# University of Connecticut & UConn Health

**Joint Audit & Compliance Committee Meeting**

**May 17, 2016**

10:00 am – 10:45 am - Executive Session
10:45 am – 12:00 pm - Public Session

## AGENDA

<table>
<thead>
<tr>
<th>Topic</th>
<th>Proposed Action</th>
<th>Tab</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Executive Session to discuss:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 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)]</td>
<td>Review</td>
<td>None</td>
</tr>
<tr>
<td>• 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)]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• C.G.S 1-200(6)(E) – Records, reports and statements privileged by the attorney-client relationship. [1-210(b)(10)]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 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)]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Opportunity for Public Comments | None |

| Minutes of the February 3, 2016 JACC Meeting | Approval | 1 |

<table>
<thead>
<tr>
<th>Storrs &amp; UConn Health Significant Compliance Activities</th>
<th>Update</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Annual Compliance Reports - Storrs / UConn Health</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Three-Year Work Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Compliance Counsel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Minors Protection Update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ICD-10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Drug Free Schools – UConn Health</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storrs &amp; UConn Health Significant Audit Activities</th>
<th>Update</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Status of Audit Assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Audit Follow-up Activity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Hiring Update</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Charter Review</th>
<th>Update</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Executive Risk Management Compliance Committee – Storrs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External Engagements</th>
<th>Presentation</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>• RSM - UConn 2000 Construction Projects’ Expenditures Annual Audit and Agreed Upon Procedures FY15</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Auditor of Public Accounts</th>
<th>Presentation</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>• State-wide Single Audit Report for the Fiscal Year Ended June 30, 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UConn Federally-Sponsored Research and Development Programs – p.274</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UConn Health Federally-Sponsored Research and Development Programs – p. 276</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UConn Federal Student Financial Assistance Awards – p. 285-312</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Informational/Educational Items</th>
<th>Information Only</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compliance Newsletters – Storrs &amp; UConn Health</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Current Issues in Compliance Newsletters – Storrs &amp; UConn Health</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Conclusion of Full Meeting

Information Session with OACE and External Auditors

*The next meeting of the JACC will be held on Wednesday, September 21, 2016 at 10:00 am*  
*Rome Commons Ballroom, Storrs*
University of Connecticut
&
UConn Health

Joint Audit & Compliance Committee Meeting
The meeting of the Joint Audit and Compliance Committee (JACC) was called to order at 9:01 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 9:53 a.m. and the JACC returned to open session at 9:55 a.m.

There were no public comments.

**Tab 1 – Minutes of the Meeting**

**ON A MOTION** made by Trustee Nayden and seconded by Director Archambault the minutes of the December 1, 2015, JACC meeting were approved.
University of Connecticut & UConn Health  
Joint Audit & Compliance Committee Meeting  
Meeting Minutes from February 3, 2016

**TAB 2 – Storrs & UConn Health Significant Compliance Activities**

The committee postponed the discussion of the Significant Compliance Activities until the next JACC meeting.

**TAB 3 – Significant Audit Activities**

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

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

S. Allen provided an update on the Status of Corrective Actions – Health Information / Record of Care Management.

**Tab 4 – Charter Review**

The committee postponed the update on the Executive Risk Management Compliance Committee – Storrs Charter until the next JACC meeting.

**Tab 5 – External Engagements**

C. Jackson and D. Coyle presented the Financial Statements as of June 30, 2015 for the University Medical Group (UMG), the John Dempsey Hospital (JDH) and Finance Corporation conducted by Marcum.

RMS (formerly McGladrey) provided an Audit Timeline for UConn 2000 Construction Program.

**Tab 6 – Auditor of Public Accounts**

Auditors of Public Accounts, J. Rasimas, J. Carroll, G. Slupecki, and N. Freitas, presented the committee with the findings of the University of Connecticut and University of Connecticut Health Center Audited Financial Statements for the year ended June 30, 2015.

They also presented the Auditors’ Report - University of Connecticut Health Center for the Fiscal Years Ended June 30, 2013 and 2014.

C. Eaton also provided a summary of GASB 68.

**Informational / Educational Items**

The committee was provided with the following:

- Compliance Newsletters – Storrs,
- Current Issues in Compliance Newsletters – Storrs 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 11:07 a.m.

Respectfully submitted,

*Angela Marsh*
University of Connecticut
&
UConn Health

Joint Audit & Compliance Committee Meeting
STORRS

Minor Protection Program – The Protection of Minors and Reporting of Child Abuse and Neglect Policy was approved and made effective April 1, 2016. The implementation of the policy includes mandatory program registration, training and background checks for activities involving minors that would fall under the jurisdiction of the policy. As of April 21st, 24 program sessions have initiated the registration process and begun to comply with the policy.

Higher Education Opportunity Act - In order to receive Title IV funding, the University is subject to requirements set forth by the Higher Education Opportunities Act (HEOA). The Office of Audit, Compliance & Ethics is partnering with the Office of Student Financial Aid Services to monitor and support HEOA compliance efforts across the University.

Breach Notification - Required notifications related to the School of Engineering breach are nearing completion

FOI Update – see charts
SIGNIFICANT COMPLIANCE ACTIVITIES

**UConn Health**

- **Overpayment refunds** –
  - Billed global package rather than professional component for select radiology reads
  - Outlier payment received on non-medically necessary lengths of stay
  - Patients treated without required Collaborative Practice Agreement between Anticoagulation Clinic's pharmacist and physician

- **2015 Annual Compliance and HIPAA training** – Due to a time restriction, final statistics were not reported at the February 2016 JACC. UConn Health achieved a 98.4% overall compliance with assigned training.
  - Included in this overall rate were two departments achieving 100%:
    - University Medical Group
    - Correctional Managed Health Care

- **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:
  - Fitness-for-Duty Privacy – in final stages
  - Workplace Violence, Violence Against Healthcare Workers – in self-assessment phase
  - Stark – initial stage
  - HIPAA Privacy and Security – Taskforce approach. First meeting held May 3rd.
  - Drug-Free Schools, Drug-Free Workplace – status presentation today
Storrs

Types of FOI Requests (2015)
DRUG FREE SCHOOLS AND WORKPLACE

PURPOSE

In accordance with the Drug Free Schools and Campuses Act and Drug Free Workplace Act, UConn Health is required to do the following:

- Establish drug and alcohol prevention programs for students and employees
- Distribute (annually) materials that include standards of conduct, legal and University sanctions, health risks, available assistance and treatment programs
- Provide written certification of adoption and implementation of prevention program
- Conduct a biennial review to determine program effectiveness, implement any needed changes and ensure that disciplinary sanctions are enforced consistently

PROGRESS


Membership:

- Chair, Human Resources
- Representative, Labor Relations/HR
- Representative, School of Medicine
- Representative, School of Dental Medicine
- Representative, Residency Program
- Director, EAP
- Chief, UConn Health Police
- Representative, Research Compliance
- Representative, Student Services
- Senior Counsel (advisory)
- Office Audit, Compliance, Ethics (advisory)

Compliance self-assessment conducted to identify gaps and priority activities. To address gaps, committee recommended using Storrs policy University-wide, with UConn Health specific amendments (i.e., health risks; applicable laws; clear statement of imposed sanctions, notification of conviction).

Amended policy vetted with Storrs Student Affairs; changes accepted by Committee with understanding that both groups will participate in refinement of next version of policy.

Executive Policy Committee review revealed operational differences related to purchase of alcohol that could not be aligned prior to the end of calendar year.

UConn Health policy amended to mirror Storrs policy and issued separately for this notification cycle. Annual notification distributed to all employees and students via email January 2016.

NEXT STEPS

- Finalize compliance program document and continue to evaluate program requirements
- Continue working toward a single University-wide policy
- Conduct Biennial review, report due November 2016
University of Connecticut
&
UConn Health

Joint Audit & Compliance
Committee Meeting

TAB 3
## 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>Human Subject Incentive Payments</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standard (PCI DSS)</td>
<td>Storrs &amp; UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FY15 Annual Faculty Consulting</td>
<td>Storrs &amp; UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Grants – Cash Management</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>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>Emergency Preparedness</td>
<td>UH</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>Transportation &amp; Parking 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>Space Management Process</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hartford Campus Relocation</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>LCD: Outpatient Physical &amp; Occupational Therapy Services</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>Logging &amp; Monitoring Policy Review</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>Mandatory Training Compliance</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Purchasing</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>TOTAL AUDITS (20)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(04)</strong></td>
<td><strong>(10)</strong></td>
<td><strong>(01)</strong></td>
<td><strong>(05)</strong></td>
<td></td>
<td></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>SHS Pharmacy</td>
<td>Storrs</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>Speech and Hearing Clinic</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>TOTAL SPECIAL PROJECTS/CONSULTING (03)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>(01)</strong></td>
</tr>
</tbody>
</table>
Corrective Actions Implemented by Department

Functional Area

- Avery Point IT
- Avery Point Marine Science
- Bursar's Office
- Chief of Staff
- CLAS IT
- Clinical
- Environmental Health and Safety
- Facilities Operations
- Foundation Administration
- Health Information Management
- Information Technology
- Law School Foundation
- Library Central Services IT
- Nursing
- Procurement Services
- Provost
- Psychiatry
- Public Safety
- Research Finance
- School of Engineering
- Sponsored Program Services
- Student Activities
- Student Health Services
- Storrs and Regional Campuses
- UConn Health

# of Corrective Actions Implemented
Implemented

- High: 10
- Medium: 29
- Low: 24

Open OverDue Items by Risk Level

- High: 47
- Medium: 98
- Low: 92
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.
University of Connecticut
&
UConn Health

Joint Audit & Compliance Committee Meeting
Role
The University of Connecticut (UConn) Executive Risk Management and Compliance Committee (Committee) is appointed to provide direction and guidance to the UConn compliance, health and safety, and public safety risk management programs and advise the President and the Joint Audit and Compliance Committee (JACC) in their oversight of these programs. The Committee’s role is an essential component of the University’s overall risk management program, focusing on UConn’s compliance with significant legal, ethical, and regulatory requirements and on managing significant health and safety (health/safety) and public safety risks.

Membership
The Committee shall be comprised of the following:

- Chief of Staff to the President & Executive Secretary to the Board of Trustees, Committee Chair;
- Chief Audit, Compliance and Ethics Officer, Executive Secretary to the Committee;
- General Counsel, Committee Counsel;
- Vice Provost for Academic Affairs;
- Executive Vice President for Administration and Chief Financial Officer;
- Vice President for Enrollment, Planning, and Management;
- Vice President for Student Affairs;
- Vice President for Research;
- Deputy Director of Athletics/Chief of Staff;
- AVP for Institutional Equity; and,
- Vice Provost and CIO.

Staff support to the committee will be provided by the Office of Audit, Compliance and Ethics. Additional voting and non-voting members may be appointed by the Chair together with the President of the University. Representatives of other University areas may also be invited to attend, as appropriate.

A quorum for any meeting will be a majority of the voting members.

Generally, each Committee member shall be independent and free from any relationship which would interfere with the exercise of independent judgment as a member of the Committee. However, should an issue arise where any member recognizes a conflict, that member will note such conflict and recuse him/herself from discussions on the topic.

Meetings
The Committee shall meet on a regularly scheduled basis throughout the year but generally not less than four times per year, as circumstances dictate. Evidence of the discussions of the Committee and the actions taken by the Committee are to be reflected in recorded minutes of the meeting.
Responsibilities

The Committee’s specific responsibilities in carrying out its oversight are as follows:

1. Provide leadership for the UConn health/safety, public safety, and compliance risk management programs by promoting and supporting a culture that builds risk and compliance consciousness into the daily activities of UConn faculty and staff.

2. Provide advice and guidance to the President and the JACC on the design and operation of the health/safety, public safety, and compliance risk management programs.

3. Work closely with University managers to help ensure university-wide compliance with relevant state and federal laws and to provide a safe working environment for the UConn community.

4. Review and approve the role, responsibilities, and structure of the UConn health/safety, public safety, and compliance committees.

5. Review and approve the designation of specific UConn health/safety, public safety, and compliance coordinators.

6. Identify and assess health/safety, public safety, and compliance risks at UConn that require executive oversight.

7. Allocate resources, when necessary, to mitigate risks in activities determined to represent a high risk.

8. Receive results of all inspections and audits that have compliance, health/safety, or public safety implications.


10. Be apprised of general compliance training outcomes.

11. Keep the President and the JACC aware of identified risks, activities, and findings.

12. Provide a forum for communication among the various units and programs within UConn for issues relevant to health/safety, public safety, and compliance.

13. Perform any other activities consistent with this Charter and University, Schools and Colleges By-laws and governing laws, as this Committee or the Joint Audit and Compliance Committee of the Boards deem necessary or appropriate.

The Committee will review the components of this charter at least annually and update the charter, as necessary, to reflect current practices and needs.
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 FY2015.</td>
<td>Marcum, LLP presented their FY2015 audited financial statements at the February 3, 2016 JACC Meeting. FY2015 engagement complete.</td>
</tr>
<tr>
<td>RSM US LLP (formerly</td>
<td>Storrs, Regionals &amp;</td>
<td>Audit of UCONN 2000 named projects substantially completed during FY2015, deferred maintenance projects with designated budgets substantially completed in FY2015 and agreed upon procedures performed on total UCONN 2000 expenditures (named projects, deferred maintenance and equipment) for FY2015.</td>
<td>FY2015 engagement is underway. RSM LLP will present their FY2015 reports at the May 17, 2016 JACC meeting.</td>
</tr>
<tr>
<td>McGladrey LLP)</td>
<td>UConn Health</td>
<td></td>
<td></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 FY2015.</td>
<td>BKD presented their FY2015 reports at the December 1, 2015 JACC meeting. FY2015 engagement complete.</td>
</tr>
</tbody>
</table>
University of Connecticut & UConn Health

Joint Audit & Compliance Committee Meeting
University of Connecticut
Single Audit Report Excerpts
FYE 6/30/2015

- Issue Date – March 30, 2016

- Complete Statewide Report -

- Applicable University Federal Programs
  1) Research and Development
  2) Federal Student Financial Assistance (FSFA)
Federal Funds

- **Total Federal Assistance Statewide** - $9,160,000,000

**Type A Program Threshold**

<$10B = Larger of $3m or FFA * .003) - $27,480,000

- **Federal Assistance Expended at the University System:**
  1. University R&D $78,000,000
  2. Health Center R&D $67,000,000
  3. Student FFA $221,000,000 (Storrs $205m UCHC $16m)

  **TOTAL FFA** $366,000,000
Audit Findings – R&D

1. Equipment and Real Property Management (UCHC)

- Title 2 Code of Federal Regulations (CFR) Section 215.34 (g) and (f)(1)(ix) states that if the recipient has no need for certain equipment, the recipient shall request disposition instructions from the federal awarding agency. Valuation must be performed to determine if equipment has a current per-unit fair market value of $5,000 or more. Further, Title 2 CFR Part 200.313 (d)(3) states that a control system must be developed to ensure adequate safeguards are in place to prevent loss, damage, or theft of property. Any loss, damage, or theft must be investigated.

During our testing of the Health Center’s equipment inventory, we noted the following:

- There is no established control process in place which provides adequate documentation that a fair market valuation was performed on federal equipment as required.
- There were 41 federal equipment items disposed of that were classified as either lost, stolen or misplaced and were not investigated as required.

Agency Response – “We agree with this finding.”
2. Student Eligibility (University)

- Title 34 Code of Federal Regulations (CFR) Section 685.200(a)(1) states that a borrower is eligible to receive federal Direct Student Loans (Direct Loan), if the student is enrolled or accepted on at least a half-time basis in a school that participates in the Direct Loan program.

- Title 34 CFR Section 668.164(b)(3) stipulates that an institution may disburse Title IV, Higher Education Act program funds to a student or parent for a payment period only if the student is enrolled for classes for that payment period and is eligible to receive those funds.

From ten students selected for testing at the University, a graduate student was awarded and disbursed an unsubsidized Direct Loan of $10,141 that he was ineligible for. Upon our discovery, the university rescinded the ineligible Direct Loan award.

Agency Response – “We agree with this finding.”
3. Reporting (University)

- In order to participate in the federally funded campus-based programs, the university is required to report on operations in a “Fiscal Operations Report and Application to Participate” (FISAP). Instructions to complete the FISAP are contained in the *Instructions Booklet for Fiscal Operations Report for 2014–2015 and Application to Participate for 2016–2017 (FISAP)*.

We reviewed the FISAP at the University and noted a number of reporting errors concerning amounts of aid disbursed, students served, and certain required statistics.

*Agency Response – ‘We agree with the finding.’*
Audit Findings - FSFA

4. Special Tests: Verification (University)

- Title 34 Code of Federal Regulations (CFR) Section 668.53 requires an institution to establish policies for verifying information contained in a student aid population.
- Title 34 CFR Section 668.56 requires that an institution must verify all Free Applications for Federal Student Aid (FAFSA) that have been selected for verification.

From ten students selected for verification testing at the University, we noted one instance in which the number of persons in the household size, and in college, reported on the verification worksheet did not agree with the reported amounts on the Institutional Student Information Report. Upon our discovery, the university returned $850 of federal Pell Grant funds.

Agency Response – ‘We agree with the finding.’
Audit Findings - FSFA

5. Special Tests: Return of Title IV Funds (University)

- Title 34 Code of Federal Regulations Section 668.22 provides guidance regarding the treatment of Title IV funds when a student withdraws from an institution. Per related guidance, if a student who began attendance and has not officially withdrawn fails to earn a passing grade in at least one course offered over an entire period, the institution must assume, for Title IV purposes, that the student has unofficially withdrawn, unless the institution can document that the student completed the period.

We selected 12 students for Return of Title IV Funds testing at the University, and noted two instances where a required calculation was not performed. Upon our discovery, the university returned the required $6,272 of federal Direct Student Loan Program funds.

Agency Response – “We agree with the finding.”
Audit Findings - FSFA

6. Special Tests: Student Loan Repayments (University)

- Title 34 Code of Federal Regulations Section 674.31(b)(2) states that repayment begins nine months after the borrower ceases to be at least a half-time regular student at the institution. Further, an institution is required to conduct exit counseling with the borrower before the student ceases to be enrolled on at least a half-time basis.

- The FSA Handbook further states that a grace period is always day specific, an initial grace period begins on the day after the day the borrower drops below half-time enrollment.

We selected ten borrowers at the University who entered repayment during the audited period and noted the following:

- In two instances, borrowers were put into repayment early.
- In two instances in which the university was aware that the borrower was graduating, exit counseling was not conducted before the end of the semester.
- In one instance in which the university was aware that the borrower ceased to be at least half-time, exit counseling was not conducted timely.
- In eight instances, the separation date, grace period end date, and first payment due date was inconsistent.

Agency Response – “We agree with the finding.”
Audit Findings - FSFA

7. Special Tests: Student Loan Repayments – Default (University)

- Title 34 Code of Federal Regulations Section 674.42(c) requires that an institution must contact a federal Perkins Loan borrower with a nine-month grace period at the 90-day, 150-day and 240-day point of the grace period.
- The 2014-2015 Federal Student Aid Handbook states that a grace period is always day specific. An initial grace period begins on the day after the day the borrower drops below half-time enrollment.

We selected an additional ten borrowers at the University whose loan went into default during the audited period and noted the following:

- Nine instances where the grace period was inconsistent for borrowers who separated, which caused the required grace letters to be sent untimely.
- One instance in which the required 90-day contact letter was not sent to the borrower. It was also noted that the borrower had the incorrect separation date.

Agency Response – “We agree with the finding.”
Audit Findings - FSFA

8. Institutional Eligibility (University)

- Per Title 34 Code of Federal Regulations 668.14(a)(1), an institution may participate in any Title IV, Higher Education Act (HEA) program, only if the institution enters into a written program participation agreement with the Secretary, on a form approved by the Secretary. A program participation agreement conditions the initial and continued participation of an eligible institution in any Title IV, HEA program upon compliance with the provisions of this part, the individual program regulations, and any additional conditions specified in the program participation agreement that the Secretary requires the institution to meet.

- The University did not include its Sixth-Year Graduate Certificate programs, for which federal aid was offered, on its application to participate in the federal student financial aid programs. The Program Participation Agreement for UConn, effective October 7, 2014, with an expiration date of June 30, 2017, did not include these Sixth-Year programs. We identified 63 students enrolled in Sixth-Year Graduate Certificate programs that received total Direct Loans of $918,975 during the current audited year.

Agency Response – “We agree with the finding.”
Title 34 Code of Federal Regulations Section 668.5(d)(3) states the institution that calculates and disburses a student's Title IV, Higher Education Act program assistance must take into account all the hours in which the student enrolls at each institution that apply to the student's degree or certificate when determining the student's enrollment status and cost of attendance.

During our review of ten consortium agreements at the University, we noted four instances in which a student’s incorrect enrollment status was reported to the National Student Loan Data System (NSLDS).

Agency Response – “We agree with the finding.”
UNIVERSITY OF CONNECTICUT

2015-500 Allowable Costs/Cost Principles – Conflict of Interest (University of Connecticut)

Federal Award Agency: National Science Foundation
Award Year: State Fiscal Year Ended June 30, 2015
Research and Development Programs:

Computer and Information Science and Engineering (CFDA #47.070)
Account #5616460 – “TWC: Medium: DoS Attacks and Countermeasures in Underwater Wireless Networks” – CNS-1228936 issued by the National Science Foundation, project period September 1, 2012 through August 31, 2016

Computer and Information Science and Engineering (CFDA #47.070)
Account #5615600 – “Collaborative Research: CI-ADDO-New: Ocean Tune: A Community Ocean Testbed for Underwater Wireless Networks” – CNS-1205665 issued by the National Science Foundation, project period June 1, 2012 through May 31, 2015

Computer and Information Science and Engineering (CFDA #47.070)
Account #5616480 – “NRI-Small: Cooperative Underwater Robotic Networks for Discovery & Rescue” – IIS-1208499 issued by the National Science Foundation, project period September 1, 2012 through August 31, 2016

Criteria: Per the National Science Foundation Proposal and Award Policies and Procedures Guide, Part II – Award & Administrative Guide, each grantee organization employing more than fifty persons is required to maintain and enforce an appropriate written policy on conflicts of interest. Any identified conflicts of interest are to be managed, reduced or eliminated prior to the expenditure of the award funds.

