaches affecting fewer than 500 individuals. Regional Offices will still retain discretion to prioritize which smaller breaches to investigate, but each office will increase its efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these breaches. Among the factors Regional Offices will consider include:

• The size of the breach;
• Theft of or improper disposal of unencrypted PHI;
• Breaches that involve unwanted intrusions to IT systems (for example, by hacking); The amount, nature and sensitivity of the PHI involved; or
• Instances where numerous breach reports from a particular covered entity or business associate raise similar issues.

Regions may also consider the lack of breach reports affecting fewer than 500 individuals when comparing a specific covered entity or business associate to like-situated covered entities and business associates.

Ransomware Reporting Requirements and New HHS Guidance, Fact Sheet


Ransomware is malicious software that denies access to data, usually by encrypting the data with a private encryption key that is only provided once a ransom is paid. Sometimes the ransomware will actually destroy, steal, or export data from information systems.

Ransomware has become a significant threat to all U.S. businesses and individuals, and a particularly dangerous threat to those in health care. Ransomware victims are not only at risk of losing their files or suffering from a data breach, but may also experience financial loss due to paying the ransom, loss of productivity, IT services, legal fees, network countermeasures, and the purchase of credit monitoring services for employees or customers if their information was referenced in the encrypted files. In health care, the consequences can be far more serious—protected health information can be lost, destroyed, or shared with malicious actors, patient treatment can be delayed, and lives could even be lost as a result of systems being locked down by malicious actors.

Due to the significant uptick of ransomware attacks and its particularly powerful threat to the health care industry, the Federal Health and Human Services Department (HHS) issued a fact sheet that provides guidance on ransomware issues and notes that hospitals and doctor offices may be required to notify HHS if they are a victim of ransomware. As it notes, “The presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures.”
Human Resources

NLRB Rules that Graduate (and Undergraduate!) Students are Employees and May Unionize


The National Labor Relations Board (Board), in Columbia University, has issued a 3-1 decision holding that graduate, and undergraduate, student assistants are common law employees within the meaning of the National Labor Relations Act and therefore are eligible to organize and bargain collectively under federal labor law. In so doing, the Board overruled its 2004 determination in Brown University. Board Member Miscimarra wrote a lengthy dissent, arguing that the educational nature of the relationship between student and educational institution should dictate that student assistants are not employees and therefore they should not be eligible to organize and bargain collectively.

After much speculation, and following an invitation for briefing in December 2015, the NLRB rejected the Brown holding that graduate assistants cannot be statutory employees because they are “primarily students and have a primarily educational, not economic, relationship with their university.” The Board first noted that it has the statutory authority to treat student assistants as statutory employees. The Board applied a common law test and indicated that when student assistants perform “work,” at the direction of a college or university, for which they are compensated, a common law employment relationship will be deemed to exist and the students will be eligible to organize and bargain collectively.

The Board indicated that the new test will apply to all student assistants, including graduate assistants engaged in research funded by external grants (and subject to the conditions of those grants). The Board also determined that the petitioned for bargaining unit at Columbia — which included graduate students, terminal Master’s degree students, and undergraduate students — constituted an appropriate unit and that none of the petitioned for classifications consisted of temporary employees who should be excluded from the unit. Finally, the Board remanded the case to the Regional Director for consideration of whether student assistants not currently performing their assistant duties should be eligible to vote based upon a continuing expectation of future common law employment.

The Board’s decision was long the subject of speculation and has been anticipated by many commentators. In the wake of the decision, colleges and universities should anticipate increased organizing activity on their campuses and will have the obligation to bargain with units comprised of student assistants if they are recognized after an NLRB election. Given the breadth of the Board’s decision, and the potential units that could be petitioned for by unions, this decision has the potential to represent a significant challenge if broad units of student assistants are voted in and certified under NLRB procedures.

Information Security

Banner Health the latest cyberattack victim

*BenefitsPRO* – August 4, 2016

After a major security breach, Banner Health Systems had to contact 3.7 million customers to inform them their information may have been compromised by hackers.

The cyberattack originally targeted systems that process food purchases at company facilities. Through that breach, hackers were able to infiltrate the company’s far more valuable health records.

“The patient and health plan information (compromised) may have included names, birth dates, addresses, physicians’ names, dates of service, claims information, and possibly health insurance information and Social Security numbers,” the company said in a statement.

The Phoenix-based company learned of the attack in early July, two weeks after it began. On Wednesday, it announced that it would mail letters to its customers, offering them a “free one-year membership in monitoring services to patients, health plan members, health plan beneficiaries, physicians and healthcare providers, and food and beverage customers who were affected by this incident.”

**Why you should care about health care hacking**

Those who have health care records hacked are in worse shape than those whose credit card numbers are swiped.
The Banner Health hacking is one of the most severe health-related cyberattacks in recent memory, but it was hardly a surprise to cybersecurity experts, who have been warning of the risk to health records by hackers for years. Health records, say experts, are a more profitable asset to fraudsters than credit card numbers.