Condition: National Science Foundation funds administered by the University of Connecticut (UConn) were used to purchase 15 specialized acoustic modems from a vendor between April and August of 2013 at a total cost of $253,500. Charges to accounts 5616460, 5615600 and 5616480 were $35,000, $175,000 and $43,500, respectively. The transactions were processed as sole source purchases and were initiated by UConn faculty who had a significant financial interest in such vendor. Three purchase requisitions were involved. Two of the three purchase requisitions, which included the statement "I certify . . . that I have no financial or other beneficial interest in the vendor," were signed by faculty that did, in fact, have an interest in the vendor.

The two faculty members involved stated that they did not read the portion of the sole source justification form they signed that contained a certification that they had no interest in the vendor. They subsequently submitted amended
Significant Financial Interest forms (Significant Financial Interest forms initially completed during the proposal stage of the award process did not disclose their conflicts of interest) that disclosed their conflicts of interest to the University of Connecticut’s Sponsored Program Services department prior to the procurement action. However, the Procurement Services department was not notified that this conflict of interest existed.

**Effect:**
The University of Connecticut did not ensure that all conflicts of interest were appropriately managed, reduced or eliminated prior to the expenditure of the award funds for each award.

**Cause:**
Control procedures in place were not adequate to ensure that all concerned parties were notified of this disclosure.

**Conclusion:**
The University of Connecticut reversed the charges to the award accounts for the modems and took steps to improve internal control in response to this incident.

**Agency Response:**
“As outlined in the conclusion section above the University has taken steps to improve internal controls and minimize continued risk in this area. The Financial Conflict of Interest in Research Committee (FCOIRC) was expanded to include broader representation of the campus community, which includes a representative from the Office of Procurement Services. A list of known faculty owned companies is also maintained by the Office of the Vice-President for Research and provided to Procurement Services on a quarterly basis. In addition, Procurement Services has implemented a number of measures in response to this matter. Specifically, for a sole source procurement, the requestor now must certify by both separate initial and signature, not to have a financial or other beneficial interest with the identified vendor. OVPR, FCOIRC and Procurement Services procedures and forms have been updated to reflect these changes.”
UNIVERSITY OF CONNECTICUT HEALTH CENTER

2015-550    Equipment and Real Property Management

Federally-Sponsored Research and Development Programs
Federal Award Agency: Various Federal Agencies
Award Year: State Fiscal Year Ended June 30, 2015
Federal Award Numbers: Various

Criteria: Title 2 Code of Federal Regulations (CFR) Part 215.34 (g) and (f)(1)(ix) states that if the recipient has no need for certain equipment items, the recipient shall request disposition instructions from the federal awarding agency. For equipment with a current per-unit fair market value of $5,000 or more, the recipient may retain the equipment for other uses provided that compensation is made to the original federal awarding agency or its successor. The amount of compensation shall be computed by applying the percentage of federal participation in the cost of the original project or program to the current fair market value of the equipment.

The recipient's property management standards for equipment acquired with federal funds and federally-owned equipment shall include disposition data, including the date of disposal and sales price, or specify the method used to determine current fair market value when a recipient compensates the federal awarding agency for its share.

2 CFR Part 200.313 (d)(3) states that a control system must be developed to ensure adequate safeguards are in place to prevent loss, damage, or theft of the property. Any loss, damage, or theft must be investigated.

Condition: During our testing of the University of Connecticut Health Center (UConn Health) equipment inventory we noted the following exceptions:

One item which may have had a fair market value greater than $5,000 dollars was not presented to the federal awarding agency for disposal instructions prior to disposition. UConn Health does not have an established control process in place which provides adequate documentation that a fair market valuation was performed on federal equipment which has a possible fair market value greater than $5,000 prior to the disposal.

There were 41 federal equipment items disposed of that were classified as either lost, stolen or misplaced and not investigated as required by the federal awarding agency. The original cost of the items ranged from $5,405 to $55,675. We noted three of these items had book value ranging from $111 to
$3,919. During further review, we estimated that seven of these items may have had fair market value greater than $5,000.

**Effect:**
UConn Health’s equipment inventory disposal records do not demonstrate compliance with the cost principals and administrative requirements established by 2 CFR Part 215.34 (g) and (f)(1)(ix) and Part 200.313 (d)(3).

**Cause:**
UConn Health was not fully aware of the federal compliance requirement pertaining to disposal of federal equipment.

**Recommendation:**
The University of Connecticut Health Center should ensure that it performs the required fair market valuations on items with an estimated fair market value of $5,000 or more, and contacts the federal awarding agency for disposition instructions on items meeting this threshold. Steps should also be taken to ensure that all safeguards are in place to prevent loss or theft of federal equipment and any missing equipment must be investigated.

**Agency Response:**
“UConn Health followed guidance related to processes for state entities which required we follow existing State guidelines issued by the Comptroller of the State of Connecticut. These guidelines include provisions for tracking of assets, proper disposal, and taking of inventory. After reviewing with the Auditors of Public Accounts, we agree that the provisions related to Institutions of Higher Education, including provisions over fair value of disposed items funded by Federal Agencies, are also applicable.

In addition, UConn Health will add procedures that establish review criteria for federally funded assets including an evaluation as to their current estimated fair value as required for Institutions of Higher Education. Assets estimated to meet the $5,000 threshold will be held for review and further instruction by the awarding agency as prescribed. We will also continue our efforts to streamline asset reporting and staff education to prevent improper disposals.”
Student Eligibility

Federal Direct Student Loans (CFDA #84.268)
Federal Award Agency: United States Department of Education
Award Year: 2014-2015

Criteria: Title 34 Code of Federal Regulations (CFR) Section 685.200(a)(1) states that a borrower is eligible to receive federal Direct Student Loans (Direct Loan), if the student is enrolled or accepted, on at least a half-time basis in a school that participates in the Direct Loan program.

Title 34 CFR Section 668.164(b)(3) stipulates that an institution may disburse Title IV, Higher Education Act program funds to a student or parent for a payment period only if the student is enrolled for classes for that payment period and is eligible to receive those funds.

Condition: From ten students selected for testing, an enrollment status of full-time was determined for a graduate student based on undergraduate courses that this student had enrolled in that would not count toward his degree, which he dropped on the last day of the add/drop period after his Direct Loan had disbursed. This student was not eligible to receive a Direct Loan as his enrollment status should have been determined to be less-than-half time based on the graduate course he was enrolled in that could be counted toward his graduate degree program.

A student was awarded and disbursed an unsubsidized Direct Loan of $10,141 that he was ineligible for. Upon our discovery, the university rescinded the ineligible Direct Loan award.

Cause: We were informed that the condition occurred when an individual who packaged the award thought the undergraduate courses were replacements for graduate program requirements.

Recommendation: The University of Connecticut should establish procedures to ensure that only courses that count toward a student’s degree, certificate, or other recognized credential are used to determine enrollment status unless they are eligible remedial courses.

Agency Response: We agree with this finding.

Corrective Action Plan: We agree with this finding. In early January 2016 we enhanced the Census Date Aid Reconciliation procedures to outline the graduate student enrollment review process. Should a graduate student enroll in undergraduate level courses, the courses are not to be counted toward the half time (+) enrollment unless the office receives documentation from the Dean of the
Graduate School (or designee) confirming that the courses serve as substitutes for graduate program requirements.

By January 30, 2016 the university will have reviewed the entire 2014/15 graduate level Direct Loan recipient population to ensure full compliance.

**Anticipated Completion Date:** January 29, 2016

---

**Reporting – Fiscal Operations Report and Application to Participate (FISAP)**

- **Federal Supplemental Educational Opportunity Grants (CFDA #84.007)**
- **Federal Work-Study Program (CFDA #84.033)**
- **Federal Perkins Loan – Federal Capital Contributions (CFDA #84.038)**
- **Federal Pell Grant Program (CFDA #84.063)**

**Federal Award Agency:** United States Department of Education  
**Award Year:** 2014-2015

**Criteria:** The instructions for completing the FISAP are contained in the *Instructions Booklet for Fiscal Operations Report for 2014–2015 and Application to Participate for 2016–2017 (FISAP)*.

**Condition:** We reviewed the FISAP at the University of Connecticut and noted the following:

- The total expended for state grants and scholarships made to undergraduates were reported as $4,629,055. The supporting documentation for the amount was $4,594,405. Upon our discovery, the university submitted a FISAP correction.
- The total number of independent professional students was reported as 3,264 in the Eligible Aid Applicant Information part of the FISAP. The supporting documentation for this amount was 3,270. Upon our discovery, the university submitted a FISAP correction.
- The expended Federal Work-Study Program (FWS) authorization was reported as $1,266,327 on the FISAP. The supporting documentation for drawdowns in G5 was $1,279,354.
- The total FWS earnings of the students for whom jobs were located or developed were reported as $3,405,000. The supporting documentation for this amount was $3,492,042. This condition was self-identified by the school; the university submitted a FISAP correction.

In our Statewide Single Audit covering the fiscal year ended June 30, 2014, we recommended that the university make corrections to the FISAP data submitted for award year July 1, 2013 through June 30, 2014, to the total number of students, and the amount of tuition and fees that were reported, due to reporting errors. The Office of Student Financial Aid Services provided us with a screen print of the FISAP Change Request Confirmation submitted on April 14, 2015. We were informed that the United States Department of Education Campus-Based Program office did not respond to the request, and did not reopen the FISAP to allow for the changes.
to these fields. Upon our discovery, the university re-contacted the federal government and submitted FISAP corrections on December 11, 2015, for the line items below:

- The total number of undergraduate and graduate/professional students was reported as 25,756 and 7,961, respectively. The supporting documentation for these amounts was 25,039 and 8,678, respectively.
- The total tuition and fees for undergraduate and graduate/professional students was reported as $331,179,707 and $144,976,850, respectively. The supporting documentation for these amounts was $334,258,285 and $140,714,322, respectively.

**Effect:**
The FISAP that the university submitted to the United States Department of Education contained errors. If an institution provides inaccurate data, the level of funding for its campus-based programs could be affected.

**Cause:**
A newly created university scholarship was included in the amount expended for state grants and scholarships to undergraduate students even though the university has the final decision on which students get the funds. Also, departments inadvertently submitted inaccurate summary information to the office responsible for the submission of the FISAP. Controls were not in place to monitor the information provided prior to data entry.

**Recommendation:**
The University of Connecticut should establish internal controls to ensure that data reported on the Fiscal Operations Report and Application to Participate (FISAP) is accurate and in compliance with instructions provided by the United States Department of Education. The University of Connecticut should make necessary corrections to the FISAP data submitted for award year July 1, 2014 through June 30, 2015 to the Federal Work-Study Program amounts, as necessary.

**Agency Response:**
We agree with this finding.

**Corrective Action Plan:**
We agree with this finding. The Office of Student Financial Aid Services has submitted the FISAP corrections identified. Further, we will enhance our FISAP “second look” review process documented procedures in order to better identify and address errors prior to filing the report and subsequently sharing it along with the supporting documentation with the state auditors on October 1st. The office will also enhance the FISAP Completion Work Plan in order to allow for additional time for the FISAP “second look” review process.

**Anticipated Completion Date:** March 1, 2016

**Special Tests: Verification**

**Federal Supplemental Educational Opportunity Grants (CFDA #84.007)**
**Federal Work-Study Program (CFDA # 84.033)**
Federal Perkins Loan Program – Federal Capital Contributions (CFDA # 84.038)
Federal Pell Grant Program (CFDA # 84.063)
Federal Direct Student Loans (CFDA # 84.268)
Federal Award Agency: United States Department of Education
Award Year: 2014-2015

Criteria: Title 34 Code of Federal Regulations (CFR) Section 668.53 requires an institution to establish policies for verifying information contained in a student aid population.

Title 34 CFR Section 668.56 requires that an institution must verify all Free Applications for Federal Student Aid that have been selected for verification.

Items that are required to be verified include household size, number of household members who are in college, food stamps (Supplemental Nutrition Assistance Program), child support paid, adjusted gross income, U.S. income taxes paid, education credits, Individual Retirement Account deductions, tax exempt interest, and certain types of untaxed income and benefits. The financial aid office verifies student and parental income and household data by comparing financial data found on tax-related documents to data found on the Institutional Student Information Report (ISIR). Furthermore, it confirms household data and other untaxed income items found on the verification worksheet to data found on the ISIR.

Condition: From ten students selected for verification testing at the University of Connecticut, we noted one instance in which the number of persons in the household size and in college reported on the verification worksheet did not agree with the reported amounts on the ISIR.

Effect: The university was not in compliance with verification requirements. The student’s Expected Family Contribution amount and award was affected. The overpayment of federal Pell awards to the student was $850. Upon our discovery, the university processed an adjustment to the Pell program.

Cause: Established verification procedures were not followed.

The employee in the financial aid office performing the review marked the verification checklist completed, while the required items were not verified.

Recommendation: The University of Connecticut should review its procedures to ensure compliance with the federal regulations pertaining to verification.

Agency Response: We agree with this finding however the recommendation is already standard operating procedure.
Corrective Action Plan:
We agree with this finding. The verification mistake was a result of human error. The employee who made the error is quite experienced and well aware of the Verification requirements.

Regardless of our staff’s financial aid experience, we conduct mandatory in-service training sessions every year to review the federal verification criteria, as UCONN policies and documented procedures prior to going into production for the new year. We also conduct a departmental verification audit each December using the Department of Education Student Financial Aid Assistance audit worksheets.

We recognize that Verification continues to be one of the national top 10 audit and program review findings each year. For this reason we conduct a departmental self-audit of a percentage of files that have been verified. For example, during the late Fall 2014 we reviewed 263 previously verified files to double check our work. During the Fall 2015 we reviewed 270 previously verified files. The results of our annual self-audit did not lead us to believe that systemic issues related to Verification exist.

Anticipated Completion Date: September 2015

Special Tests: Return of Title IV Funds

Federal Supplemental Educational Opportunity Grants (CFDA #84.007)
Federal Work-Study Program (CFDA #84.033)
Federal Perkins Loan – Federal Capital Contributions (CFDA #84.038)
Federal Pell Grant Program (CFDA #84.063)
Federal Direct Student Loans (CFDA #84.268)
Teacher Education Assistance for College and Higher Education Grants (CFDA #84.379)
Federal Award Agency: United States Department of Education
Award Year: 2014-2015

Criteria: Title 34 Code of Federal Regulations Section 668.22 provides guidance regarding the treatment of Title IV funds when a student withdraws from an institution.

Per Dear Colleague Letter GEN-04-03, if a student who began attendance and has not officially withdrawn fails to earn a passing grade in at least one course offered over an entire period, the institution must assume, for Title IV purposes, that the student has unofficially withdrawn, unless the institution can document that the student completed the period.

Condition: Twelve students were selected for Return of Title IV Funds testing at the University of Connecticut. We noted the following:
- Two students who withdrew from the university in the fall 2014 semester did not have a Return of Title IV Funds calculation performed. Per audit calculation, a total of $6,272 should have been
returned to the federal Direct Student Loans (Direct Loan) program. Upon our discovery, the university returned the funds. However due to the error and subsequent correction, the funds were returned 354 and 313 days after the 45-day deadline for the return of funds.

- In one instance, there was a delay of eight days in the return of $1,785 to the Direct Loan program.

**Effect:**

The university was not in compliance with the federal regulations governing the Return of Title IV Funds.

Students for who Title IV refunds were not calculated were allowed to retain 100 percent of their federal aid. Upon audit notification, the university returned $6,272 to the Direct Loan program.

The Return of Title IV funds did not occur with the established deadlines.

**Cause:**

Institutional policy and protocol were not followed by certain regional/professional school staff, and therefore did not trigger the appropriate action by other university offices.

**Recommendation:**

The University of Connecticut should review its procedures to ensure compliance with the federal regulations contained in Title 34 Code of Federal Regulations Section 668.22 governing the treatment of Title IV funds when a student withdraws. The University of Connecticut should ensure that all staff responsible for collecting information necessary for the Return of Title IV Funds process is adequately trained.

**Agency Response:**

We agree with this finding.

**Corrective Action Plan:**

We agree with this finding. As of the first day of the spring semester, January 19, 2016, the Graduate School will process withdrawals for graduate students for all professional schools. This will ensure the withdrawals are processed correctly, triggering the Return of Title IV Funds. Additional university-wide trainings are scheduled to ensure policy and protocol are followed.

**Anticipated Completion Date:** January 2016

**Special Tests: Student Loan Repayments**

**Federal Perkins Loan – Federal Capital Contributions (CFDA #84.038)**

**Federal Award Agency:** United States Department of Education

**Award Year:** 2014-2015

**Criteria:**

Title 34 Code of Federal Regulations (CFR) Section 674.31(b)(2) states that repayment begins nine months after the borrower ceases to be at least a half-time regular student at the institution.
Title 34 CFR Section 674.42(b) requires an institution to conduct exit counseling with the borrower either in person, by audiovisual presentation, or electronically before the student ceases to be enrolled on at least a half-time basis. If a borrower withdraws without the institution’s prior knowledge or fails to complete an exit counseling session, the institution must provide the exit counseling material to the borrower within 30 days.

The 2014-2015 Federal Student Aid Handbook states that a Perkins borrower is entitled to an initial grace period of nine consecutive months after dropping below half-time enrollment. If the borrower returns to school on at least a half-time basis before the nine months has elapsed, the initial grace period has not been used. The borrower is entitled to a full initial grace period of nine consecutive months from the date that he or she graduates, withdraws or drops below half-time enrollment again.

The Federal Student Aid Handbook further states that a grace period is always day specific, an initial grace period begins on the day after the day the borrower drops below half-time enrollment.

**Condition:**
From a sample of ten borrowers at the University of Connecticut who entered repayment during the audited period, we noted the following:

- In two instances in which the university was aware that the borrower was graduating, exit counseling was not conducted before the end of the semester. The exit counseling was conducted 31 and 38 days after the end of the semester.
- In one instance in which the university was aware that the borrower ceased to be at least half-time, exit counseling was not conducted within 30 days. The exit counseling materials were sent 26 days late.
- In two instances borrowers were put into repayment early. One borrower was put into repayment three months early and only received six months of his entitled nine month grace period; and one borrower was put into repayment one year early and subsequently placed into student deferment.
- In eight instances, the separation date, grace end date, and first payment due date was inconsistent for borrowers whose term end date prior to dropping below half-time status was May 10, 2014. Six of these borrowers had a separation date of May 11, 2014, a grace end date of March 1, 2015, and began repayment on April 1, 2015; and two borrowers had a separation date of May 10, 2014, a grace end date of February 1, 2015, and began repayment on March 1, 2015. The May 10, 2014 separation date should have been used as that is the effective status date reported on the National Student Loan Data System.

**Effect:**
The university was not in compliance with federal due diligence requirements.

**Cause:**
The university’s procedures are not in compliance with the federal regulations governing repayment and exit counseling.
University procedures during our audited period were to send an anticipated graduation list to its service provider after four weeks into the semester when the deadline for students to apply for graduation was over. We were informed exit counseling was not conducted before graduation for those students that self-certified graduation candidate status or where changes were made to the expected graduation term late in the semester.

We were informed that the program used for billing by the university’s service provider starts counting the grace period at the beginning of the month following separation as bills are sent out once a month in order to ensure that the full nine month grace period is provided. The calculations are based on a flag that is set on the school file record. The first payment due date is then one month following the grace period end date. If the flag was not set, then the grace period will begin the first of the month of the separation.

**Recommendation:** The University of Connecticut should ensure that policies and procedures regarding Perkins Loans repayments and exit counseling are in compliance with the federal regulations.

**Agency Response:** We agree with this finding.

**Corrective Action Plan:**

We agree with this finding. Since the Spring 2014 semester, the University has further enhanced our procedures by sending our third party servicer additional anticipated graduation lists after the deadline to apply has passed. This will ensure students who apply late are given exit counseling before graduation. Additionally, starting in the Spring 2015 semester, the University began reconciling the anticipated graduation list with the actual graduation list to ensure students who have not yet graduated even though they have applied, are not separated.

The third party servicer was using two different exit programs resulting in inconsistent “grace” start dates. In October 2015, we instructed them to change the program logic to accurately reflect the appropriate dates.

**Anticipated Completion Date:** January 2016

**Special Tests: Student Loan Repayments - Default**

**Federal Perkins Loan – Federal Capital Contributions (CFDA #84.038)**

**Federal Award Agency:** United States Department of Education

**Award Year:** 2014-2015

**Criteria:** Title 34 Code of Federal Regulations Section 674.42(c) requires that an institution must contact a federal Perkins Loan borrower with a nine-month grace period at the 90-day, 150-day and 240-day point of the grace period.
The 2014-2015 Federal Student Aid Handbook states that a grace period is always day specific, an initial grace period begins on the day after the day the borrower drops below half-time enrollment.

**Condition:**
We selected ten borrowers at the University of Connecticut whose loan went into default during the audited period and noted the following:

- One instance where the required 90-day contact letter was not sent to the borrower. It was also noted that the borrower had the incorrect separation date. The borrower’s separation date was December 15, 2012; however, the separation date that was recorded by the university’s service provider was January 15, 2013.

- Nine instances where the grace period was inconsistent for borrowers who separated, which caused the required grace letters not to be sent timely. In six of these instances, the university’s service provider notified borrowers that their grace end date was on the first of the month following the actual grace ending date. In three of these instances, the university’s service provider notified the borrower’s that their grace end date was the first of the month prior to the actual grace ending date.

**Effect:**
The university was not in compliance with federal due diligence requirements.

In the absence of completing the federal due diligence requirements, the likelihood that the university may not collect outstanding loan funds is increased.

In the instances where the university’s service provider notified borrowers that their grace end date was on the first of the month following the actual grace ending date, these grace letters were generally sent late. In the instances where the university’s service provider notified the borrower’s that their grace end date was the first of the month prior to the actual grace ending date, these grace letters were sent early.

**Cause:**
The first required contact letter to one borrower selected in our sample was not sent due to this student being separated late.

We were informed that the program used for billing by the university’s service provider starts counting the grace period at the beginning of the month following separation as bills are sent out once a month in order to ensure that the full nine month grace period is provided. The calculations are based on a flag that is set on the school file record. The first payment due date is then one month following the grace period end date. If the flag was not set, then the grace period will begin the first of the month of the separation.

**Recommendation:**
The University of Connecticut should ensure that policies and procedures regarding Perkins Loans due diligence requirements are being performed in accordance with federal regulations.

**Agency Response:**
We agree with this finding.
Corrective Action Plan:

We agree with this finding. The University’s third party servicer, was using two different exit programs resulting in inconsistent “grace” start dates. In October 2015, we instructed them to change the program logic to accurately reflect the appropriate dates. Based upon the inconsistent start dates of the grace periods, as mentioned in the previous finding, this affected the timing of the required grace letters deeming them incorrect as well. These two findings are linked and were a result of the use of inconsistent exit programs.

Anticipated Completion Date: January 2016

Special Tests: Written Arrangements

Federal Supplemental Educational Opportunity Grants (CFDA #84.007)
Federal Work-Study Program (CFDA # 84.033)
Federal Perkins Loan Program – Federal Capital Contributions (CFDA # 84.038)
Federal Pell Grant Program (CFDA # 84.063)
Federal Direct Student Loans (CFDA # 84.268)
Federal Award Agency: United States Department of Education
Award Year: 2014-2015

Background: If an enrolled student is unable to complete required classes at the host institution, then an approved consortium agreement may be used to allow the student to take the required course(s) at another eligible institution and retain financial aid.

Criteria: Title 34 Code of Federal Regulations Section 668.5(d)(3) states the institution that calculates and disburses a student's Title IV, Higher Education Act program assistance must take into account all the hours in which the student enrolls at each institution that apply to the student's degree or certificate when determining the student's enrollment status and cost of attendance.

Condition: During our review of ten consortium agreements at the University of Connecticut, we noted four instances where a student’s incorrect enrollment status was reported to the National Student Loan Data System (NSLDS).

Effect: Inaccurate enrollment information was sent to the NSLDS, which affected these students enrollment reporting status.

Cause: The university did not include the credit hours in which students were enrolled at another institution under an approved consortium agreement when reporting enrollment information to the NSLDS.

Recommendation: The University of Connecticut should implement procedures to ensure that applicable consortium agreement credits are accounted for in determining student’s enrollment status. Additionally, the university should ensure that
enrollment information reported to the National Student Loan Data System is timely and accurate, in accordance with federal regulations.

Agency Response: We agree with this finding.

Corrective Action Plan: We agree with this finding. In November 2015 the Office of Student Financial Aid Services has identified all students with Consortium Agreement approvals from 2013-2014 forward as well as their federal student loan servicers. Deferment requests were completed by the Registrar’s Office and sent to the loan servicers to report accurate enrollment status impacting the grace period and repayment calculations. The instances noted in this finding were included in the University’s corrective plan in November 2015.

Furthermore, the Office of Student Financial Aid Services worked with the Office of the Registrar to establish enhanced procedures to ensure students’ enrollment status is being reported correctly to the National Student Loan Clearing House for students with active consortium agreements participating in a consortium agreement. Effective December 2015 the Office of Student Financial Aid Services monitors all consortium students by confirming the enrollment status with the host school every thirty days. Any enrollment changes are reported to the Registrar’s Office, during the first week of the month, so that the accurate enrollment status is reported to the National Clearing House.

Anticipated Completion Date: November 2015

Institutional Eligibility

Federal Work-Study Program (CFDA # 84.033)
Federal Perkins Loan Program – Federal Capital Contributions (CFDA # 84.038)
Federal Direct Student Loans (CFDA #84.268)
Federal Award Agency: United States Department of Education
Award Year: 2014-2015

Background: Per the 2014-2015 Federal Student Aid Handbook, to participate in the Federal Student Aid programs, a school must apply to and receive approval from the United States Department of Education. The Sixth-Year diploma is not a degree but is generally recognized as an academic credential beyond the master’s degree. In general, the school’s eligible non-degree programs are specifically named on the Eligibility and Certification Approval Report. Per Office of Management and Budget Form No. 1845-0012, Application for Approval to Participate in Federal Student Financial Aid Programs, Section E, an institution is required to provide information for each educational program that it is requesting to be eligible to participate in federal student financial aid programs that will be provided as of the date of the application or that will be provided during the current award year.
Criteria: Per Title 34 Code of Federal Regulations 668.14(a)(1), an institution may participate in any Title IV, Higher Education Act (HEA) program, other than the Leveraging Educational Assistance Partnership and National Early Intervention Scholarship and Partnership programs, only if the institution enters into a written program participation agreement with the Secretary, on a form approved by the Secretary. A program participation agreement conditions the initial and continued participation of an eligible institution in any Title IV, HEA program upon compliance with the provisions of this part, the individual program regulations, and any additional conditions specified in the program participation agreement that the Secretary requires the institution to meet.

Condition: The University of Connecticut (UConn) did not include its Sixth-Year Graduate Certificate programs, for which federal aid was offered and disbursed, on its application to participate in the federal student financial aid programs. The Program Participation Agreement (PPA) for UConn, effective October 7, 2014 with an expiration date of June 30, 2017, did not include these Sixth-Year programs.

In our Statewide Single Audit covering the fiscal year ended June 30, 2014, we noted the same condition. In that report, we disclosed that the university reported that 70 students enrolled in Sixth-Year Graduate Certificate programs received federal Direct Student Loans (Direct Loan) of $868,964; Grad PLUS loans of $154,800; Federal Perkins Loans of $10,000; and Federal Work-Study of $3,000 during the fiscal year ended June 30, 2014.

Subsequent to this condition being disclosed, UConn has been working diligently with the United States Department of Education regarding resolution of this matter. As of December 1, 2015, the university has returned the prior year questioned costs associated with the Federal Perkins Loans and the Federal-Work-Study award was cancelled.

Effect: The university offered federal aid to students enrolled in Sixth-Year Graduate Certificate programs, which were not included on the university’s PPA. We identified 63 students enrolled in Sixth-Year Graduate Certificate programs that received federal Direct Loans of $918,975 during the current audited year.

Cause: The university’s procedures for students enrolled in Sixth-Year Graduate Certificate programs were to classify these students as 2nd Master’s Degree students.

Recommendation: The University of Connecticut should ensure its procedures are in compliance with federal requirements governing eligible non-degree programs for participation in the federal student financial aid programs. The university should obtain approval from the United States Department of Education for authorization to award federal aid to Sixth-Year Graduate Certificate
program students. The university should continue to work with the United States Department of Education regarding resolution of this finding.

*Agency Response:* We agree with this finding.

*Corrective Action Plan:*  
We agree with this finding. On January 22, 2016, the School of Education Sixth-Year Graduate Certificate programs have been designated “eligible certificate programs” and officially added to the UConn Program Participation Agreement.

*Anticipated Completion Date:* January 2016
University of Connecticut
&
UConn Health

Joint Audit & Compliance Committee Meeting
State Code of Ethics Enforcement Update

The Office of State Ethics announced a former state employee agreed to pay $5,000 to settle Ethics Code Violations. According to the Office of State Ethics’ press release, the individual operated a private business using state time and resources including use of his work computer, e-mail account, and his state-provided office space. The former employee also accepted clients into his private practice that were referred to him by another employee.

According to the State Code of Ethics, public officials and state employees are prohibited from using their positions to obtain personal financial gain. Additionally, the decision to accept clients into his personal practice could have affected the clients’ access to state funds and services and impaired the employee’s judgment as to his state responsibilities.

This situation demonstrates the real-life consequences associated with violating the State Code of Ethics. All employees of the university are expected to be familiar with the Code of Ethics and comply with all of its provisions. In an effort to assist employees in determining what conduct is prohibited so that it may be avoided, the University also maintains a Guide to the State Code of Ethics at http://policy.uconn.edu/?p=387. Faculty members should also be aware of the University’s Consulting Policy and Procedures, as it specifically addresses consulting, private professional practice, teaching, and other outside employment situations.

Non-Retaliation Reminder

The University’s Non-Retaliation Policy defines how the University provides protection for any person or group within its community, who, in good faith, reports or participates in the investigation of alleged violations of policies, laws, rules or regulations applicable to the University. The University encourages individuals to bring forward information and/or complaints about the types of violations noted above as well as violations of state and/or federal law. The policy does not protect an individual who files a false report, provides false information as part of an investigation, files a bad faith retaliation claim, or who participates in illegal conduct.

Please review the full policy at: http://policy.uconn.edu/?p=415.

If you believe you have been subjected to retaliation, you should contact the office to which the initial complaint was filed, or any of the specific University offices noted in the policy.
Each year, the University of Connecticut offers a wide range of opportunities for non-matriculated minors (individuals under the age of 18) to participate in University-sponsored activities. As we prepare to enter the peak season for these type of activities, we wanted to make you aware of some of the initiatives underway for University-sponsored activities involving minors.

**Overview of Program**

**What is the purpose of the Minor Protection Program?**

The Minor Protection Program establishes consistent standards intended to support the University in meeting its commitments to promote the protection of minors who participate in activities sponsored by the University and to inform all members of the University community of their obligation to report any instances of known or suspected child abuse or neglect.

**What does the program entail and who is required to participate?**

The program incorporates training and education, a centralized system for registering youth programs, guidance on reporting child abuse and neglect, background checks for individuals supervising minors, and other requirements and resources. Program participation is mandatory for University-sponsored activities involving minors.

**What is a “University Sponsored Activity Involving Minors”?**

A program or activity open to the participation of minors that is sponsored, operated, or supported by the University and where minors, who are not enrolled or accepted for enrollment in credit-granting courses at the University or who are not an employee of the University, are under the supervision of the University or its representatives.

**Important Reminders?**

**How is the term “minor” defined?**

Any individual under the age of 18, who has not been legally emancipated.

**If I have any concerns about a minor, who do I contact?**

Pursuant to state law, all University employees (except student employees) are Mandated Reporters of Child Abuse and/or Child Neglect and must comply with the reporting requirements in Connecticut’s mandated reporting laws. For additional guidance on where and how to report known or suspected child abuse visit: [http://minorprotection.uconn.edu/reporting/](http://minorprotection.uconn.edu/reporting/).

**Where can I learn more?**

Further information about the Minor Protection Program is available at [http://minorprotection.uconn.edu](http://minorprotection.uconn.edu). Any and all questions regarding the program or reporting obligations may be directed to:

Omar Andujar, CCEP
Minor Protection Coordinator
Office of Audit, Compliance & Ethics
(860) 486-5682
Omar.andujar@uconn.edu

Is there a policy? If so where can I find it?

The President’s Cabinet approved an institution-wide Policy on the Protection of Minors and Reporting of Child Abuse and Neglect on March 23rd, with an effective date of April 1st. The full policy is available at: [http://minorprotection.uconn.edu/policy/](http://minorprotection.uconn.edu/policy/).
Did You Know?

- We feature policy updates in the Daily Digest?
- We have a Listserv highlighting important Compliance and Ethics news and information?
- The Joint Audit and Compliance Committee (JACC) Meeting Minutes are viewable here?

Policy Updates

At times, UConn engages in activities, research, and the development of new technologies that are subject to export control laws and restrictions. Research Compliance Services of the Office of the Vice President for Research has established an Export Control Policy and related procedures to support compliance with federal regulations. Individuals acting on behalf of the University, including faculty, staff and students, are responsible for adhering to the requirements set forth in this policy and related procedures. To learn more, visit http://policy.uconn.edu/?p=6564.

Earlier this year the President’s Cabinet approved a Contractor Parking Policy to ensure parking resources are appropriately allocated. This policy applies to all general and trade contractors, construction managers, trucking and delivery drivers and workers while conducting University-contracted business at the Storrs and Depot Campuses. The full policy is available at http://policy.uconn.edu/?p=6706.

The Board of Trustees approved revisions to the Policy on the Selection of Outside Legal Counsel. This policy defines the approved method for the selection of Outside Counsel pursuant to statute and in other circumstances where the University may select outside Counsel on its own behalf. The full policy is available at http://policy.uconn.edu/?p=2508.

Records and Information Management

One of the key topics being presented during this year’s Annual Compliance Training is Records and Information Management (RIM). At UConn we have records of all types: financial; research; administrative; student; personnel and more - the thought of addressing the vast range of records and data can be overwhelming. Let our office help you to make RIM a little bit easier.

RIM education and support can benefit you in a couple of big ways. The training, tools and resources provided can 1) help you to create space in your work environment and 2) help you to ensure you are doing everything you can to safeguard sensitive records.

Please contact Laurie Neal, Compliance and Records Management Specialist at (860) 486-4805 to request assistance.

For more information, visit: http://rim.uconn.edu/.

Compliance Training

Compliance Training is still available! The deadline for completing the Annual Compliance Training is May 20, 2016.

Faculty and Staff may complete the training online or in person.

Help us achieve 100%

For more information, including how to register, visit: http://audit.uconn.edu/?p=339.
Healthcare fraud and abuse is a serious offense. Several laws describe what constitutes fraud, waste and abuse including the False Claims Act, the Anti-kickback Statute, and the Physician Self-Referral Law (Stark). You should not knowingly submit false or deceptive claims information to the government or any other payers, or ignore knowledge you may have that a claim is false. Claims for health care services should be accurate and supported by legible, properly authenticated medical record documentation. All medical records should be retained in accordance with records retention requirements. The Department of Health & Human Services, Office of Inspector General website offers a wealth of information regarding fraud and abuse prevention, detection and reporting. Members of the UConn Health Community are required to report all suspected fraud and abuse activities to your immediate supervisor; your immediate supervisor’s supervisor (if the concern relates to your immediate supervisor); an appropriate manager with the UConn Health operating structure; Associate/Assistant Dean or Dean of the appropriate school; or the Office of Audit, Compliance and Ethics at (860) 679-4180, email: compliance.officer@uchc.edu or Report Line 1-888-685-2637 (anonymous reporting 24 Hours/Day, 7 Days a Week).

In addition to internal reporting options, any employee as well as persons doing business with UConn Health or members of the general public may report fraud and abuse to the State Auditors of Public Accounts. State Auditors contact information: Phone: (860)566-6150; Toll Free: (800)797-1702, Website: http://www.state.ct.us/apa/

For questions related to this article, please contact Margaret DeMeo, Associate Compliance Officer, at 860-679-1226 or demeo@uchc.edu

Conflicts of interest may occur in a variety of research, clinical or business situations. When substantial or even potential conflicts arise, compliance with the State Code of Ethics is an important part of appropriately managing the situation. In such instances, an employee must submit a signed written statement describing the situation to his or her immediate supervisor. The matter must then be assigned to another individual who is not under the involved employee’s supervision and who is completely free of any associated conflicts of interest.

Remember to seek guidance before taking any action that may lead to a potential or actual conflict of interest and possibly implicate the Code of Ethics.

Additional information and a conflict of interest disclosure form are located on the Office of State Ethics website at: http://www.ct.gov/ethics/lib/ethics/forms/eth-coi_11-25-08.pdf.

For questions, please contact Ginny Pack, UConn Health Ethics Liaison at 860-679-1280 or pack@uchc.edu or the Office of State Ethics at 860-263-2400 or ethics.code@ct.gov.
Memo to Managers - Anonymous Reports Are a Good Thing

UConn Health offers a number of avenues for employees to raise questions or concerns but you, as a manager, are always our first line of defense for your team members. An alternate resource is our company’s REPORTLINE which employees can use to report either anonymously or offer their name and contact information. We support and protect anonymous reporting and, as managers, it is important for all of us to align on this point and to respect this option. Anonymous reports allow our employees to make reports that they simply may not be comfortable making in person.

We also recognize that having an anonymous report lead to an investigation in our own organization can be uncomfortable. Here are some factors and guidance for you to consider should you find yourself in this situation:

- Do not feel as though employees are going above you to report anonymously. Research has shown that historically 6 out of 10 reports coming in through the hotline and web reporting channels are made anonymously so this is not unique to you or your department.
- Supporting (and not demeaning) anonymous reports or reporters shows that you want the reporting experience to remain a safe and confidential way to make a report.
- When an anonymous report comes in through our REPORTLINE, it is imperative that you do not seek out the identity of the reporter. Maintaining the integrity of anonymous reports will allow UConn Health to continue to receive actionable reports from all across locations/departments.

One critical aspect of these reports – that will assist in the substantiation of anonymous reports – is advising all reporters follow-up with their report. The Office of Audit, Compliance and Ethics (OACE) has made it part of our intake process to highlight the importance of following-up, but needs your support in reminding and encouraging employees who may report anonymously to stay engaged in the process and see it through. You can do this in a group or staff meeting as part of a discussion of the overall REPORTLINE process. If you need additional information about our processes, contact OACE at x4180 and we will be happy to assist.

We encourage all managers to embrace their role in developing the culture surrounding the use of the REPORTLINE and all of our reporting options. See UConn Health’s Reporting Compliance Concerns Policy. Consistent and positive encouragement can increase the effectiveness of these processes, and continue to make our workplace one where we are all invested in our culture.

1 Taken from NAVEX Global’s Compliance Communicator - March 2015
OIG Hospital Compliance Reviews

In 2011, the Office of Inspector General (OIG) initiated hospital compliance reviews to assess whether acute hospitals comply with Medicare billing regulations. The OIG utilizes data mining and trend evaluations of paid Medicare claims to select hospitals that may be at risk for noncompliance. The reviews are conducted on-site and include claims for both inpatient and outpatient services. Overpayments associated with review findings of non-compliance must be refunded.

As of February 2016, the OIG conducted compliance reviews at 147 hospitals and identified $76,447,380.00 in overpayments. In 2015, the OIG hospital compliance reviews focused on the following risk areas:

- inpatient claims billed; with high-severity-level DRG codes
- inpatient claims billed with kyphoplasty services
- inpatient claims with payments greater than $150,000
- inpatient and outpatient manufacturer credits for replaced medical devices
- outpatient dental claims
- outpatient claims billed with modifier –59
- outpatient claims billed for Doxorubicin Hydrochloride
- outpatient claims billed for Herceptin
- outpatient claims with payments greater than $25,000

The table below provides a summary of the six most recent compliance reviews:

<table>
<thead>
<tr>
<th>Facility</th>
<th>Total Claims Reviewed</th>
<th>Correct Claims</th>
<th>Inpatient Claims with Errors</th>
<th>Outpatient Claims with Errors</th>
<th>Total Overpayment</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Minnesota</td>
<td>255</td>
<td>125</td>
<td>29</td>
<td>101</td>
<td>565,286</td>
</tr>
<tr>
<td>Nebraska Methodist</td>
<td>138</td>
<td>119</td>
<td>17</td>
<td>2</td>
<td>111,116</td>
</tr>
<tr>
<td>UC, Davis</td>
<td>231</td>
<td>130</td>
<td>92</td>
<td>9</td>
<td>2,430,502</td>
</tr>
<tr>
<td>Sierra View</td>
<td>30</td>
<td>5</td>
<td>23</td>
<td>2</td>
<td>798,064</td>
</tr>
<tr>
<td>Naples Community</td>
<td>225</td>
<td>134</td>
<td>63</td>
<td>28</td>
<td>4,584,571</td>
</tr>
<tr>
<td>Boca Raton</td>
<td>211</td>
<td>161</td>
<td>50</td>
<td>0</td>
<td>2,628,112</td>
</tr>
</tbody>
</table>

For any questions about this article, contact Kim Bailot, Associate Finance Compliance Officer, x4746 or email at KBailot@uchc.edu
It’s one of the parts of your job you like the least: you receive a complaint about a team member, and an internal investigation is underway.

As a manager, your participation in workplace investigations is critical in creating optimal outcomes. You also have the very important role of maintaining confidentiality and coaching all of the team members who may be involved to do “the right things right,” both during and after the investigation.

Here are some do’s and don’ts to keep in mind:

- **Do**: Be open and honest with investigators. Now is not the time to shade the facts to steer the outcome of the investigation. We need to know what actually happened, good or bad.
- **Don’t**: Discuss details of the investigation with other members of your team. If other team members become aware of an investigation, a good talking point to use is, “For a variety of important reasons, details of the investigation are confidential, and that means I can’t discuss this issue with you. I hope you understand.”
- **Do**: Ask questions about the role (if any) you are expected to play in the investigation – the compliance, HR, and legal teams want to be a resource to you.
- **Don’t**: Take any steps to investigate the issue yourself unless the steps have been approved. Often, actions that seem like they would be helpful (questioning a member of the team or going through emails or files) can compromise an investigation.
- **Do**: Be objective. Stay neutral during an investigation: the outcome may surprise you.
- **Don’t**: Retaliate. It can be difficult to keep personal feelings out of an investigation. But no matter your perspective, no retaliation is acceptable—whether against the subject of the investigation, the person who brought forward the complaint, or a witness who participates in the investigation.
- **Do**: Think about what, if anything, you can do as a manager to change your team culture or processes to address the root cause of a complaint.

Workplace investigations can be difficult for everyone involved. But ultimately, going through the process of an investigation is essential in helping correct issues that can undermine a healthy corporate culture.

For any questions about this article, contact Iris Mauriello at x3501 or email at Mauriello@uchc.edu

*Taken from NAVEX Global’s COMPLIANCE COMMUNICATOR™ January 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). Topics for this month include the following:

- Legislation and Regulation
- Third Party Risk
- Workplace Safety

Legislation and Regulation

Obama Administration Modifies HIPAA to Strengthen the Firearm Background Check System

HHS Office for Civil Rights in Action – January 5, 2016

On January 4, 2016, the Department of Health and Human Services (HHS) moved forward on the Administration’s
commitment to modify the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to expressly
permit certain covered entities to disclose to the National Instant Criminal Background Check System (NICS) the
identities of those individuals who, for mental health reasons, already are prohibited by Federal law from having a
firearm.