"It is perfect for ID theft," Nicola Fulford, an attorney who deals with identity theft issues, told the BBC. “You have everything you need to make fraudulent health insurance claims, for example."

The concerns have become mainstream in the wake of a number of prominent incidents. One notable hacking resulted in Hollywood Presbyterian Medical Center in Los Angeles paying a $17,000 to hackers who had infiltrated the hospital’s computer system with a “ransomware,” which demands payment in bitcoins, the cybercurrency. The sum of money meant little to the hospital, but the payment prompted predictable concerns that negotiations with hackers would only encourage further attacks.

PBS reported earlier this year that in 2015 alone, 113 million health records were compromised by cyberattacks.

Some also argue that the aggressive push to implement electronic health records by the Obama administration hit providers too hard, too fast, and was not accompanied by enough training or awareness of cybersecurity.

The administration and Congress have been exploring solutions to improve security for the health care system. In March, the Department of Health and Human Services announced the creation of a task force, composed of government and industry leaders, dedicated to coming up with ways to bolster security. Congress is currently considering a bipartisan bill that would establish a position within the department specifically focused on cybersecurity.

### Stark Law Compliance

**Best Practices for Assessing and Enhancing Compliance Prior to an Incident**

_Corporate Compliance Insights_ – August 3, 2016

In today’s litigation and regulatory climate, companies involved in an incident causing injuries or environmental damage can expect intense scrutiny from litigants, regulators and prosecutors. While initial questions may focus on the immediate causes of the incident, inquiries quickly broaden. Soon all aspects of a company’s operations may be under the microscope, including its pre-incident compliance record and culture.

Often, the intense post-incident scrutiny brings to light negative evidence that helps opponents portray companies as being callously indifferent to safety regulations, potentially exposing them to findings of gross negligence, enhanced fines and penalties and even criminal charges. For example, in the ongoing trial of PG&E for alleged knowing and willful violations of federal pipeline safety regulations and obstruction in connection with the September 2010 explosion that killed eight people and destroyed 38 homes in San Bruno, California, jurors have seen emails suggesting the company ignored safety concerns in the months leading up to the incident and describing pre-incident cuts in safety spending as “near-criminal.” Similarly, parties to the liability trial following BP’s Gulf of Mexico oil spill focused on documents and actions in the days preceding the blowout as reflective of a corporate culture that put “profits over safety.” In his decision finding BP grossly negligent, U.S. District Judge Carl Barbier cited various “profit-driven” decisions as reflecting a “conscious disregard of known risks” by BP.

In addition to potentially helping to avoid an incident in the first place, proactively assessing and enhancing compliance prior to an incident will leave companies in a much better position should the unthinkable occur. While evidence of pre-incident compliance problems, particularly knowing or reckless non-compliance with safety regulations, can certainly make things easier for opponents, the opposite is also true—a robust and effective compliance program makes it harder for opposing parties to demonstrate the extreme departure from standards of care typically required to establish gross negligence or support a finding of punitive damages. It can also lead to fewer or lesser criminal charges and even help companies avoid such charges altogether.

**Where to Begin?**

Undertaking a comprehensive search for every undotted “i” and uncrossed “t” could be prohibitively expensive, if not entirely impossible, for most companies. Fortunately, lessons from prior incidents highlight common problems and can help identify priorities.
A review of investigation reports following incidents involving multiple fatalities and environmental damage in North America over the past several years indicates the following issues are repeatedly cited as contributing causes of such incidents:

- Poor safety culture or an emphasis on putting profits ahead of safety;
- Insufficient, or incomplete implementation of, safety management systems;
- Gaps between corporate policies and day-to-day operations;
- Deficiencies in employee training and supervision;
- Confusion in lines of responsibility or accountability;
- Failure to close out audit findings or implement lessons learned from prior incidents.

Due to their apparent prevalence preceding major incidents, these issues provide a good initial list of high priority items against which to consider your track record and the effectiveness of your policies and procedures before you have an incident.

**What to do?**

While there is no one size-fits-all approach to assessing and enhancing compliance, the goals are clear: (1) identify gaps where current activities fall short (or appear to fall short) of regulatory requirements or company procedures and (2) work to close those gaps. Experience with prior incidents suggests the following actions can be effective:

- Assess safety culture, including through employee surveys and interviews, and continually emphasize safety over profits such as by empowering all employees and contractors to exercise stop-work authority whenever they feel conditions are unsafe and ensure they will not face reprisal for doing so;
- Conduct a privileged review of your safety management system and health, safety and environmental policies and procedures to confirm they are sufficient to ensure compliance and that they have been implemented everywhere intended;
- Periodically audit operations to confirm day-to-day activities meet or exceed regulatory requirements and comply with company policies and procedures;
- Regularly review and refresh training materials and seek to identify and remediate any potential deficiencies;
- Take steps to identify any confusion in lines of responsibility or accountability, for example through employee interviews and annual reviews, and clarify any identified issues;
- Confirm that recommendations from prior investigations have been implemented or reasons for non-implementation have been appropriately documented.