This modification better enables the reporting of the identities of prohibited individuals to the background check
system and is an important step toward improving the public’s safety while continuing to strongly protect individuals’
privacy interests.

The final rule gives States improved flexibility to ensure accurate but limited information is reported to the NICS. This
rulemaking makes clear that, under the Privacy Rule, certain covered entities are permitted to disclose limited
information to the NICS. The information that can be disclosed is the limited identifying information about
individuals who have been involuntarily committed to a mental institution or otherwise have been determined by a
lawful authority to be a danger to themselves or others or to lack the mental capacity to manage their own affairs –
that is, only about those who are covered under the pre-existing mental health prohibitor.

The new modification is carefully and narrowly tailored to preserve the patient-provider relationship and ensure that
individuals are not discouraged from seeking voluntary treatment. This rule applies only to a small subset of HIPAA
covered entities that either make the mental health determinations that disqualify individuals from having a firearm or
are designated by their States to report this information to NICS. The rule does not apply to most treating providers.

It is important to note that the vast majority of Americans with mental health conditions are not violent and that those
with mental illness are in fact more likely to be victims than perpetrators. An individual who seeks help for mental
health problems or receives mental health treatment is not automatically legally prohibited from having a firearm; nothing in this final rule changes that. HHS continues to support efforts by the Administration to dispel negative
attitudes and misconceptions relating to mental illness and to encourage individuals to seek voluntary mental health
treatment. And the Department remains committed to robust enforcement of the civil rights laws that bar
discrimination based on disability by entities that receive funding from the Department.

The Final Rule is available for review at: http://www.federalregister.gov.

Third Party Risk

Manage 3rd Party Risk Exposure in an Interconnected World

grc2020 – January 6, 2016

The world is flat, risk is pervasive, and organizations have no boundaries. We operate in a global and interconnected
world. Organizations are no longer defined by brick and mortar walls nor by employees. The term insider used to be
a synonym for employee. Today, more than half of insiders in many organizations are not employees. Organizations
are a complex web of vendors, suppliers, contractors, consultants, temporary workers, service providers, outsourcers,
brokers, dealers, intermediaries and agents.
In this interconnected world; governance, risk management, and compliance (GRC) are no longer defined by traditional organization boundaries that no longer exist. The organization must holistically look at the web of relationships that form the organization and nest in deep supply chains and subcontractor relationships. Third party risk is the organizations risk. Their issues are your issues. Their compliance and ethics problems are your problems.

Consider the wit of Douglas Adams in this context . . .

_The connections between causes and effects are often much more subtle and complex than we with our rough and ready understanding of the physical world might naturally suppose . . . Let me give you an example. If you go to an acupuncturist with a toothache, he sticks a needle instead into your thigh. Do you know why he does that . . .?_

— Douglas Adams, Dirk Gently’s Holistic Detective Agency

The exposure organizations face from third party relationships is significant. These include:

- Bribery, Corruption & Fraud
- Business Continuity
- Contractual
- Financial
- Environmental
- Ethical
- Geo-Political
- Health & Safety
- Human Rights, Trafficking & Slavery
- Import/Export & Customs
- Labor Standards
- Legal
- Privacy
- Operational
- Regulatory Compliance
- Reputational
- Sanctions
- Security
- Strategic
- Sourcing

Third party regulation and legislation has been particularly active over the past few years. Consider a fraction of what is happening:

- **Bribery & Corruption.** We have seen expanded and increased enforcement of the US FCPA, with a focus on effective compliance. The UK Bribery Act has been in place for a few years with enforcement happening. There also is expanding regulation globally on bribery and corruption.

- **Conflict Minerals.** As part of the Dodd Frank Act, thousands of companies have gone through two years of compliance with conflict mineral requirements and reporting. US publicly traded companies have to trace tin, tantalum, tungsten, and gold to see if they come from the Democratic Republic of the Congo or nine surrounding countries known for crimes against humanity and report on this.

- **FTC Power to Sue in Data Breach.** This past August the U.S. Court of Appeals for the Third Circuit affirmed in FTC v Wyndham the FTC powers to sue organizations in the event of a data breach. Given over half of insiders in many organizations are third parties and the variety of breaches that involved a third party, this is going to cause increased scrutiny and attention in third party risk management.

- **OCC Regulations of Third Party Risk Management.** The OCC has significantly expanded vendor risk management requirements in financial services over the past several years, making this a board level issue. Besides a legion of banks asking me questions, I am getting regular inquiries for third party relationships of banks that are responding to the greater scrutiny of the banks they do business with.

- **PCI DSS.** In version 3 of PCI DSS we have seen expanded requirements on IT vendor risk assessments in context of contractual requirements if you accept major credit cards. I fully expect this to expand further in the next version after the Target incident that exposed millions of credit cards and the doorway into the breach was a heating and air-conditioning vendor that had a connection to the Target network. A hacker breached this vendor, got into Target IT systems and compromised point of sale systems across Target.

- **U.K. Modern Slavery Act.** This really surprises me as I am not seeing organizations reacting to it. This past October the Modern Slavery Act went into effect and impacts a wide range of organizations. Basically, if you supply goods or services, have any connection into the United Kingdom, such as a single employee, and do £36 million or more in revenue regardless of size of your UK operations, you need to prepare an annual Slavery and Human Trafficking statement detailing the steps it is taking to prevent slavery and human trafficking throughout its business and third party relationships (down into the depth of supply chains). The guidance given on this statement requests organizations detail:
• Organization structure, operations, and map of supply chains
• Policies and procedures related to slavery and human trafficking
• Due diligence processes to prevent slavery and human trafficking
• Risk assessment of the organization and suppliers where there is risk of slavery and human trafficking
• Key performance indicators that the organization uses to benchmark effectiveness in preventing slavery and human trafficking
• Training conducted with employees and third parties/suppliers in context of anti-slavery and human trafficking

These risks are complex and interconnected themselves. Third party risk cannot be managed in isolated and disconnected silos. It requires an integrated process of third party governance, risk management, and compliance throughout the lifecycle of third party relationships. However, many organizations manage third party risk in ad hoc siloed manners with different departments doing things in different ways, disconnected and redundant. These processes are usually inefficient and costly as they require significant amount of time compounded as the number of third party relationships grows in organizations.

An integrated and effective third party management process enables the organization to consistently manage the lifecycle of third party relationships across:

1. **On-boarding.** Automate the process of standardizing the identification of third parties to work with and moving them through registration and on-boarding while collecting required third party information and conducting appropriate due-diligence in context of the nature of the relationship. This includes third party:
   - Identification
   - Qualification
   - Contracting
   - On-boarding

2. **Ongoing communication processes.** The organization manages the ongoing periodic tasks of communications, attestations and interactions with third parties. This includes cyclical and event driven interactions with each third party on:
   - Policies
   - Training
   - Attestation
   - Self-assessments/questionnaires
   - Reporting

3. **Monitoring processes.** Enable the management and automation of the array of processes to continuously monitor third party relationships over their lifecycle in the organization. This includes third party:
   - Performance monitoring
   - Risk monitoring
   - Compliance monitoring
   - Ongoing due diligence monitoring
   - Issue reporting & resolution
   - Audit & inspections

4. **Forms & approvals.** Manage the development and automation of internal processes to collect and report information and route things for approval in context of third party relationships. This includes:
   - New vendor/supplier request
   - Gifts, hospitality & entertainment
   - Political & charitable contributions
   - Facilitated payments

5. **Metrics & reporting.** Through a solid information architecture and reporting engine, the organization brings together the data elements of the entire lifecycle to provide end-to-end reporting and metrics on third party relationships at the relationship level, risk area, or in aggregate.

6. **Renewal or Off-boarding.** Utilizing the detailed history of interactions, issues, performance, non-conformance, and evolving risk scenarios, the organization manages the processes to evaluate, maintain, and renew third party relationships. All good things must come to an end, the third party management lifecycle is concluded by managing the tasks and details many organizations neglect, or forget, in off-boarding relationships that are no longer needed.

To accomplish an integrated third party management process requires that the organization formulate an overall third party management strategy and process that spans roles and functions involved. This is supported by an integrated and consistent third party information and technology architecture to provide a holistic system of record and accountability across internal functions and third parties.
However, the market has a maze of solutions to offer organizations. GRC 20/20 current tracks and monitors over 130 third party management technology solutions and over 50 third party information/content offerings. Some of these solutions are broad and meant to support a holistic integrated third party management program while others are very function and issue specific. Navigating the maze of offerings and selecting the right elements to build a third party information and technology architecture is not a trivial task. GRC 20/20 is here to help organizations understand the range of solutions available and select the right solution(s) for each organization specific third party management strategy and process, whether this is an integrated third party management strategy as proposed, or for a specific function or issue.

**Workplace Safety**

**Under New DOJ Policy, An Unsafe Workplace Could Be a Crime**

*Corporate Counsel* – January 6, 2016

Workplace safety is emerging as a key issue in 2016 and corporate executives could find themselves criminally responsible for failing to protect their employees. The U.S. Departments of Labor and Justice announced on Dec. 17 a new joint initiative to crack down on environmental and workplace safety crimes. Under the new plan, known as the worker endangerment initiative, prosecutors will seek to prosecute workplace safety violations under federal environmental laws, in addition to long-standing workplace safety statutes such as the Occupational Safety and Health Act (OSHA).

In a recent blog post, lawyers at Holland & Hart explained the reasons for this shift in enforcement strategies. Here’s what they say you need to know:

- **Bigger penalties:** The marriage of environmental and safety prosecutions is really about imposing stiffer criminal penalties. That’s because OSHA and other workplace safety statutes generally provide for misdemeanor penalties, while federal environmental laws call for criminal penalties. “By looking for environmental offenses to add to workplace safety violations, prosecutors will be able to seek felony convictions and enhanced penalties,” the Holland & Hart lawyers explain.

- **The government’s rationale:** The DOJ and DOL say environmental violations and violations of workplace safety laws go hand in hand. As the agencies see it, employers who cut corners on worker safety laws are also likely to violate environmental regulations. “In essence, this initiative provides the government with a mechanism to turn a workplace safety investigation into an examination of a company’s environmental compliance,” the lawyers argue.

- **Individual accountability:** Holland & Hart lawyers note that there has been an increased focus on individual accountability by the DOJ, as the agency outlined in a September memorandum known as the Yates memo. They predict that the new workplace safety initiative is one area where we’ll see more individual executives in the crosshairs.
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:

- Compliance Programs
- HIPAA Compliance
- Medical Devices
- Pharmacy Standards
- Stark

Compliance Programs

Report Shows ‘Explosion’ in Health Care Whistleblower Suits

Corporate Counsel – January 5, 2016

There’s been a steady increase in False Claims Act litigation in recent years, particularly in the health care industry. Recently released data confirms that whistleblower cases, as opposed to government investigations, have been the driving force behind this explosion.

According to a report by Kevin McGinty of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, which is based on data the U.S. Department of Justice made available on Dec. 3, “health care-related cases—specifically, privately-instituted health care-related qui tam cases—have overwhelmingly been the largest factor in the growth in FCA cases and recoveries over the past twenty years.” And, for most of the last decade, about 80 percent of all health care-related FCA recoveries have resulted from whistleblowers, or qui tam, lawsuits.

The FCA is the government’s primary civil remedy to redress false claims related to government funding and contracts, as well as fraud within government programs such as Medicare, veteran benefits or federally insured loans and mortgages. Under the FCA’s qui tam provisions, whistleblowers can receive a bounty of up to 30 percent of the total recovery.

Private litigation activity related to the FCA now dramatically offsets government referrals and investigations, which have gradually dropped off in the past two decades, McGinty found. Zeroing in on recent health care claims, McGinty points out that the DOJ went from seeing no health care-related FCA claims back in 1987 to more than 400 claims in each of the past five years.

The number of cases filed related to the Department of Defense. Back in the late 1980s, DOD cases were the predominant category among FCA claims, “a trend consistent with burgeoning levels of defense spending at the end of the Cold War,” the report states.

The data “validates what we and other people believe they’d been seeing,” McGinty says.

HIPAA Compliance

Obama Administration Modifies HIPAA to Strengthen the Firearm Background Check System

HHS Office for Civil Rights in Action – January 5, 2016

On January 4, 2016, the Department of Health and Human Services (HHS) moved forward on the Administration’s commitment to modify the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to expressly permit certain covered entities to disclose to the National Instant Criminal Background Check System (NICS) the identities of those individuals who, for mental health reasons, already are prohibited by Federal law from having a firearm.
This modification better enables the reporting of the identities of prohibited individuals to the background check system and is an important step toward improving the public’s safety while continuing to strongly protect individuals’ privacy interests.

The final rule gives States improved flexibility to ensure accurate but limited information is reported to the NICS. This rulemaking makes clear that, under the Privacy Rule, certain covered entities are permitted to disclose limited information to the NICS. The information that can be disclosed is the limited identifying information about individuals who have been involuntarily committed to a mental institution or otherwise have been determined by a lawful authority to be a danger to themselves or others or to lack the mental capacity to manage their own affairs – that is, only about those who are covered under the pre-existing mental health prohibitor.

The new modification is carefully and narrowly tailored to preserve the patient-provider relationship and ensure that individuals are not discouraged from seeking voluntary treatment. This rule applies only to a small subset of HIPAA covered entities that either make the mental health determinations that disqualify individuals from having a firearm or are designated by their States to report this information to NICS. The rule does not apply to most treating providers.

It is important to note that the vast majority of Americans with mental health conditions are not violent and that those with mental illness are in fact more likely to be victims than perpetrators. An individual who seeks help for mental health problems or receives mental health treatment is not automatically legally prohibited from having a firearm; nothing in this final rule changes that. HHS continues to support efforts by the Administration to dispel negative attitudes and misconceptions relating to mental illness and to encourage individuals to seek voluntary mental health treatment. And the Department remains committed to robust enforcement of the civil rights laws that bar discrimination based on disability by entities that receive funding from the Department.

The Final Rule is available for review at: http://www.federalregister.gov.

If You Provide Behavioral Health Services, Do the New HIPAA Reporting Rules Apply to You?


In early January, the Office for Civil Rights of the United States Department of Health and Human Services (“OCR”) issued new regulations regarding the right of certain HIPAA covered entities to disclose mental health information to the National Instant Criminal Background Check System (“NICS”). Since these final regulations have been published, we have received many questions from our clients regarding the final rule and its application to them. We drafted this alert to explain the new regulations and, most importantly, their very limited scope.

Background

NICS is a national system maintained by the FBI to conduct background checks on persons who may be disqualified from receiving firearms based on prohibited categories under state or federal law. The prohibited categories include individuals who have been involuntarily committed to a mental institution, found incompetent to stand trial or not guilty by reason of insanity, or otherwise have been determined by a court of law to be a danger to themselves or others or to lack mental capacity.

In recent years, concerns were raised that certain health care-related entities with NICS-related information were unable to disclose the information because they were located in states that do not require such disclosure by law. OCR’s rulemaking attempts to address this concern and permit these entities to disclose relevant information to the NICS.

What the New Regulations Mean For You

In order to disclose PHI to the NICS pursuant to the new regulations, a covered entity must fit into one of the following two categories:

- The covered entity functions as a data repository of information (e.g. registrar) relevant to the NICS on behalf of a state (note that OCR expects states to identify which covered entities in the state, if any, serve such a function); or

- The covered entity is a board, commission, or other lawful authority that makes involuntary commitments or other adjudications that make an individual subject to the NICS.
Such covered entities may disclose PHI directly to the NICS or to an entity designated by a state as a repository of data for purposes of reporting to the NICS. The PHI that may be disclosed is limited to what is necessary for NICS reporting purposes.

Medical Devices

Cybersecurity in Postmarket Medical Devices: New Guidance From the FDA

_Wiggin and Dana_ – January 29, 2015

On January 22, 2016, the U.S. Food and Drug Administration ("FDA") issued draft guidance for the medical device industry. The guidance outlines the steps medical device manufacturers should take to monitor, identify, and address the postmarket cybersecurity risks inherent in medical devices containing software or programmable logic, and in software that is a medical device. The FDA is seeking public input, and the comment period will remain open for 90 days.

Calling cybersecurity threats to medical devices "a growing concern," the FDA urges device manufacturers to improve cybersecurity risk management throughout the product lifecycle in a manner commensurate with the evolving cyber threat. The guidance focuses in particular on the steps medical device companies should take to assess and mitigate cybersecurity vulnerabilities after their products go to market.

Although the guidance is nonbinding, the FDA's recommendations in effect create new postmarket cybersecurity standards for reasonable behavior. Here are some of the key takeaways:

**Cybersecurity Risk Management Programs Are Essential.** The guidance states that it is "essential" for device manufacturers to implement cybersecurity risk management programs and documentation that address postmarket complaint handling, quality audit, corrective and preventative action, software validation and risk analysis, and servicing, consistent with the Quality System Regulation (21 CFR part 820). The guidance also identifies the following "critical components" of an effective cybersecurity risk management program:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing, and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining "essential clinical performance" so that potential compromise of essential clinical performance can be identified and mitigation strategies developed that protect, respond, and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigation strategies that address cybersecurity risk early and prior to exploitation.

**Follow the NIST Cybersecurity Framework.** The guidance further explains that a cybersecurity risk management program for a medical device should cover both its premarket and postmarket phases. To accomplish cybersecurity across a product's lifecycle, the FDA strongly encourages manufacturers to develop their cybersecurity risk management programs using the Cybersecurity Framework developed by the National Institute of Standards and Technology ("NIST"). The NIST Cybersecurity Framework is a voluntary, risk-based tool that outlines five core functions (Identify, Protect, Detect, Respond, and Recover) related to cybersecurity risk.

The guidance includes an appendix that walks through the Framework's core elements in the context of a medical device manufacturer's cybersecurity risk management program. According to the guidance, medical device companies should use the Framework to develop programs that include methods for (1) identifying, characterizing, and assessing cybersecurity vulnerabilities; (2) analyzing, detecting, and assessing threat sources; and (3) adopting device-based features and compensatory controls to address unacceptable risk.

**Join an ISAO, Avoid Reporting (Usually).** The guidance strongly encourages medical device manufacturers to join an Information Sharing Analysis Organization ("ISAO"). ISAOs enable cybersecurity information sharing within the private sector and between the private sector and the government. ISAOs are designed to encourage the sharing of actionable information—that is, identification of cyber risk in real time. Information shared through an ISAO is protected from release under the Freedom of Information Act or state sunshine laws and may be exempt from both regulatory use and civil litigation.
The guidance states that the FDA considers ISAO participation "a critical component" of a device manufacturer's approach to postmarket cybersecurity. As an incentive, the FDA "does not intend to enforce certain reporting requirements of the Federal Food, Drug, and Cosmetic Act" if companies participate in an ISAO voluntarily and follow the recommendations in the guidance. Specifically, if a medical device manufacturer identifies and quickly addresses a vulnerability that "sufficiently reduces the harm to patients," then the FDA will not enforce urgent reporting to the Agency, if the following conditions are met:

- There are no known serious adverse events or deaths associated with the vulnerability;
- Within 30 days of learning of the vulnerability, the manufacturer notifies users and reduces the risk to acceptable levels; and
- The manufacturer is a participating member of an ISAO and reports the vulnerability, its assessment, and remediation to the ISAO.

The guidance notes that in the "majority of cases" when a manufacturer addresses a cybersecurity vulnerability, its actions will be considered "cybersecurity routine updates or patches" that will not require advance notification or reporting under 21 CFR 806. Device manufacturers will need to notify the FDA if there is a serious adverse event or death associated with a cybersecurity vulnerability or upon identification of an unremediated vulnerability that could compromise a device's essential clinical performance.

HIPAA Settlement Reinforces Lessons for Users of Medical Devices

HHS.gov – November 25, 2015

Lahey Hospital and Medical Center (Lahey) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules with the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR). Lahey will pay $850,000 and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Lahey is a nonprofit teaching hospital affiliated with Tufts Medical School, providing primary and specialty care in Burlington, Massachusetts.

Lahey notified OCR that a laptop was stolen from an unlocked treatment room during the overnight hours on August 11, 2011. The laptop was on a stand that accompanied a portable CT scanner; the laptop operated the scanner and produced images for viewing through Lahey’s Radiology Information System and Picture Archiving and Communication System. The laptop hard drive contained the protected health information (PHI) of 599 individuals. Evidence obtained through OCR’s subsequent investigation indicated widespread non-compliance with the HIPAA rules, including:

- Failure to conduct a thorough risk analysis of all of its ePHI;
- Failure to physically safeguard a workstation that accessed ePHI;
- Failure to implement and maintain policies and procedures regarding the safeguarding of ePHI maintained on workstations utilized in connection with diagnostic/laboratory equipment;
- Lack of a unique user name for identifying and tracking user identity with respect to the workstation at issue in this incident;
- Failure to implement procedures that recorded and examined activity in the workstation at issue in this incident; and
- Impermissible disclosure of 599 individuals’ PHI.

“It is essential that covered entities apply appropriate protections to workstations associated with medical devices such as diagnostic or laboratory equipment,” said OCR Director Jocelyn Samuels. “Because these workstations often contain ePHI and are highly portable, such ePHI must be considered during an entity’s risk analysis, and entities must ensure that necessary safeguards that conform to HIPAA’s standards are in place.”

In addition to the $850,000 settlement, Lahey must address its history of noncompliance with the HIPAA Rules by providing OCR with a comprehensive, enterprise-wide risk analysis and corresponding risk management plan, as well as reporting certain events and providing evidence of compliance.
CMS and the Revised Pharmacy Standards: What Every Hospital Should Know

*AHCH Media* – January 11, 2016

CMS has issued a 45-page advance survey memo, which revises the hospital pharmacy conditions of participation (CoPs) in 2016. The changes were made to bring the pharmacy interpretive guidelines into alignment with accepted standards of practice, such as the U.S. Pharmacopeia/National Formulary (USP/NF). CMS also recommends hospitals follow prescribed best practices, such as those from the American Society of Health System Pharmacists (ASHP) and the Institute for Safe Medication Practices (ISMP).

This CMS memo also amends Appendix A, which is the manual for larger hospitals, as well as provide for changes to 10 tag numbers or sections: 489, 490, 491, 492, 500, 501, 502, 505, 507, and 510.

These new interpretive guidelines address compounding medication, especially compounded sterile preparations (CSP).

Additionally, the CMS memo includes determining beyond-use dates (BUDs), changes regarding safe and appropriate storage and use of medications, and addresses tag number 405, which is located in the nursing section.


California Hospital to Pay More Than $3.2 Million to Settle Allegations That It Violated the Physician Self-Referral Law

*The United State Department of Justice* – January 15, 2016

Tri-City Medical Center, a hospital located in Oceanside, California, has agreed to pay $3,278,464 to resolve allegations that it violated the Stark Law and the False Claims Act by maintaining financial arrangements with community-based physicians and physician groups that violated the Medicare program’s prohibition on financial relationships between hospitals and referring physicians, the Justice Department announced today.

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 an enumerated exception. 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.

“The settlement of this matter reflects not only our commitment to protect the integrity of the healthcare system through enforcement of the Stark Law, but also our willingness to work with providers who disclose their own misconduct,” said Principal Deputy Assistant Attorney General Benjamin C. Mizer, head of the Justice Department’s Civil Division.

The settlement announced today resolves allegations that Tri-City Medical Center maintained 97 financial arrangements with physicians and physician groups that did not comply with the Stark Law. The hospital identified five arrangements with its former chief of staff from 2008 until 2011 that, in the aggregate, appeared not to be commercially reasonable or for fair market value. The hospital also identified 92 financial arrangements with community-based physicians and practice groups that did not satisfy an exception to the Stark Law from 2009 until 2010 because, among other things, the written agreements were expired, missing signatures or could not be located.

“Patient referrals should be based on a physician’s medical judgment and a patient’s medical needs, not on a physician’s financial interests or a hospital’s business goals,” said U. S. Attorney Laura E. Duffy of the Southern District of California. “This settlement reinforces that hospitals will face consequences when they enter into financial agreements that don’t meet relevant standards.”
arrangements with physicians that do not comply with the law. We will continue to hold health care providers accountable when they shirk their legal responsibilities to the detriment of tax payer-funded health care programs.”

“Together with our law enforcement partners, our agency’s investigators and attorneys will continue to work with health care providers who use the self-disclosure protocol to resolve their billing misconduct,” said Special Agent in Charge Chris Schrank of the U.S. Department of Health and Human Services Office of Inspector General (HHS-OIG), Los Angeles region.”

This 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 $27.1 billion through False Claims Act cases, with more than $17.1 billion of that amount recovered in cases involving fraud against federal health care programs.

This matter was handled by the U.S. Attorney’s Office of the Southern District of California, the Civil Division’s Commercial Litigation Branch and HHS-OIG. The claims settled by this agreement are allegations only, and there has been no determination of liability.

Memorial Health, Affiliates Settle Medicare Overbilling Litigation for $9.8 Million

savannahnow.com – December 23, 2015

Memorial Health Inc., the parent corporation of Memorial Health University Medical Center Inc., Provident Health Services Inc., and MPPG, Inc. d/b/a Memorial Health University Physicians agreed to pay $9,895,043 to resolve allegations that they violated the False Claims Act by submitting false and fraudulent claims for Medicare reimbursement based on prohibited referrals by physicians whose financial relationships violated federal law.

The settlement is the largest civil health care fraud recovery in the history of the U.S. Attorney’s Office for the Southern District of Georgia.

“This settlement demonstrates the U.S. Attorney’s Office’s continued commitment to ensure that health care providers do not violate the Stark Law and all medical decisions are based strictly on the best interests of patients, not the financial interests of providers,” U.S. Attorney Edward J. Tarver said.

The settlement resolves allegations that were originally part of a federal lawsuit filed under the whistle blower provisions of the False Claims Act, which allow private citizens with knowledge of false claims to file suit on behalf of the government and to share in the recovery. As part of this settlement, Memorial entered into a five-year corporate integrity agreement with the Office of Inspector General, Department of Health and Human Services.

“Let this settlement act as a reminder to health care providers, large and small, that the Office of Inspector General is committed to pursuing allegations of Stark Law violations,” said Derrick L. Jackson, Special Agent in Charge of the U.S. Department of Health and Human Services, Office of Inspector General in Atlanta. “Financial incentives for referrals should never come into play for health care providers when they are determining the best course of care for our nation’s citizens.”

In its comment Thursday, Memorial Health officials said, “In order to bring conclusion to a whistle blower lawsuit brought about by former CEO Phillip Schaengold relating to specific physician employment agreements from 2008 to 2010, Memorial Health has agreed to terms with the government to settle the case.

“Memorial has cooperated fully with the government and acted in good faith. Memorial expressly denies allegations in the lawsuit and believes that its processes have been, and continue to be, compliant with all legal and regulatory statutes. Memorial is committed to serving the community and providing the highest quality care for our patients.”

The government action stemmed from claims filed under seal in 2011 by Phillip Schaengold, former Memorial Health Inc. president and CEO beginning in June 2009. He was abruptly dismissed by Memorial’s board on Jan. 5, 2011.
The government’s civil case, filed in U.S. District Court in Savannah, cited violations of the False Claims Act and laws designed to curb overbilling for Medicare services by physicians who refer patients to facilities in which they have a financial interest.

It contended Memorial’s leadership, recognizing they were facing financial problems in 2007, pursued primary care referrals and sought to entice primary care physicians to address dwindling patient volume. It contained allegations that Memorial recruited Dr. Paul S. Bradley and his Eisenhower Medical Associates, an internal medicine group of three doctors, and paid them salaries and compensation packages in excess of market benchmarks.

Neither Bradley nor his medical group nor individual partners were named as defendants in the suit. Their relationship with Memorial ended in February 2011.

Memorial’s attorneys called allegations in the lawsuit “a simple story which is fundamentally untrue.”

They denied recruiting or enticing physicians with Eisenhower Medical Associates, but said they were approached by the group after they decided to leave the St. Joseph’s/Candler medical system.

Memorial also denied that their financial relationship with Eisenhower Medical Associates was inappropriate.
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:

- Information Security and Privacy
- Legislation
- Regulatory Requirements
- Title IX

Information Security and Privacy

Hollywood Presbyterian Concedes to Hacker’s Demands in Ransomware Attack


In a chain of events that should be a wake-up call to any entity using and storing critical health information, Hollywood Presbyterian Medical Center (“HPMC”) has announced that it paid hackers $17,000 to end a malware attack on the hospital’s computer systems. On February 5, HPMC fell victim to an attack that locked access to the medical center’s electronic medical record (“EMR”) system and blocked the electronic exchange of patient information. Earlier reports indicated that the hackers had originally demanded $3,400,000.

Such “ransomware” attacks are caused by computer viruses that wall off or encrypt data to prevent user access. Hackers hold the data ransom, demanding payment for the decryption key necessary to unlock the data. The attacks are often caused by email phishing scams. The scams may be random or target particular businesses or entities. In the case of HPMC, the medical center’s president and CEO indicated to media outlets that the attack was random, though Brian Barrett, writing for *Wired*, questioned that assertion.

The medical center’s announcement of the resolution of the incident indicates that there is no evidence that patient or employee information was accessed by the hackers as part of the attack. Even if the data was not compromised, the attack led to enormous hassles at the hospital, returning it to a pre-electronic record-keeping system.

On February 2, 2016, three days before the HPMC attack, the Department of Health & Human Services Office for Civil Rights (“OCR”) announced the launch of its new Cyber-Awareness Initiative. That announcement included information on ransomware attacks and prevention strategies. Suggested prevention strategies from OCR included:

1. Backing up data onto segmented networks or external devices and making sure backups are current.
2. Ensuring software patches and anti-virus are current and updated.
3. Installing pop-up blockers and ad-blocking software.
4. Implementing browser filters and smart email practices.

Most of these prevention strategies are HIPAA security measures that ought to be in place generally. As OCR indicates, smart email practices and training the workforce on them are key elements to preventing phishing scams. Before clicking on a link in an email or opening an attachment, consider contextual clues in the email. The following types of messages should be considered suspicious:

- A shipping confirmation that does not appear to be related to a package you have actually sent or expect to receive.
- A message about a sensitive topic (e.g., taxes, bank accounts, other websites with log-in information) that has multiple parties in the To: or cc: line.
- A bank with whom you do not do business asking you to reset your password.
- A message with an attachment but no text in the body.

All health care providers, payors, and their business associates need to take notice of the HPMC attack and take steps to ensure that they are not the next hostages in a ransomware scheme.
White House’s Cybersecurity National Action Plan (CNAP) Includes Cybersecurity Awareness Campaign, Creation of Federal Privacy Council

Cybersecurity – February 9, 2016

Following the announcement of the President’s Cybersecurity National Action Plan (CNAP), an initiative designed to “enhance cybersecurity capabilities within the Federal Government and across the country,” the White House has released a fact sheet outlining the different components of the CNAP. The announcement of the CNAP follows the President’s request for $19 billion in funding for cybersecurity initiatives in fiscal year 2017, an increase of 35% over the previous year’s request. The CNAP includes a mixture of near-term measures and long-term objectives, with the ultimate goal of enhancing the federal government’s cybersecurity posture while encouraging private citizens and businesses to do the same. Some of the most significant aspects of the CNAP, discussed further below, include:

- The launch of a cybersecurity awareness campaign to promote the use of multi-factor authentication;
- A “systematic” review by the White House to identify areas where the federal government can reduce the use of Social Security Numbers as individual identifiers;
- Plans for the development of a Cybersecurity Assurance Program to test and certify connected devices against certain security standards;
- The creation of a Chief Information Security Officer (CISO) position within the federal government, coupled with a $3.1 billion initiative to modernize federal agencies’ IT systems and applications;
- The establishment of a commission of private sector cybersecurity experts to offer recommendations on cybersecurity initiatives; and
- The establishment of a Federal Privacy Council, composed of representatives from various key federal agencies, to coordinate guidelines for the federal government’s collection and storage of data.

Legislation

Obama’s Budget


Two enforcement goals for the Education Department appear in Obama’s proposed federal budget.

A couple of lines in the budget’s appendix confirm the administration's plans for the Education Department to hold colleges accountable. Here's the first:

OFFICE OF CIVIL RIGHTS

For expenses necessary for the Office of Civil Rights, as authorized by section 203 of the Department of Education Organization Act, [$107,000,000] $137,708,000. (Department of Education Appropriations Act, 2016.)

Program and Financing (in millions of dollars)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0001 Civil rights ..........................</td>
<td>100</td>
<td>107</td>
<td>138</td>
</tr>
</tbody>
</table>

Last year, you might recall, President Obama asked for a $31-million increase in funding for the department's Office for Civil Rights, which enforces the Title IX rules that require colleges to investigate and resolve complaints of sexual misconduct. He ended up getting a boost of $7 million instead.

This year he is again seeking $31 million more — enough to create more than 150 new, full-time positions in the office.
Here's the second key line:

Employment Summary

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1001 Direct civilian full-time equivalent employment ...</td>
<td>1,375</td>
<td>1,537</td>
<td>1,621</td>
</tr>
</tbody>
</table>

This is a request for more than 80 new positions in the Office of Federal Student Aid. Education Department officials announced on Monday their intent to create a new "Student Aid Enforcement Unit" to root out abuses in student lending and related areas. The department plans to move some existing employees into that unit, but it's also looking to staff up.

**Regulatory Requirements**

**To Get Credit for Cooperating with a DOJ Investigation, Get Ready to Certify Your Disclosures**

_Dentons.com – February 9, 2016_

Late last week, the _Wall Street Journal_ reported that the US Department of Justice's (DOJ's) fraud section is developing a process for settling companies to certify that they have disclosed fully all information about individuals involved in wrongdoing before finalizing a settlement agreement. This means that the company not only must "name names" as established by the recent _Yates Memorandum_, but now a corporate officer will be required to certify and "confirm to [the DOJ] that they have, in fact, turned over all non-privileged information about individuals."

The impact of such a certification should have ripple effects back to the initiation of any internal investigation, informing how even initial interviews and discussions are conducted. And, like the Yates Memo, eventual certification must be dropped into the complex considerations of whether or not to self-disclose.

On September 9, 2015, Deputy Attorney General Sally Q. Yates sent a memorandum within the DOJ, adding to and clarifying the Department's _Principles of Federal Prosecution_ policy, which sets out the requirements for receiving cooperation credit in plea or settlement agreements. A key portion of that Memorandum adopted an unwritten, and inconsistently enforced, requirement that in order to get any cooperation credit, a corporation must investigate, determine and identify responsible individuals, and must provide a "complete" disclosure of "all" individuals involved in, or responsible for the misconduct, regardless of the person's position. The information that must be disclosed to the DOJ is "all facts" related to the misconduct, not just the relevant facts. The "cooperation credit" is **often a critical factor** in charging decisions and the mitigation of any fine or penalty handed down for wrongful conduct.

Now apparently, the DOJ will be stacking a certification process on top of the Yates Memo that will require cooperating corporations to enter a written statement of cooperation, where the corporation certifies it has in fact provided all of this information. Once adopted by the DOJ, a General Counsel, Chief Compliance Office, Board Member, Director or Audit Committee Member will have to put himself or herself on the hook regarding the company's disclosure.

One big resulting question is, what can the organization do to ensure the integrity of any disclosure made to the government? A related consideration is what can a corporate officer or director do to provide some protection for themselves when making the disclosure certification? The best course in response to both issues will be to change the way the company conducts pre-investigation planning, and to engage in some difficult discussion up-front, before an investigation is underway. Investigation team members within "the-need-to-know" group should understand from the outset (and be reminded during an investigation) that any evidence of individual misconduct found during a report of, or investigation into, wrongdoing must be disclosed in order to earn cooperation credit. Further, the investigative team must understand that someone will be required to certify that all information about alleged wrongdoers has been disclosed.

Knowing the disclosure of wrongdoing may be in the best interests of the organization may also raise questions whether certain individuals are adverse to the interests of the organization. While it may be unclear where interests line-up at the start of an investigation, planning for the issue and how you will address it at the outset may avoid problems down the road. This is particularly true when it is clear the government will use real or imagined conflicts to challenge the integrity of the investigation.
From the time a call on the hotline is reported, this certification and what the company must do for cooperation credit must be part of the decision-making process. Pre-investigation planning and an understanding of this obligation amongst the investigation team will lay a necessary foundation for that task down the road. It also must be considered in the company's ultimate decision to cooperate and disclose information to the government, as well as related indemnification and appointment of counsel considerations throughout an investigation.

The company's plan on handling this certification, and the accompanying issues it creates, should be closely linked to the company's internal investigations and indemnification policies. Those policies will establish a consistent approach for an investigations team and responsible officers to follow when addressing the expanding challenges they must face in the company's fight for cooperation credit.

In the end, DOJ's latest action demonstrates that pre-investigation planning is a critical step in ultimately deciding how you are going to mitigate your risk if your efforts detect conduct that creates legal risk.

Title IX

A Closer Look at 7 Common Requirements in Resolved Federal Sex-Assault Inquiries

The Chronicle of Higher Education – February 8, 2016

The Chronicle has posted the 20 or so publicly available resolution agreements in its Title IX investigation tracker.

Those agreements spell out policies and procedures that need to change or be added in order to bring colleges that were under investigation back on the right side of the law.

As of last month OCR had resolved 46 of the more than 240 investigations included in The Chronicle’s tracker. Thirty of those ended in resolution agreements.

When the Ncherm Group, which advises colleges on Title IX compliance and other issues, pored over many of the resolution agreements, it came up with a 37-point checklist of what OCR was looking for.

A Chronicle review of the resolution agreements issued since 2011 identified several key takeaways. Here are a few:

1. Every campus must have a Title IX coordinator.

"There are certain basic commandments, and the first is, ‘Thou shalt have a Title IX coordinator,’” says Peter F. Lake, chair and director of the Center for Excellence in Higher Education Law and Policy at Stetson University’s College of Law. "That comes screaming through in every document."

Detailed contact information and procedures for filing complaints should be clearly communicated to students and employees, not just in policy statements that few people read, but in pamphlets, student newspapers, and frequently visited websites.

Along with investigating and adjudicating individual cases of sexual misconduct, Title IX offices should study patterns of behavior among specific student groups, like athletes and freshmen, to determine whether any of them are particularly prone to bad behavior.

2. "Preponderance of the evidence" should be the standard.

Sexual-misconduct policies must all use a "preponderance of the evidence" yardstick for assessing responsibility. Under that standard, which is lower than those used in criminal cases, an accused student is found guilty if the college determines it’s more likely than not that an incident occurred.

Harvard Law School is among the institutions forced to change its standard of proof to meet the lower threshold after the civil-rights office found that its policies violated Title IX. Some Harvard Law professors have joined advocates of accused students in questioning whether that lower threshold is fair.

3. Colleges must offer extensive and continuing training to both students and employees.

At minimum, they should offer freshmen orientation sessions that discuss sexual misconduct, as well as the link between drinking and drugs and sexual violence.

Those sessions, which should be repeated annually for students living in residence halls, should spell out the differences between the Title IX process and the criminal process.

Students should know what to expect from the university and the police when they make a complaint, including the interim steps colleges will take to keep them safe, like changing class schedules or issuing no-contact orders.
Regular training is also required for Title IX coordinators, investigators, and other employees involved in grievance procedures.

4. **Colleges should use clear and consistent definitions to describe sexual misconduct.**
   Guides should include terms such as sexual harassment, sexual violence, and consent. Training should include specific examples of each type of misconduct, from racist jokes to rape. Sexual harassment, for instance, is described in at least one resolution agreement as "unwelcome conduct of a sexual nature" that can include "unwelcome sexual advances, requests for sexual favors, and other verbal, nonverbal, or physical conduct of a sexual nature, such as sexual assault or acts of sexual violence."

   Many of the resolution agreements have "boilerplate language" defining sexual harassment and what constitutes a hostile environment, Mr. Lake says. "They use the language repeatedly so it’s become currently understood that that language has to make it into your policy almost word for word."

5. **Investigations should be completed within a reasonable time — usually 60 days.**
   Unless a college faces "extraordinary circumstances," it should wrap up cases within 60 calendar days and shouldn’t use pending criminal action as an excuse for delay.

   Both parties should get regular updates on the progress of a case, as well as written notice of the outcome.

   OCR has had a tough time completing its own cases in a reasonable time as the pace of new cases accelerates, with most taking more than a year to resolve.

6. **"Responsible employees" must promptly report sexual harassment and violence they hear about.**
   They could include faculty members, coaches, and resident advisers — basically, anyone except for a clergy member or counselor who has a confidential relationship with a student.

   The University of Virginia’s resolution agreement states that "all employees designated as responsible employees will notify the Title IX coordinator or designee within 24 hours of receiving information about possible sexual harassment or sexual violence against students," whether or not the student expresses interest in filing a complaint. If they delay responding, that could constitute a hostile environment and thus a Title IX infraction.

7. **Campuses should conduct annual climate surveys.**
   Among other things, the surveys should measure students’ experiences with sexual misconduct, their knowledge about how to report it, and suggestions on how to prevent it.

   "Surveys give campuses a tool to measure whether or not, at a minimum, the social perceptions on campus are changing with improved policies," says S. Daniel Carter, board president of SurvJustice, an advocacy group for victims. "You can’t adequately take on the challenge until you know the full scope of the problem."
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:

- Exclusions Checking
- HIPAA
- Information Security and Privacy
- Legislation
- Regulatory Requirements
- Title IX

Exclusion Checking

Settlements Over Excluded Employees Pile Up; Screening Snags Bedevil Compliance

*Report on Medicare Compliance – January 5, 2016*

A wave of settlements with the HHS Office of Inspector General (OIG) over excluded employees is a cautionary tale for health care organizations, even as they face stumbling blocks in their exclusion screening. In the last four months of 2015, 21 health care organizations resolved civil monetary penalty (CMP) cases for employing people who had been thrown out of federal health care programs, with settlement amounts ranging from $24,128 to $21 million. OIG has intensified its enforcement of CMP and exclusion cases with its “litigation team”, and state Medicaid agencies are cracking down on exclusions. But there are still imperfections in the screening process that are exacerbated by the fact that sometimes employees are oblivious to their exclusions or try to pull the wool over their employers’ eyes, lawyers say.

Exclusion screening “is the painful cost of doing business, but it’s important that you do it and not take shortcuts,” said attorney Mary Malone, with Hancock, Daniel, Johnson & Nagle, at a Jan. 25 webinar sponsored by the HealthCare Compliance Association.

The implications of billing for services provided by excluded employees and contractors were set out by OIG in its 2013 bulletin on exclusions. According to OIG, no federal health care program payment will be made for goods or services provided by an excluded person or entity or at the medical direction or on the prescription of an excluded person, regardless of payment methodology (e.g., DRGs, cost reports, fee schedules, bundled payments, capitation). This includes direct care, such as physicians’ services, and indirect care, such as preparing surgical trays and reviewing treatment plans. Excluded persons also are forbidden to furnish “administrative and management services that are payable by the Federal health care programs,” the bulletin says. That means excluded people can’t serve in executive or leadership roles, such as CEO, CFO, general counsel, director of health information management or physician practice office manager.

Ensuring excluded people and vendors are kept at bay can be harder than it sounds, Malone said. Sometimes it’s because the employees didn’t know they were excluded. OIG is required by law to notify people and entities they have been excluded by sending letters to their last known address, but OIG is not obligated to confirm they were received, said attorney W. Clay Landa, with Hancock, Daniel, Johnson & Nagle, who also spoke at the webinar. What an excluded person doesn’t know can hurt future employers, he said.