In undertaking the foregoing steps, involve your legal department and/or outside counsel where appropriate to maximize available privilege protections. Doing so can dramatically lessen the likelihood of self-inflicted wounds that can lead to increased liability.

**Conclusion**

While it may not be possible to prevent every incident, companies that proactively assess and enhance compliance prior to an incident will be much better positioned to manage the intense scrutiny that follows should an incident occur. Taking steps such as those identified above may serve companies well in the inevitable investigations and litigation that follow incidents as evidence of corporate responsibility and adherence to standards of care. Companies that do so will be less likely to be found to have engaged in conduct rising to the level of gross negligence or subject to enhanced fines and penalties and may face fewer or lesser criminal charges, or even avoid them altogether.

---

**United States District Court Enjoins Enforcement of Dear Colleague Letter on Transgender Students; Decision May Impact OCR Guidance on Sexual Violence**


On August 21, 2016, in a case entitled *State of Texas et al. v. United States of America et al.*, Judge Reed O’Connor of the United States District Court for the Northern District of Texas issued a nationwide preliminary injunction
prohibiting the United States government (specifically, the Office for Civil Rights of the Department of Education (“OCR”), the Department of Justice (“DOJ”), the Department of Labor and the Equal Employment Opportunity Commission) from enforcing the terms of the May 13, 2016 Dear Colleague Letter issued by OCR and DOJ. As institutions are aware, the Dear Colleague Letter articulated OCR’s and DOJ’s interpretation of Title IX and its implementing regulations as requiring K-12 schools, colleges and universities to treat a student’s gender identity as the student’s “sex” for purposes of Title IX’s prohibition against discrimination based on sex, and described several areas where schools and institutions must provide transgender students with equal access to education programs and activities “even in circumstances in which other students, parents and community members raise objections or concerns.”

In reaching its decision, the Court found that there was a likelihood that the plaintiffs (13 states and two school districts) would prevail on their claim that the Departments’ interpretation of Title IX is contrary to the plain language of the statute and its implementing regulations, and is therefore incorrect as a matter of law. Specifically, the Court determined that the term “sex,” as understood at the time that the statute and regulations were initially adopted, was understood to refer to an individual’s biological sex, rather than the individual’s gender identity.

Perhaps more significantly, in an aspect of the decision that could impact OCR’s enforcement strategy in other areas, the Court also determined that OCR and DOJ were required to comply with the federal Administrative Procedure Act (the “APA”) prior to issuing the Dear Colleague Letter, and that their failure to do so rendered the Dear Colleague Letter invalid. By way of background, the APA requires federal agencies to publish proposed rules in the Federal Register, and to provide the public a period of time to comment on them (this is commonly referred to as the “notice and comment” process). The purpose of this requirement is to enable an agency to consider the perspectives of persons or entities that would be impacted by proposed rules before they are finalized. However, not every action an agency takes is required to go through the notice and comment process, and the APA specifically excludes from its ambit agency pronouncements that amount merely to interpretations of existing rules (rather than the imposition of new substantive requirements).

In concluding that OCR and DOJ were required (and failed) to comply with the APA prior to issuing the Dear Colleague Letter, the Court noted that OCR and DOJ have applied the guidance contained in the Dear Colleague Letter as if it were binding law in a manner different than the underlying regulation had previously been applied, and that the guidance is “compulsory in nature” in that schools must comply with the guidance or be deemed in breach of their Title IX obligations.

This decision is obviously significant insofar as it impacts the enforceability of the May 13, 2016 Dear Colleague Letter. However, colleges and universities that have voluntarily implemented measures consistent with the Dear Colleague Letter may certainly continue to do so, unless they are located in states that have adopted legislation prohibiting such action. Where the decision (or, at a minimum, the reasoning underlying the decision) may have a greater impact is in its potential effect on OCR’s subregulatory guidance with respect to institutions’ obligations to prevent and address sexual violence (e.g., OCR’s April 3, 2011 Dear Colleague Letter and its April 29, 2014 Questions and Answers on Title IX and Sexual Violence). Although the arguments for and against the validity of OCR’s substantive interpretation of Title IX are different as between these two subject areas, there are certainly parallels between OCR’s use of purported subregulatory guidance on both issues. Indeed, the District Court noted the impact of the May 13, 2016 Dear Colleague Letter on institutions, as evidenced by the government’s efforts to enforce its requirements, as a significant factor in characterizing it as legislative (and thus subject to the APA) rather than interpretive in nature, and OCR’s enforcement of its guidance on sexual violence is undeniable, with over 250 active investigations at more than 200 institutions currently pending.

It is certainly possible, and perhaps even likely, that the federal government will appeal the Court’s decision in State of Texas, and in any event OCR can be expected to assert that the Court’s rationale does not apply to its guidance on sexual violence. However, the Court’s decision will certainly be used in support of pending litigation challenging the validity of OCR’s guidance on sexual violence, and in connection with congressional efforts to overturn that guidance. Needless to say, the situation merits further watching.