For example, Malone represented a hospital that settled a CMP case over a certified coder who worked there for nearly a dozen years before her exclusion came to OIG’s attention. Neither the hospital nor the coder was aware of it. The exclusion was unrelated to the employee’s work as a coder, but resulted from a plea deal the coder entered into at the urging of her attorney when she was working in a clinical position in another facility years earlier. The coder was unaware the plea would affect her license or cause Medicare exclusion. The coder lived with her parents at the time, and they all said they never got an exclusion letter. After “reinventing herself” as a coder, she got married and took a job in the hospital’s billing office, Malone said. Years after the criminal case, the hospital was surprised to learn she...
was persona non grata with Medicare, although OIG wouldn’t reveal how it found out, Malone said. Even though the hospital has a screening program, it didn’t detect the coder’s exclusion. “She was screened every month for 11 years, and it never came up because” she was excluded under her maiden name and screened with her married name. To arrive at a CMP settlement amount, OIG had the hospital look at payer mix and determine how much time the coder spent working on federal health care payer claims. The hospital then paid the corresponding amount of her compensation multiplied by 11-plus years.

**Try Searching LEIE With Three Letters**

The hospital’s missing the exclusion because of a name change underscores the importance of looking more than skin deep at OIG’s exclusion database, the List of Excluded Individuals and Entities (LEIE). There are two ways for health care organizations to search the LEIE, Landa said. One option: Download the entire database every month, merge it with your employee and vendor list and see what pops out. “The downloadable files don’t have Social Security numbers or employee identification numbers, but they have dates of birth,” Malone said. “Any potential matches have to be verified.”

The second option: Health care organizations enter employee and vendor names on the OIG website, five at a time, to see if any match, although this approach “is not operationally possible” for larger organizations, according to Malone and Landa. They tend to hire screening vendors, Landa said. “It’s helpful but won’t protect providers from liability if the vendor makes mistakes and doesn’t identify an excluded employee working within the health system,” Malone noted.

Whichever route health care organizations take, they can’t assume they’re home free with searches based on one version of the name. Malone advised running variations of the name — maiden, married and hyphenated — through the LEIE. Keep in mind that employees who know they are excluded may try to evade detection. “Consider entering only a few letters of the [last] name to get an accurate result,” such as “Smi” instead of “Smith,” Landa said. When you have a possible match, use the Social Security number to nail it down.

The LEIE is not foolproof. One Virginia nursing home client got an OIG repayment demand because it had an employed nurse on the exclusion list. Although the nurse was, in fact, on the LEIE, she shouldn’t have been. While working in New York state, the nurse had a board of nursing hearing, but it went well, and her license was intact, Malone said. Loss of license is a driving force behind exclusions, but in this case the exclusion was a mistake, and Malone said it all ended well. The experience was a wake-up call for the nursing home to screen employees for exclusions, she noted.

Sometimes health care organizations are duped by employees who know they’re excluded. That was the case with a certified coder who was brought into a hospital billing department through a staffing company that was responsible for exclusion screening, Malone said. As it turns out, she was a paroled felon. The coder was good at her job, but she was perceived as a troublemaker, clashing with her supervisor, who felt the coder insinuated the supervisor had compliance problems. The charade ended when someone who knew the coder called the hospital and spilled the beans about the coder’s stint in prison for fraudulent billing in a previous job and her subsequent exclusion. She managed to conceal it from the hospital in terms of tax forms and the background check by changing one digit of her Social Security number, but it’s inexplicable why the billing company didn’t detect the exclusion, Malone said. “This woman was a professional criminal,” she noted. “She knew how to work the system and how to avoid detection.”

Hospitals have more than OIG to worry about when it comes to exclusions. Many states require providers to screen for Medicaid exclusions, and 39 states have their own lists to check for excluded employees/vendors, Landa said. “Providers may just be checking the LEIE, but states can have exclusions, and OIG is not required to exclude a person from Medicare based on a state exclusion,” Landa said. However, under the Affordable Care Act, it’s all for one and one for all in terms of Medicaid: When one state excludes, they all must exclude, if providers are “excluded for cause,” he said. What “cause” means is a little fuzzy, although CMS has indicated that “cause” includes adverse licensure actions, fraud, billing for services that were not furnished or medically necessary, misusing a billing number and falsifying information on applications or medical records, Landa said.
CMS told states in 2009 to require Medicaid providers to screen for exclusions monthly, and the majority of states followed suit, Malone said. “But there is still confusion and a lack of consistency in the frequency,” she noted. “Our suggestion is, whether the state requires it or not, screen every 30 days to ensure you are catching updates.” That’s consistent with the recommendation in OIG’s 2013 exclusion guidance.

When health care organizations identify an excluded employee or vendor, they don’t necessarily have to spill their guts to OIG, Landa contended. “There is no affirmative obligation to report an excluded provider” under the CMP law. They are obliged, however, to return overpayments stemming from exclusions within 60 days of identification, according to the 60-day Medicare overpayment refund rule, he noted. Some health care organizations take that route. “We know facilities that adjust their cost report and state, ‘we are removing the salary associated with the excluded provider,’” Landa explained. Of course, if OIG finds out about exclusion, it may levy a CMP, with the health care organization losing the benefits of self-disclosure.

According to the Self-Disclosure Protocol (SDP), which OIG updated in 2013, health care organizations that come clean about potential misconduct probably avoid corporate integrity agreements and settle CMP cases for reduced amounts — generally a 1.5 multiplier on damages. If it’s an exclusion matter, Landa said, submissions to the SDP should:

- Explain how the exclusion was discovered by the health care organization and why it was overlooked initially.
- Describe the screening program. “Don’t fall into the category where OIG thinks you stuck your head in the sand,” he advised.
- Show how the employment of an excluded person was an anomaly.
- Update policies and procedures to ensure exclusions are identified.

HIPAA

Provider Confusion and Interoperability Concerns Prompt OCR and ONC to Release Guidance on PHI Sharing


Last Friday, the U.S. Department of Health and Human Services Office of the National Coordinator for Health IT (“ONC”) and the Office for Civil Rights (“OCR”) released two fact sheets regarding permitted uses and disclosures of protected health information (“PHI”) among health care providers and other entities covered by HIPAA. ONC and OCR developed these fact sheets after health care providers expressed confusion over if and when PHI can be shared without the patient’s prior written consent under the HIPAA Privacy Rule (the “Privacy Rule”). Additionally, as ONC
has been actively pushing health care providers toward interoperability of electronic health recordkeeping systems, many view the lack of clarity and understanding around the Rules a hindrance to achieving this goal.

In the fact sheets, ONC and OCR provide specific examples of these uses and disclosures allowed by HIPAA if particular safeguards have been established. The first fact sheet is directed toward Covered Entities and addresses uses and disclosures for health care operations. The first fact sheet reminds Covered Entities that a Covered Entity can disclose PHI to another Covered Entity or the Covered Entity’s business associate for certain health care operations of the Covered Entity receiving the patient information. Such health care operations include developing protocols or clinical guidelines, performing case management or care coordination, and implementing quality assessment or improvement activities. However, Covered Entities may only exchange PHI in these instances if (1) the other Covered Entity also has a relationship with the patient; (2) the PHI relates to the relationship between the Covered Entity and patient; and (3) the Covered Entity discloses the minimum information necessary to accomplish the health care operation.

The second fact sheet provides examples of when Covered Entities may share PHI for a patient’s treatment. The Privacy Rule broadly defines treatment to include providing, coordinating, and managing a patient’s care, as well as consulting between providers and referring patients to another provider. The fact sheet clarifies that when one Covered Entity properly provides PHI to another Covered Entity for a patient’s treatment, the disclosing entity is responsible for securely transmitting the information, and the receiving entity is responsible for safeguarding the information once received. The fact sheet describes the requirements for different relationships between Covered Entities, such as between a hospital and the patient’s physician, a physician and a care planning company hiring to coordinate care for the physician’s patients, and a hospital and long-term care facility to which a patient is discharged.

The fact sheets do not alter the ways in which Covered Entities may use PHI for health care operations or treatment, but they do provide useful guidance to Covered Entities for when and how PHI may be shared.

Information Security and Privacy

FDA Releases Draft Guidance for Medical Device Cybersecurity

Health Law and Policy Matters – February 1, 2016

It seems that everything in our life is getting connected to the Internet. We now live in an age where household items like refrigerators have Internet-connected LCD screens and privacy experts talk about the so-called “Internet of Things.” Medical devices are increasingly becoming connected as well, and like any connected device, they are at risk of getting hacked. In 2014, the U.S. Food and Drug Administration (“FDA”) released final guidance recommending that device manufacturers consider cybersecurity risks when designing and developing their devices. Last month, FDA released separate draft guidance with recommendations for how companies should address the cybersecurity of medical devices after they are released into the market.

Principles of a Postmarket Cybersecurity Management Program

The cornerstone of FDA’s cybersecurity guidance for industry — in both the premarket and postmarket context — is the development of a risk management program. In its new guidance, the FDA identifies a number of critical components that should be included in the device manufacturer’s postmarket risk management program. These include:

• Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
• Understanding, assessing, and detecting presence and impact of a vulnerability;
• Establishing and communicating processes for vulnerability intake and handling;
• Clearly defining essential clinical performance to develop mitigations that protect, respond, and recover from the cybersecurity risk;
• Adopting a coordinated vulnerability disclosure policy and practice; and
• Deploying mitigations that address cybersecurity risk early and prior to exploitation.
**Essential Clinical Performance**

The fourth component mentioned above introduces a concept that is central to the guidance: “essential clinical performance.” As noted by FDA, the majority of actions taken by manufacturers to address cybersecurity vulnerabilities and exploits are considered “cybersecurity routine updates or patches.” In these cases, the FDA would not require advance notification, premarket review or reporting under its regulations. However, a small subset of vulnerabilities and exploits may, according to the draft guidance, compromise the essential clinical performance of a device and thus present a reasonable probability of serious adverse health consequences or death. In these circumstances, FDA would require the manufacturer to notify the agency. FDA defines essential clinical performance as “performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer.”

According to the draft guidance, manufacturers should define the essential clinical performance of their device, the resulting severity outcomes if compromised, and the risk acceptance criteria. Manufacturers should conduct this analysis in an objective manner by considering two factors:

1. The exploitability of the cybersecurity vulnerability; and
2. The severity of the health impact to patients if the vulnerability were to be exploited.

FDA acknowledges that objectively assessing the exploitability of a device is difficult, especially if there is an absence of data. Instead of using conventional medical device risk management approaches, FDA suggests that manufacturers consider using a cybersecurity vulnerability assessment tool or similar scoring system, such as the Common Vulnerability Scoring System. In terms of objectively assessing the severity of the health impact, moreover, FDA recommends that manufacturers use the qualitative severity levels described in the International Standard Organization’s Standard for the application of risk management to medical devices.

**Controlled vs. Uncontrolled Risks**

According to FDA, a key purpose of conducting the above assessment is to evaluate whether the risk to essential clinical performance of the device is controlled (acceptable) or uncontrolled (unacceptable). One method of assessing the acceptability of risk to essential clinical performance is by indicating in a matrix which combinations of “exploitability” and “severity impact to health” represent risks that are controlled or uncontrolled. The draft guidance contains an example of an approach that could be used to assess the risk to the device’s essential clinical performance:

As is apparent from the matrix above, not every assessment will yield a black or white result. FDA acknowledges this grey area, but nevertheless recommends that manufacturers make a binary determination that a vulnerability is either controlled or uncontrolled. The result of this binary determination is crucial: if a manufacturer concludes that there is uncontrolled risk to their device’s essential clinical performance, FDA expects the manufacturer to report these vulnerabilities to FDA according to 21 C.F.R. 806 (mandatory reports of product corrections or removals). At the same time, the FDA has also decided to exercise discretion in this area, and it does not intend to enforce these reporting requirements if:

1. There are no known serious adverse events or deaths associated with the vulnerability;
2. Within 30 days of learning of the vulnerability, the manufacturer identifies and implements device changes and/or compensating controls to bring the residual risk to an acceptable level and notifies users; and
3. The manufacturer is a participating member of an Information Sharing Analysis Organization (“ISAO”), such as the National Health Information Sharing & Analysis Center.

The fact that FDA makes participation in an ISAO a condition of the agency’s discretionary enforcement sends a strong message to device manufacturers that cooperation across the industry is a critical component of postmarket cybersecurity. To this end, the agency recently held a public workshop to discuss these issues, which we plan to highlight in a future blog post. In the meantime, interested parties can submit comments on the new cybersecurity draft guidance until April 21, 2016.
Hackers demand ransom from California hospital

*Bricker and Eckler – February 17, 2016*

Hollywood Presbyterian Medical Center has been the victim of a recent cyber-attack that shut down the hospital’s network and placed it in a state of crisis. The attack was conducted using a type of malware known as ransomware. The hack has caused a state of emergency for the hospital and has compromised the hospital’s ability to care for its patients. Medical professionals have been unable to access patient records stored on the hospital’s network, and it is unknown whether patient or employee records have been compromised in the attack. The attackers are demanding an unprecedented $3.6 million ransom to release the hospital’s network.

From a cybersecurity perspective, ransomware infects computers and restricts users’ access to their files or threatens the permanent destruction of their information unless a ransom is paid. There are different types of ransomware — some prevent users from accessing their computer’s operating system, some encrypt files to prevent access and others stop certain applications from running (such as a web browser). Ransomware can infect a computer via a malicious email or website, or attackers can deliver it directly if they’ve already infected a computer with a backdoor through which they can enter. Several individuals and organizations have been victims, and, in January 2015, the FBI issued a warning that there has been an uptick in the use of ransomware by cyber criminals lately.

This is the first high profile incident of ransomware used against a hospital. It remains to be seen what the HIPAA implications are from this event. It was reported that the hospital has stated that there is no evidence that medical records have been accessed or extracted by the hackers. It appears the ransomware may only be blocking the hospital from its own system. However, if the hackers have control of the medical records, it would appear that this would be a HIPAA breach. Additionally, the HIPAA Security Regulations require that a covered entity have procedures for obtaining necessary electronic protected health information during an emergency. The preamble to the regulations state that “…in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or man-made disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.” This may not be exactly what they had in mind by “man-made disaster,” but it would seem to present the same issue and, thus, may be a HIPAA violation merely if the hospital cannot access its own records.

Hollywood Presbyterian Concedes to Hacker’s Demands in Ransomware Attack

*Health Law and Policy Matters – February 19, 2016*

In a chain of events that should be a wake-up call to any entity using and storing critical health information, Hollywood Presbyterian Medical Center (“HPMC”) has announced that it paid hackers $17,000 to end a malware attack on the hospital’s computer systems. On February 5, HPMC fell victim to an attack that locked access to the medical center’s electronic medical record (“EMR”) system and blocked the electronic exchange of patient information. Earlier reports indicated that the attack was random, though Brian Barrett, writing for *Wired*, questioned that assertion.

The medical center’s announcement of the resolution of the incident indicates that there is no evidence that patient or employee information was accessed by the hackers as part of the attack. Even if the data was not compromised, the attack led to enormous hassles at the hospital, returning it to a pre-electronic record-keeping system.

On February 2, 2016, three days before the HPMC attack, the Department of Health & Human Services Office for Civil Rights (“OCR”) announced the launch of its new Cyber-Awareness Initiative. That announcement included information on ransomware attacks and prevention strategies. Suggested prevention strategies from OCR included:

1. Backing up data onto segmented networks or external devices and making sure backups are current.
2. Ensuring software patches and anti-virus are current and updated.
3. Installing pop-up blockers and ad-blocking software.
4. Implementing browser filters and smart email practices.

Most of these prevention strategies are HIPAA security measures that ought to be in place generally. As OCR indicates, smart email practices and training the workforce on them are key elements to preventing phishing scams. Before clicking on a link in an email or opening an attachment, consider contextual clues in the email. The following types of messages should be considered suspicious:

- A shipping confirmation that does not appear to be related to a package you have actually sent or expect to receive.
- A message about a sensitive topic (e.g., taxes, bank accounts, other websites with log-in information) that has multiple parties in the To: or cc: line.
- A bank with whom you do not do business asking you to reset your password.
- A message with an attachment but no text in the body.

All health care providers, payors, and their business associates need to take notice of the HPMC attack and take steps to ensure that they are not the next hostages in a ransomware scheme.

White House’s Cybersecurity National Action Plan (CNAP) Includes Cybersecurity Awareness Campaign, Creation of Federal Privacy Council

Cybersecurity – February 9, 2016

Following the announcement of the President’s Cybersecurity National Action Plan (CNAP), an initiative designed to “enhance cybersecurity capabilities within the Federal Government and across the country,” the White House has released a fact sheet outlining the different components of the CNAP. The announcement of the CNAP follows the President’s request for $19 billion in funding for cybersecurity initiatives in fiscal year 2017, an increase of 35% over the previous year’s request. The CNAP includes a mixture of near-term measures and long-term objectives, with the ultimate goal of enhancing the federal government’s cybersecurity posture while encouraging private citizens and businesses to do the same. Some of the most significant aspects of the CNAP, discussed further below, include:

- The launch of a cybersecurity awareness campaign to promote the use of multi-factor authentication;
- A “systematic” review by the White House to identify areas where the federal government can reduce the use of Social Security Numbers as individual identifiers;
- Plans for the development of a Cybersecurity Assurance Program to test and certify connected devices against certain security standards;
- The creation of a Chief Information Security Officer (CISO) position within the federal government, coupled with a $3.1 billion initiative to modernize federal agencies’ IT systems and applications;
- The establishment of a commission of private sector cybersecurity experts to offer recommendations on cybersecurity initiatives; and
- The establishment of a Federal Privacy Council, composed of representatives from various key federal agencies, to coordinate guidelines for the federal government’s collection and storage of data.

Legislation

Final Rule Regarding Return of Medicare Overpayments Is More Favorable to Providers Than Anticipated
One element of the Affordable Care Act (ACA), enacted in March 2010, requires providers to identify, report and return Medicare overpayments. A provider’s failure to do so can result in False Claims Act liability, Civil Monetary Penalties and, in serious cases, exclusion from federal health care programs. On February 11, the Centers for Medicare and Medicaid Services (CMS) issued a long-awaited final rule implementing this requirement. A few key provisions of this final rule are much more favorable to providers than those contained in CMS’ earlier proposed rule.

The ACA requires that providers report and return any Medicare overpayments by the later of (i) 60 days after the date on which the provider identified the overpayment or (ii) the date that any corresponding cost report is due. Until the issuance of the final rule, providers were uncertain of two things. First, how far back does the obligation to return overpayments extend? In other words, how far back does a provider need to look in determining whether it was overpaid? Second, when is a provider deemed to have “identified” an overpayment, starting the 60-day clock? We now have answers to these questions.

Look Back Period

The final rule requires that a provider report and return an overpayment if it identifies the overpayment within six years of the date that the overpayment was received. This 6-year look back period is down from the 10-year period reflected in the proposed rule. This change aligns the final rule with similar state and federal record retention requirements and helps to address providers’ concerns regarding the burden and cost of a 10-year look back period.

Identification of an Overpayment

The final rule also provides additional helpful guidance regarding when an overpayment is "identified" and thus when the 60 day clock starts ticking to return the overpayment. Prior to the issuance of this final rule, providers felt immense pressure to investigate a potential overpayment at lightning speed, trying to balance the accuracy of the investigation and the subsequent report with the need to act rapidly. The final rule makes clear that the 60-day clock starts only after the provider, using reasonable diligence, determines and quantifies the amount of the overpayment. "Reasonable diligence" is demonstrated through the timely, good faith investigation of credible information, which takes a maximum of six months following the receipt of the credible information, except in extraordinary circumstances (i.e. complicated self-referral law violations, natural disasters or states of emergency). We note that CMS’ commentary makes clear that reasonable diligence may include an audit and subsequent extrapolation to arrive at the reasonable overpayment amount. However, CMS’ commentary also makes clear that providers must engage in proactive measures to determine whether they have received overpayments – simply waiting for a problem to come to light is not enough. As you would expect, maintaining documentation of all investigatory efforts is critical and should not be overlooked. Of course, if the provider did in fact receive an overpayment and fails to conduct reasonable diligence, the 60-day clock starts to tick on the date that the provider received credible evidence of the overpayment.
Obama’s Budget

Two enforcement goals for the Education Department appear in Obama’s proposed federal budget.

A couple of lines in the budget's appendix confirm the administration's plans for the Education Department to hold colleges accountable. Here's the first:

**OFFICE OF CIVIL RIGHTS**

For expenses necessary for the Office of Civil Rights, as authorized by section 203 of the Department of Education Organization Act, [$107,000,000] $137,708,000. (Department of Education Appropriations Act, 2016.)

<table>
<thead>
<tr>
<th>Program and Financing (in millions of dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification code 091-0700-0-1-751</td>
</tr>
<tr>
<td>Obligations by program activity:</td>
</tr>
<tr>
<td>0001 Civil rights ...................................</td>
</tr>
<tr>
<td>2015 actual   100</td>
</tr>
</tbody>
</table>

Last year, you might recall, President Obama asked for a $31-million increase in funding for the department's Office for Civil Rights, which enforces the Title IX rules that require colleges to investigate and resolve complaints of sexual misconduct. He ended up getting a boost of $7 million instead.

This year he is again seeking $31 million more — enough to create more than 150 new, full-time positions in the office.

Here's the second key line:

**Employment Summary**

<table>
<thead>
<tr>
<th>Identification code 091-0202-0-1-502</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obligations by program activity:</td>
</tr>
<tr>
<td>1001 Direct civilian full-time equivalent employment ...</td>
</tr>
<tr>
<td>2015 actual   1,375</td>
</tr>
</tbody>
</table>

This is a request for more than 80 new positions in the Office of Federal Student Aid. Education Department officials announced on Monday their intent to create a new "Student Aid Enforcement Unit" to root out abuses in student lending and related areas. The department plans to move some existing employees into that unit, but it's also looking to staff up. — B.R.

Regulatory Requirements

To Get Credit for Cooperating with a DOJ Investigation, Get Ready to Certify Your Disclosures
Dentons.com – February 9, 2016

Late last week, the *Wall Street Journal* reported that the US Department of Justice's (DOJ's) fraud section is developing a process for settling companies to certify that they have disclosed fully all information about individuals involved in wrongdoing before finalizing a settlement agreement. This means that the company not only must "name names" as established by the recent Yates Memorandum, but now a corporate officer will be required to certify and "confirm to [the DOJ] that they have, in fact, turned over all non-privileged information about individuals."

The impact of such a certification should have ripple effects back to the initiation of any internal investigation, informing how even initial interviews and discussions are conducted. And, like the Yates Memo, eventual certification must be dropped into the complex considerations of whether or not to self-disclose.
On September 9, 2015, Deputy Attorney General Sally Q. Yates sent a memorandum within the DOJ, adding to and clarifying the Department's Principles of Federal Prosecution policy, which sets out the requirements for receiving cooperation credit in plea or settlement agreements. A key portion of that Memorandum adopted an unwritten, and inconsistently enforced, requirement that in order to get any cooperation credit, a corporation must investigate, determine and identify responsible individuals, and must provide a "complete" disclosure of "all" individuals involved in, or responsible for the misconduct, regardless of the person's position. The information that must be disclosed to the DOJ is "all facts" related to the misconduct, not just the relevant facts. The "cooperation credit" is often a critical factor in charging decisions and the mitigation of any fine or penalty handed down for wrongful conduct.

Now apparently, the DOJ will be stacking a certification process on top of the Yates Memo that will require cooperating corporations to enter a written statement of cooperation, where the corporation certifies it has in fact provided all of this information. Once adopted by the DOJ, a General Counsel, Chief Compliance Office, Board Member, Director or Audit Committee Member will have to put himself or herself on the hook regarding the company's disclosure.

One big resulting question is, what can the organization do to ensure the integrity of any disclosure made to the government? A related consideration is what can a corporate officer or director do to provide some protection for themselves when making the disclosure certification? The best course in response to both issues will be to change the way the company conducts pre-investigation planning, and to engage in some difficult discussion up-front, before an investigation is underway. Investigation team members within "the-need-to-know" group should understand from the outset (and be reminded during an investigation) that any evidence of individual misconduct found during a report of, or investigation into, wrongdoing must be disclosed in order to earn cooperation credit. Further, the investigative team must understand that someone will be required to certify that all information about alleged wrongdoers has been disclosed.

Knowing the disclosure of wrongdoing may be in the best interests of the organization may also raise questions whether certain individuals are adverse to the interests of the organization. While it may be unclear where interests line-up at the start of an investigation, planning for the issue and how you will address it at the outset may avoid problems down the road. This is particularly true when it is clear the government will use real or imagined conflicts to challenge the integrity of the investigation.

From the time a call on the hotline is reported, this certification and what the company must do for cooperation credit must be part of the decision-making process. Pre-investigation planning and an understanding of this obligation amongst the investigation team will lay a necessary foundation for that task down the road. It also must be considered in the company's ultimate decision to cooperate and disclose information to the government, as well as related indemnification and appointment of counsel considerations throughout an investigation.

The company's plan on handling this certification, and the accompanying issues it creates, should be closely linked to the company's internal investigations and indemnification policies. Those policies will establish a consistent approach for an investigations team and responsible officers to follow when addressing the expanding challenges they must face in the company's fight for cooperation credit.

In the end, DOJ's latest action demonstrates that pre-investigation planning is a critical step in ultimately deciding how you are going to mitigate your risk if your efforts detect conduct that creates legal risk.

Title IX

A Closer Look at 7 Common Requirements in Resolved Federal Sex-Assault Inquiries

The Chronicle of Higher Education – February 8, 2016

Say your campus likes to encourage students to resolve sexual-misconduct cases through mediated discussions. When a student confides in a professor that a guy took advantage of her while she was drunk and asks her not to tell anyone, the professor obliges.

Clear and convincing evidence is the standard your disciplinary panel insists on before finding someone responsible for an assault.
If you haven’t already heard from the U.S. Department of Education’s Office for Civil Rights, you may soon be in its cross hairs, because when it comes to the gender-equity law known as Title IX, you’re doing it all wrong.

That would be obvious to anyone who has slogged through the hundreds of pages of documents the civil-rights office, or OCR, has released since April 2011, when it issued a pivotal "Dear Colleague" letter that put more pressure on colleges to resolve students’ reports of rape. The Chronicle has posted the 20 or so publicly available resolution agreements in its Title IX investigation tracker.

Those agreements spell out policies and procedures that need to change or be added in order to bring colleges that were under investigation back on the right side of the law.

As of last month OCR had resolved 46 of the more than 240 investigations included in The Chronicle’s tracker. Thirty of those ended in resolution agreements.

"The minute one of these drops, experts are running around saying, ‘What’s the lesson I’m supposed to take away today?’" says Peter F. Lake, chair and director of the Center for Excellence in Higher Education Law and Policy at Stetson University’s College of Law.

It may be buried in a 40-page document. The requirements, he says, "keep getting bigger and broader and more challenging all the time."

Peter Lake: "There are certain basic commandments, and the first is, ‘Thou shalt have a Title IX coordinator.’"

Some requirements are ubiquitous in the agreements. Such mandates include designating a Title IX administrator, putting in place extensive training programs, and using a lower standard of evidence in investigations. Other common elements are climate surveys, reporting requirements, and a warning that informal dispute resolution isn’t appropriate — even on a voluntary basis — when sexual assault or violence is involved.

Colleges face intense pressure today to get it right. Title IX requires that campus officials investigate reports of sexual harassment and assault, whether or not the police are called in. If colleges don’t handle complaints promptly and fairly, they can face penalties, including the loss of all federal funds.

In the early days of its shift toward stricter Title IX enforcement, OCR cut colleges some slack, praising them for whatever improvements they were making. But as the pace of complaints has intensified, the tone has become harsher.

When the Ncherm Group, which advises colleges on Title IX compliance and other issues, pored over many of the resolution agreements, it came up with a 37-point checklist of what OCR was looking for.

A Chronicle review of the resolution agreements issued since 2011 identified several key takeaways. Here are a few:

1. Every campus must have a Title IX coordinator.

"There are certain basic commandments, and the first is, ‘Thou shalt have a Title IX coordinator,’" says Mr. Lake.

"That comes screaming through in every document."

Detailed contact information and procedures for filing complaints should be clearly communicated to students and employees, not just in policy statements that few people read, but in pamphlets, student newspapers, and frequently visited websites.

Along with investigating and adjudicating individual cases of sexual misconduct, Title IX offices should study patterns of behavior among specific student groups, like athletes and freshmen, to determine whether any of them are particularly prone to bad behavior.

2. "Preponderance of the evidence" should be the standard.

Sexual-misconduct policies must all use a "preponderance of the evidence" yardstick for assessing responsibility. Under that standard, which is lower than those used in criminal cases, an accused student is found guilty if the college determines it’s more likely than not that an incident occurred.

Harvard Law School is among the institutions forced to change its standard of proof to meet the lower threshold after the civil-rights office found that its policies violated Title IX. Some Harvard Law professors have joined advocates of accused students in questioning whether that lower threshold is fair.
3. Colleges must offer extensive and continuing training to both students and employees.

At minimum, they should offer freshmen orientation sessions that discuss sexual misconduct, as well as the link between drinking and drugs and sexual violence.

Those sessions, which should be repeated annually for students living in residence halls, should spell out the differences between the Title IX process and the criminal process.

Students should know what to expect from the university and the police when they make a complaint, including the interim steps colleges will take to keep them safe, like changing class schedules or issuing no-contact orders.

Regular training is also required for Title IX coordinators, investigators, and other employees involved in grievance procedures.

4. Colleges should use clear and consistent definitions to describe sexual misconduct.

Guides like this, posted by Indiana University, should include terms such as sexual harassment, sexual violence, and consent. Training should include specific examples of each type of misconduct, from racist jokes to rape. Sexual harassment, for instance, is described in at least one resolution agreement as "unwelcome conduct of a sexual nature" that can include "unwelcome sexual advances, requests for sexual favors, and other verbal, nonverbal, or physical conduct of a sexual nature, such as sexual assault or acts of sexual violence."

Many of the resolution agreements have "boilerplate language" defining sexual harassment and what constitutes a hostile environment, Mr. Lake says. "They use the language repeatedly so it’s become currently understood that that language has to make it into your policy almost word for word."

Anything OCR can do to simplify the hodgepodge of definitions colleges currently use to describe sexual misconduct would be welcome, says Wendy Murphy, a lawyer who has helped students file federal discrimination complaints against several universities.

"Having complicated definitions of sexual misconduct is becoming a pernicious form of injustice by confusion," she wrote in an email. "Schools should have the same short definition of sex discrimination that they have for race discrimination, which should include examples of covered conduct but not boondoggle definitions that make everything needlessly complicated."

5. Investigations should be completed within a reasonable time — usually 60 days.

Unless a college faces "extraordinary circumstances," it should wrap up cases within 60 calendar days and shouldn’t use pending criminal action as an excuse for delay.

Both parties should get regular updates on the progress of a case, as well as written notice of the outcome.

OCR has had a tough time completing its own cases in a reasonable time as the pace of new cases accelerates, with most taking more than a year to resolve.

6. "Responsible employees" must promptly report sexual harassment and violence they hear about.

They could include faculty members, coaches, and resident advisers — basically, anyone except for a clergy member or counselor who has a confidential relationship with a student.

The University of Virginia’s resolution agreement states that "all employees designated as responsible employees will notify the Title IX coordinator or designee within 24 hours of receiving information about possible sexual harassment or sexual violence against students," whether or not the student expresses interest in filing a complaint. If they delay responding, that could constitute a hostile environment and thus a Title IX infraction.

"When you’re a Title IX coordinator, that sends a chill down your spine," says Mr. Lake. "You may have hundreds of ‘responsible employees’ someone could have confided in, and if one drops the ball on reporting potential harassment, the federal government could crack down."

7. Campuses should conduct annual climate surveys.

Among other things, the surveys should measure students’ experiences with sexual misconduct, their knowledge about how to report it, and suggestions on how to prevent it.
"Surveys give campuses a tool to measure whether or not, at a minimum, the social perceptions on campus are changing with improved policies," says S. Daniel Carter, board president of SurvJustice, an advocacy group for victims. "You can’t adequately take on the challenge until you know the full scope of the problem."
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:

- Drone Legislation
- Environmental Protection
- Financial Aid
- Human Resources
- Information Security and Privacy
- International Students
- Risk Management
- Title IX

Drone Legislation

Higher Education Unmanned Aircraft Systems Modernization Act

NACUA – March 7, 2016

Legislation (S. 2626) introduced in the U.S. Senate by Senators Gary Peters (D-MI) and Jerry Moran (R-KS) entitled the "Higher Education Unmanned Aircraft Systems Modernization Act." The bill would allow institutions of higher education to operate small unmanned aircraft systems (sUAS) for educational and research purposes. After being introduced on March 3, the bill was referred to the Committee on Commerce, Science, and Transportation.

Note: A the proposed legislation would require institutions of higher education to have established policies that include a central point of contact for review, approval, and control of drone operations and certification of safety and pilot capability.

Environmental Protection

Oregon State University Agrees to Safely Manage Hazardous Waste to Better Protect Students and Faculty

EPA – March 14, 2016

Oregon State University has agreed to provide comprehensive training for its personnel to properly identify hazardous waste generated at its campus in Corvallis, Oregon. In the settlement announced today by the Environmental Protection Agency, the university will also pay $275,000 in penalties for multiple violations of federal hazardous waste identification rules and agreed to comply with waste management requirements.

“Strict accountability for hazardous waste is vital to protecting people and the environment at every step of the way,” said Director Ed Kowalski of EPA’s Pacific Northwest Office of Compliance and Enforcement. “Without knowing what its hazardous wastes were from the very beginning, it was impossible for Oregon State University to ensure its chemicals were handled safely, which could have put students, faculty, and first responders at significant risk.”

In 2013, EPA inspectors found nearly 2000 containers of hazardous wastes, in at least six OSU campus laboratories and other buildings that were not properly identified, managed or safely stored, in violation of the federal Resource Conservation and Recovery Act (RCRA). Multiple types of hazardous wastes were found, including solvents and other flammable liquids, acids and other caustic, toxic and reactive chemicals, and used oil. In addition, OSU did not have a RCRA permit to manage and store the hazardous wastes.

Failure to accurately identify hazardous wastes increases the likelihood that it will be improperly managed as non-hazardous waste, or that not all of the hazards will be identified before treatment or disposal. Considerable quantities of hazardous chemicals are found not just at large manufacturing facilities, but at a variety of facilities, where they pose the very same risks. OSU is a college campus with more than 25,000 students and 4,700 full time employees, and the potential for harm was substantial if a release, fire, or explosion had occurred near a classroom or other
building where hazardous wastes were being generated. Several of the locations where mismanaged waste was accumulated were in close proximity to students and faculty.

OSU’s failure to identify all of the hazards associated with each waste also posed a safety threat to the facilities with which OSU contracts to transport, treat and dispose of the waste. If a spill occurred during transportation, the flammable, reactive or other hazards from the waste might not be known to the transporter or emergency responders, putting them at risk. If misidentified wastes were sent to a treatment and disposal facility then incineration, neutralization, and even mixing with water could have resulted in fires or explosions.

In addition, because OSU failed to properly identify its hazardous wastes, waste disposed of as non-hazardous may well have been hazardous, and therefore unsuitable for disposal in a non-hazardous solid waste landfill. Landfill workers who subsequently handled these materials were put at risk of harm in handling wastes that should have been identified as hazardous wastes.

If OSU had identified its hazardous wastes at the point of generation as required by RCRA, the wastes could have been safely managed and this potential for harm could have been significantly decreased.

Financial Aid

**Student Aid Enforcement Unit Formed to Protect Students, Borrowers, Taxpayers**

_**U.S. Department of Education**—February 8, 2016_

As part of the Obama Administration's aggressive action to protect students and taxpayers, the U.S. Department of Education is creating a Student Aid Enforcement Unit to respond more quickly and efficiently to allegations of illegal actions by higher education institutions.

"When Americans invest their time, money and effort to gain new skills, they have a right to expect they'll actually get an education that leads to a better life for them and their families," said Acting Secretary of Education John B. King Jr. "When that doesn't happen we all pay the price. So let me be clear: schools looking to cheat students and taxpayers will be held accountable."

The Enforcement Unit will be led by Robert Kaye, one of the nation's top enforcement attorneys - most recently as a leader in the Federal Trade Commission's work protecting consumers. Through his work as the Bureau of Consumer Protection's Chief Litigation Counsel and as a manager in the Bureau's Division of Enforcement, Kaye has considerable experience supervising and advising managers and attorneys engaged in consumer protection investigations, as well as federal court and administrative litigation.

Kaye will report to Jim Runcie, the Chief Operating Officer of the Office of Federal Student Aid (FSA), under the oversight of the Under Secretary Ted Mitchell. The Chief Enforcement Officer will work closely with James Cole Jr., General Counsel, Delegated the Duties of Deputy Secretary, to establish policies and practices.

As part of the 2017 budget, the President is requesting $13.6 million in additional funds to strengthen FSA's enforcement and oversight activities. The office will work with closely with federal and state agencies to investigate and bring actions against bad actors in order to best protect students and taxpayers. The Enforcement Unit will consist of the following four divisions:

- **Investigations Group** — to identify potential misconduct or high-risk activity among higher education institutions and protect federal funding.

- **Borrower Defense Group** —to provide legal analysis, support and advice concerning claims of borrowers of Direct Loans. The unit will analyze claims to make determinations of injury, investigate institutions in connection with borrower defense claims and coordinate with federal and state agencies regarding those claims.

- **The Administrative Actions and Appeals Service Group (AAASG)** —to impose administrative actions such as Emergency, Termination, Limitation, Suspension or Fine actions. This group will continue to resolves appeals by program participants from final audit and final program review determinations, initiate debarment and suspension actions, and issue school revocation and denials of re-certification.
**Human Resources**

**Colleges Brace for Overtime Overhaul**


Schools across the country are bracing for a surge in personnel costs as they prepare for the Obama administration’s overhaul to overtime-pay rules.

Under the plan, Obama would increase the threshold under which salaried workers receive overtime pay from $23,660 to $50,440 making about 5 million U.S. workers newly eligible for overtime pay.

While the rule will apply to employers of all kinds, higher-education institutions say their missions and circumstances mean they’ll be hit in ways that other types of employers aren’t. School officials, who say they’re under pressure to keep a lid on tuition, have warned of cuts in student services, degree offerings and labor-intensive research on issues such as climate change and cancer.

The new requirements are creating a clash between two White House priorities: strengthening the middle class by raising pay for many workers and relieving tuition burdens on college students.

Given the administration’s desire to rein in student debt, many colleges question the wisdom of the details in the overtime-pay proposal, saying that doubling the salary threshold is too extreme, for example. “Adding additional financial burdens on higher education institutions does not make good fiscal sense,” Southeast Missouri State University told the Labor Department. The university said the rule could cause schools to curb bonuses and other benefits.

The rule reached its final stages of review last week when the Labor Department sent it to the White House’s Office of Management and Budget. That office will have 90 days to review it, including analyzing the costs and benefits, though that could be extended.

Administration officials say inflation has eroded the value of the existing threshold of $23,660 a year since it was last updated in 2004, leaving too few workers eligible for overtime pay while working more than 40 hours a week.

Universities are busy determining which workers will be affected and what their costs will be if regulators don’t scale back the proposal. Though professors and others who primarily teach are expected to be untouched by the rule under a longtime teaching exemption that still leaves a huge swath of staff.

To afford the cost of compliance, institutions say they’ll likely use a combination of raising salaries, paying overtime, and forbidding some work.

Research universities reliant on postdoctoral associates—academic employees and trainees who have earned Ph.D.s and take on labor-intensive projects to advance their careers—will feel a particular blow, say school officials who fund some of these positions with federal grants that have been stagnant or declining.

“It’s a finite bucket of money in higher education,” said David Blake, chairman of the public-policy group for the College and University Professional Association for Human Resources.
Information Security and Privacy

10 Lessons from FTC Guidance on Data Security

Corporate Counsel – March 1, 2016

“Not if, but when.” These simple words are enough to keep corporate counsel, compliance officers and IT managers up at night when faced with the reality that their network will at some point be breached. This is no surprise given the spate of corporate breaches and unauthorized network intrusions reported in recent years as well as the costs, reputational harm and investigations and lawsuits that follow in their wake. While there are no silver bullets to stop breaches from occurring, understanding and following legal actions brought by regulatory agencies and heeding security guidance they issue could go a long way in preventing security lapses and unauthorized attacks.

There is no omnibus federal law that prescribes the level of security that companies must use to protect consumer information. Instead, Congress has identified certain categories of sensitive data that warrant regulation, such as health and financial information, and online information collected from children under 13, resulting in the Health Information Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Children’s Online Privacy Protection Act, respectively.

Each of the above laws (and their implementing regulations) to some extent dictates specific data security standards for companies that possess consumer information in these industries. But for the vast number of companies that do not fall within these categories, knowing what standards they are expected to employ to protect consumer information remains an elusive task. Notwithstanding this void, companies that fail to develop a comprehensive data security plan and implement at least some level of minimum security measures to protect consumer information remain vulnerable to attacks, lawsuits and regulatory investigations.

Enter the FTC

Companies that experience a data breach of some sort can expect to hear from the Federal Trade Commission shortly following the breach becoming public. The agency has brought over one hundred privacy and data security cases under its broad jurisdiction authority pursuant to Section 5 of the FTC Act (15 U.S.C. § 45), which empowers it to investigate and halt unfair and deceptive acts and practices in commerce.

The FTC’s privacy enforcement docket has historically involved companies that failed to abide by their posted privacy policies, which the agency claims violated the FTC Act for being a deceptive trade practice. But the FTC has also brought cases against companies that have failed to take adequate precautions to protect consumer information, alleging that such failure was unfair to consumers, since they could not reasonably avoid the harm that may result from such inadequacies.

But therein lies the rub. How can the FTC claim that a company has not adequately protected consumer information if it and Congress have not given industry specific guidance to follow?

Two companies took the FTC to task on this issue by challenging the agency’s authority to bring data security enforcement cases in the absence of clear and prior guidance. Both of these cases have recently reached resolution, with differing, though logical, results.

Last summer, the U.S. Court of Appeals for the Third Circuit upheld a district court’s finding that the FTC does have the authority to review and scrutinize a company’s data security practices under Section 5 of the FTC Act. The FTC sued Wyndham Worldwide Corporation in federal district court in December 2012 for failing to employ reasonable and appropriate protections for consumer information, which resulted in several data breaches and caused “the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers’ accounts, and more than $10.6 million in fraud loss.”

Wyndham moved to dismiss the action by challenging the FTC’s authority to bring claims under Section 5 in the absence of specific and particular data security standards. The district court rejected Wyndham’s motion and the Third Circuit affirmed.

Three months later an FTC administrative law judge ruled against the agency in a case involving a cancer-screening laboratory’s failure to adequately protect sensitive consumer information. The ALJ dismissed the agency’s August 2013 complaint alleging that LabMD failed to employ “reasonable and appropriate” data security for consumer
information, which “caused, or is likely to cause substantial injury to consumers.” Like Wyndham, the FTC investigation followed several breaches by LabMD that collectively exposed personal information of approximately 10,000 consumers. The FTC’s complaint alleged that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network, and company documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves.

The complaint concluded that LabMD’s alleged failure to employ such measures amounted to an unfair trade practice under the FTC Act by causing, or being likely to cause, substantial harm to consumers that is not reasonably avoidable by consumers or outweighed by benefits to consumers or competition. The ALJ disagreed, finding that “FTC complaint counsel had failed to carry its burden of proving that LabMD’s alleged failure to employ reasonable data security constitutes an unfair trade practice, because complaint counsel failed to prove that the allegedly unreasonable conduct caused or was likely to cause substantial injury to consumers.” He added, “At best, Complaint Counsel has proven the ‘possibility’ of harm, but not any ‘probability’ or likelihood of harm. Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) [of the FTC Act] requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case.”

This matter is far from over, since the FTC has appealed the decision to the full FTC Commission, which will likely result in the decision being overturned. But the ALJ’s finding does fall in line with a string of cases questioning whether regulatory investigations and class actions are appropriate where no harm resulted from an actual or potential data breach.

While these decisions may appear conflicting, they address very different issues and are in fact mutually exclusive. Wyndham involved actual proven consumer harm whereas LabMD did not. Query whether the Third Circuit and the lower court would have upheld the FTC’s authority to prosecute inadequate security practices in the absence of provable and discernible harm. The lack of harm was very much the centerpiece issue for the FTC’s ALJ in LabMD.

Regardless of the final outcome of these cases, companies that collect and maintain consumer information, particularly sensitive information such as account numbers, must develop and implement sound data security policies and procedures designed to prevent unauthorized breach and intrusion. In the absence of statutory prescriptions to follow, the FTC has published a document that many consider to be a treasure map to the FTC’s secret vault of security expectations.

This document, titled “Start with Security: A Business Guide,” follows a series of FTC workshops and papers involving privacy and data security. It highlights the following 10 practical lessons that can be drawn from over 50 data security cases the agency has brought over the last decade.

1. The FTC urges companies to factor security into every aspect of their business, especially when developing data collection, retention and use policies. Specifically, companies should not collect unneeded personal information, should only retain collected information for as long as needed, and should not use such information for unnecessary purposes.

2. Companies should limit access to personal information to only those employees and vendors who need it.

3. Companies should require persons with access to personal data to use strong and effective passwords and employ encryption devices when the nature of the data warrants stronger protection.

4. Companies should maintain sensitive personal information securely throughout its life cycle, both when in storage and when in transit.

5. They should design networks to separate internal networks containing consumer information from the Internet and employ intrusion detection software to monitor for malicious activity.

6. Given the explosive growth of telecommuters and vendors that remotely access company networks, companies should secure endpoint security by requiring strong passwords and antivirus software on all remote computers and devices.

7. They should employ security sensitivities in all new product development so that engineers and developers consider current and future product uses and scaling. Companies should also consider the platform guidelines on which the products may be run and accessed.
8. Businesses should require third-party service providers to implement appropriate security measures commensurate with the work they will perform and the data to which they will have access and should monitor their activity.

9. They should keep antivirus and third-party software updates current, implement required patches as quickly as possible, and take network vulnerability warnings seriously.

10. Finally, they should apply the same level of sensitivity and diligence to office hardware and paper files as they would electronic files. Specifically, companies should develop and implement security policies for the storage of files and hardware while on and off company premises as well as the destruction of such materials when no longer needed.

Data breaches are the new reality. As hackers continue to develop technological capabilities faster than data protection specialists can, and companies increasingly allow remote access to corporate networks by employees and vendors, it is virtually impossible to protect these networks from unauthorized attacks. But, following the FTC’s guidance outlined above will go a long way in preventing such events from occurring. In the event of a breach and a follow-on FTC inquiry, being able to show that this guidance was followed might stave off a full regulatory investigation and consent agreement. And better yet, following the guidance just makes good business sense.

PwC Report: Cybercrime on the Rise

Cybercrimes like data breaches are getting lots of attention these days. But does the average company need to worry about them? The answer is a resounding yes, according to a survey from Pricewaterhouse Cooper, which found that cybercrime has become the second most common type of economic crime.

Of the 6,000 executives across the world who participated in the survey, 38 percent reported that their organizations dealt with economic crime in the last 48 months. Cybercrime increased big time, with 32 percent reporting an incident in the last two years. That’s an 8 percent increase from a year ago. Cybercrime was up and is now the second-most-reported type of economic crime (asset misappropriation is No. 1).

Cybercrimes can cause major losses, according to the report. Of the respondents affected by cybercrime, about 15 percent reported losses of more than $1 million; 2 percent reported losses in excess of $100 million.

Despite this potential for losses, many boards of directors aren’t focusing on cybercrime. Globally, just 27 percent of boards request information about the company’s state of cyber-readiness more than once a year, the report found.

International Students

Final rule published in the Federal Register by the Department of Homeland Security amending its F-1 nonimmigrant student visa regulations on optional practical training (OPT) for students with degrees in science, technology, engineering, or mathematics (STEM) from accredited U.S. higher education institutions. The final rule allows F-1 STEM degree students pursuing twelve months of OPT in the United States to extend the training period by 24 months. The rule also includes "Cap-Gap" relief for any F-1 student who has filed a timely H-1B petition and request for change of status. The final rule will go into effect on May 10, 2016.

Risk Management

More organizations are realizing that additional risk management sophistication is warranted given the fast pace at which complex risks are emerging, according to results of the fourth annual joint survey assessing the current risk
Current Issues in Compliance  
March 2016

environment by global consulting firm Protiviti and the Enterprise Risk Management (ERM) Initiative at the North Carolina State University Poole College of Management.

Released today, Executive Perspectives on Top Risks for 2016 (www.protiviti.com/TopRisks) summarizes the concerns of 535 Board members, C-suite and other top-level executives around the world and across industries. In the survey, respondents rate the significance of 27 risk issues for the coming year, spanning three risk categories: macroeconomic, strategic and operational.

Regulatory change and heightened regulatory scrutiny is the number one risk cited by survey respondents for the fourth consecutive year, highlighting its dominance on the minds of Board members and executives worldwide. The majority (60 percent) of respondents believe this risk will continue to have a significant impact on their organizations, indicating business executives remain highly concerned about the effect of the regulatory landscape on their strategic direction.

The Top 10 Risks for 2016

The following are the top 10 risks identified in the annual Board member and executive risk survey, along with the percentages of respondents who identified each risk as having a “significant impact” on their business:

1. Regulatory changes and regulatory scrutiny may heighten, noticeably affecting the manner in which products or services will be produced or delivered (60 percent)
2. Economic conditions in markets currently served may significantly restrict growth opportunities for the organization (60 percent)
3. The organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt its core operations and/or damage its brand (57 percent)
4. The organization’s succession challenges and ability to attract and retain top talent may limit its ability to achieve operational targets (52 percent)
5. Ensuring privacy/identity management and information security/system protection may require significant resources for the organization (53 percent)
6. Rapid speed of disruptive innovations and/or new technologies within the industry may outpace the organization’s ability to compete and/or manage the risk appropriately, without making significant changes to its business model (51 percent)
7. Resistance to change may restrict the organization from making necessary adjustments to the business model and core operations (49 percent)
8. Anticipated volatility in global financial markets and currencies may create significantly challenging issues for the organization to address (50 percent)
9. The organization’s culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect core operations and achievement of strategic objectives (45 percent)
10. Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in the organization’s existing customer base (46 percent)

Title IX

University Found Responsible for Bias on an Internship

Inside Higher Ed – March 9, 2016

The U.S. Court of Appeals for the Sixth Circuit has affirmed a jury finding that Wayne State University failed to respond to pregnancy-based discrimination against one of its students. For failing to do so, Wayne State must pay $850,000.

The case illustrates that universities that place students in required internship programs are covered by Title IX of the Education Amendments of 1972 even when the initial alleged discrimination is by an internship provider -- in this case the Salvation Army -- that is not covered by Title IX.
Tina Varlesi, the former student, had been earning good grades in a master's program in social work when she was assigned to an internship at the Salvation Army -- and when she failed at the internship, her ability to graduate was effectively blocked.

Testimony in the trial established that Varlesi's Salvation Army supervisor criticized her pregnancy, telling her not to rub her belly and to wear looser clothes because men in Salvation Army programs were "turned on by her pregnancy." The supervisor also questioned Varlesi's marital status (she was not married) and told others that Varlesi "had relations with someone" and that men in the program could "look but they cannot touch."

The Salvation Army is not covered by Title IX, but the findings against Wayne State are based on how it responded to Varlesi's complaints about how she was treated at the internship.

First, the university did not offer assistance when she raised concerns about what she was being told to do, and the court found that the university even encouraged her to follow some of her supervisor's advice.

Second and perhaps most important, the appeals court decision describes what happened when Varlesi appealed the failing grade she received on the internship to Wayne State, again citing the way her supervisor repeatedly commented on her pregnancy in discriminatory ways. Wayne State told Varlesi that it had investigated and rejected those charges. But as the appeals court noted, the social work dean admitted in the court proceedings that no such investigation ever took place.

Wayne State appealed the jury verdict -- and the size of the award -- on a range of issues. The appeals court unanimously rejected every argument offered by the university.

Matt Lockwood, a spokesman for the university, told The Detroit Free Press that Wayne State was disappointed with the appeals court's decision and was reviewing it.

Deborah Gordon, Varlesi's lawyer, told the newspaper that the decision reflected Wayne State's "complete arrogance" on how it responded to Varlesi. "They pay a lot of lip service to the law and not tolerating any discrimination, but at the end of the day, it's hollow. Now the taxpayers have to foot the bill."
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:

- Financial Aid
- HIPAA
- Human Resources
- Information Security and Privacy
- International Students
- NOTICE Act Compliance
- Risk Management
- Stark Law Compliance

Financial Aid

Student Aid Enforcement Unit Formed to Protect Students, Borrowers, Taxpayers

U.S. Department of Education – February 8, 2016

As part of the Obama Administration's aggressive action to protect students and taxpayers, the U.S. Department of Education is creating a Student Aid Enforcement Unit to respond more quickly and efficiently to allegations of illegal actions by higher education institutions.

"When Americans invest their time, money and effort to gain new skills, they have a right to expect they'll actually get an education that leads to a better life for them and their families," said Acting Secretary of Education John B. King Jr. "When that doesn't happen we all pay the price. So let me be clear: schools looking to cheat students and taxpayers will be held accountable."

The Enforcement Unit will be led by Robert Kaye, one of the nation's top enforcement attorneys - most recently as a leader in the Federal Trade Commission's work protecting consumers. Through his work as the Bureau of Consumer Protection's Chief Litigation Counsel and as a manager in the Bureau's Division of Enforcement, Kaye has considerable experience supervising and advising managers and attorneys engaged in consumer protection investigations, as well as federal court and administrative litigation.

Kaye will report to Jim Runcie, the Chief Operating Officer of the Office of Federal Student Aid (FSA), under the oversight of the Under Secretary Ted Mitchell. The Chief Enforcement Officer will work closely with James Cole Jr., General Counsel, Delegated the Duties of Deputy Secretary, to establish policies and practices.

As part of the 2017 budget, the President is requesting $13.6 million in additional funds to strengthen FSA's enforcement and oversight activities. The office will work with closely with federal and state agencies to investigate and bring actions against bad actors in order to best protect students and taxpayers. The Enforcement Unit will consist of the following four divisions:

- **Investigations Group** — to identify potential misconduct or high-risk activity among higher education institutions and protect federal funding.

- **Borrower Defense Group** — to provide legal analysis, support and advice concerning claims of borrowers of Direct Loans. The unit will analyze claims to make determinations of injury, investigate institutions in connection with borrower defense claims and coordinate with federal and state agencies regarding those claims.

- **The Administrative Actions And Appeals Service Group (AAASG)** — to impose administrative actions such as Emergency, Termination, Limitation, Suspension or Fine actions. This group will continue to resolves appeals by program participants from final audit and final program review determinations, initiate debarment and suspension actions, and issue school revocation and denials of re-certification.
• **Clergy Group** — to ensure institutions comply with the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, requiring colleges and universities participating in federal financial aid programs to disclose campus crime statistics and security information.

The new unit will collaborate with, and incorporate evidence gathered in investigations by, partner state and federal agencies, in building cases against institutions of higher education. The unit will also collaborate with the Program Compliance Unit regarding evidence which may impact ongoing program compliance reviews. Moreover, the new Investigations Group will utilize a broad set of interventions and tools, including subpoena authority, document demands, and interrogatories and interviews to enforce against violations of federal law.

The Department remains strongly committed to investigating violations that harm students and taxpayers and taking swift and immediate action as necessary. These new resources would help ensure such activities are completed in an effective and efficient manner, including supporting more reviews of high-risk institutions, responsive to the concerns raised by states' and other federal agencies' investigations of such institutions, as well as by complaints by students.

The creation of the new Enforcement Unit builds on steps the Obama Administration has taken over the past seven years to hold schools accountable for providing a quality education, including:

- Developing a wealth of consumer tools to help provide families with clear information to make a smart college choice
- Establishing gainful employment regulations to help ensure that students at career colleges don't end up with debt they cannot repay
- Creating a federal interagency taskforce to crack down on bad actors through investigations and enforcement actions
- Enforcing the ban on incentive compensation to protect students from aggressive recruiting practices
- Proposing to close the 90/10 loophole so institutions do not take advantage of service members

In recent weeks, the Department of Education has taken a series of enforcement actions, including actions against DeVry Education Group, Marinello Schools of Beauty, and Computer Systems Institute.

**HIPAA**

**$1.55 million settlement underscores the importance of executing HIPAA business associate agreements**

_HHS Office for Civil Rights in Action - March 16, 2016_

North Memorial Health Care of Minnesota has agreed to pay $1,550,000 to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to implement a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information. North Memorial is a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities.

“Two major cornerstones of the HIPAA Rules were overlooked by this entity,” said Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). “Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure.”

OCR initiated its investigation of North Memorial following receipt of a breach report on September 27, 2011, which indicated that an unencrypted, password-protected laptop was stolen from a business associate’s workforce member’s locked vehicle, impacting the electronic protected health information (ePHI) of 9,497 individuals.

OCR’s investigation indicated that North Memorial failed to have in place a business associate agreement, as required under the HIPAA Privacy and Security Rules, so that its business associate could perform certain payment and health care operations activities on its behalf. North Memorial gave its business associate, Accretive, access to North
Memorial’s hospital database, which stored the ePHI of 289,904 patients. Accretive also received access to non-electronic protected health information as it performed services on-site at North Memorial.

The investigation further determined that North Memorial failed to complete a risk analysis to address all of the potential risks and vulnerabilities to the ePHI that it maintained, accessed, or transmitted across its entire IT infrastructure -- including but not limited to all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes.

In addition to the $1,550,000 payment, North Memorial is required to develop an organization-wide risk analysis and risk management plan, as required under the Security Rule. North Memorial will also train appropriate workforce members on all policies and procedures newly developed or revised pursuant to this corrective action plan.

New guidance and information from OCR and ONC on patient access to medical information

Bricker.com – March 7, 2016

Recently, there have been several important communications from the Office of Civil Rights (OCR) and the Office of National Coordinator (ONC) regarding patient access to medical information.

OCR FACT SHEET AND FAQs

In January 2016, OCR released a Fact Sheet and the first in a series of FAQs, entitled "Individuals’ Right under HIPAA to Access their Health Information 45 CFR § 164.524.” In a January 7, 2016, OCR Director Jocelyn Samuels introduced the new Fact Sheet, stating the Individual Right of Access in the HIPAA Privacy Rule “…is critical to enabling individuals to take ownership of their health and well-being….Unfortunately, based on recent studies and our own enforcement experience, far too often individuals face obstacles to accessing their health information, even from entities required to comply with the HIPAA Privacy Rule. This must change.”

The Fact Sheet summarizes the existing HIPAA rules on the right of individuals to access and receive a copy of their protected health information (PHI). It also reiterates the rules (largely stemming from the Omnibus Rule) regarding the form and format of individual requests and access, responding to requests by individuals for a copy of their PHI to be sent to a designated third party, and fees that may be charged for copies of PHI.

On February 25, 2016, OCR released the second set of FAQs regarding this topic (which is combined with the Fact Sheet and found in the link above).

The Fact Sheet and FAQs are detailed and comprehensive. Providers should review the entirety of the guidance from OCR. A brief summary of notable information from the Fact Sheet and FAQs and our analysis of this guidance are provided below.

ACCESS VS. AUTHORIZATION

The FAQs provide the following new guidance on the distinction between access and authorization:

• Covered entities may require that an individual’s request for a copy of his or her own PHI be in writing.

• When an individual directs the covered entity to send the copy of PHI to another designated person, the request must be made in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.

• Covered entities may require the use of their own forms for these requests for access, provided the form does not create a barrier or unreasonably delay the individual from obtaining access to his or her PHI.

• The FAQs emphasize that covered entities should not use an authorization form for these access requests. The FAQs state: “As explained elsewhere in the guidance, a HIPAA authorization is not required for individuals to request access to their PHI, including to direct a copy to a third party – and because a HIPAA authorization requests more information than is necessary or that may not be relevant for individuals to exercise their access rights, requiring execution of a HIPAA authorization may create impermissible obstacles to the exercise of this right. Where it is unclear to a covered entity, based on the form of a request sent by a third party, whether the
request is an access request initiated by the individual or merely a HIPAA authorization by the individual to disclose PHI to the third party, the entity may clarify with the individual whether the request was a direction from the individual or a request from the third party.”

Our analysis

The distinction between what is a request by a patient for a copy to be provided to a third party (which falls under access right) and a request by a third party based on a patient authorization (which does not fall under the access right) seems very unclear even with the new guidance. The FAQs state: “Where the third party is initiating a request for PHI on its own behalf, with the individual’s HIPAA authorization (or pursuant to another permissible disclosure provision in the Privacy Rule), the access [rules] do not apply. However,… where the third party is forwarding – on behalf and at the direction of the individual – the individual’s access request for a covered entity to direct a copy of the individual’s PHI to the third party, the [access rules] apply.” But when is a third party “initiating” a request versus “forwarding” a request from a patient? The FAQs answer: “Where it is unclear to a covered entity, based on the form of a request sent by a third party, whether the request is an access request initiated by the individual or merely a HIPAA authorization by the individual to disclose PHI to the third party, the entity may clarify with the individual whether the request was a direction from the individual or a request from the third party.” While likely challenging for covered entities to analyze every request from a third party for a patient’s medical record, there is a significant risk for not doing so. On March 1, 2016, at the HIMSS16 conference, Deven McGraw, Deputy Director of Health Information Privacy at OCR, stated that she believes requiring a patient to sign an authorization form to access his or her own information is a potential HIPAA violation on the grounds that it may create an unreasonable barrier to access. This is a much more strict view of this issue than has previously been communicated. Covered entities should be aware of the increased focus on this issue by OCR.

SCOPE, TIMELINESS AND OTHER DETAILS OF ACCESS

Regarding various additional details related to access, the FAQs provide the following guidance:

- A covered entity may not require an individual to come physically to a facility to pick up his or her records, insist that an individual submit a request through a web portal or require an individual to give a reason why he or she is requesting access.


A new round of federal privacy and security audits will target the business associates of healthcare providers, insurers and other HIPAA-covered entities along with the entities themselves, according to the Office for Civil Rights at HHS.

HHS' Office for Civil Rights has started sending out e-mails to obtain and verify contact information for covered entities and business associates of various types for possible inclusion in the pool of potential audit subjects.

The health IT sections of the American Recovery and Reinvestment Act of 2009 added a number of more stringent privacy and security provisions to HIPAA. The law also required that HHS initiate a series of audits to verify compliance with the rules.

Another new provision in the 2009 stimulus law placed the businesses that do data handling, processing and analysis in healthcare on the same legal footing as the hospitals, physicians, insurance companies and claims clearinghouses they work for.

These so-called “business associates” were largely given a pass in the first round of audits in completed in December 2012.

According to a 2013 report by the OCR, two-thirds of the entities audited—including 47 of 59 healthcare providers, 20 out of 35 health plans—lacked complete and accurate risk assessments.

Last week, the office announced a pair of settlement agreements totaling nearly $5.5 million with the Feinstein Institute for Medical Research in New York and North Memorial Health Care in Minnesota to settle possible HIPAA violations. The Memorial Health Care case also involved a business associate, the Chicago-based revenue cycle management firm Accretive Health, according to the OCR, which said the provider and its contractor did not have a HIPAA-required agreement in place.

Getting an audit letter, even if it's only for confirmation of a covered entity's contact information, should serve as notice to healthcare leaders, said Timothy McCrystal, partner and Gershi's co-chair at Ropes & Gray.

“You're in the audit lottery,” McCrystal said. He advises letter recipients to pull out their current HIPAA security risk assessment (which typically produces a work plan) and follow up on open areas. “Now is the time to be spending internal time and resources remediating those issues.
Covered entities must provide an individual with access to all of his or her PHI in the designated record set (DRS), subject to certain limited exceptions (such as psychotherapy notes). Covered entities are not, however, required to create new information, such as explanatory materials or analyses, that does not already exist in the DRS.

Individuals do not have a right to access PHI that is not in a DRS – such as PHI in a peer review file. But the FAQs reiterate that including PHI in a peer review file (or other file outside of a DRS) does not shield the PHI itself.

An individual has the right to access PHI that is maintained by a business associate if the business associate maintains a DRS on behalf of the covered entity. The FAQs also note that if the same PHI that is the subject of an access request is maintained in both the DRS of the covered entity and the business associate, the PHI need only be produced once in response to the request for access.

A covered entity must act on an individual’s request for access no later than 30 calendar days after receipt of the request. If the covered entity is not able to act within this timeframe, the entity may have up to an additional 30 calendar days, as long as it provides the individual – within that initial 30-day period – with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request.

The FAQs note that “these timelines are outer limits, and it is expected that many covered entities should be able to respond to requests for access well before these outer limits are reached.” Additionally, the FAQs state that if it may take close to these outer time limits to fulfill the request, the covered entity “is encouraged to provide the requested information in pieces as it becomes available, if the individual indicates a desire to receive the information in such a manner.”

**Our analysis**

Covered entities should ensure that they can provide access to all PHI in a DRS, not just in the “medical record.” The “medical record” is commonly defined by hospitals in a more limited fashion than HIPAA’s broad definition of PHI in a DRS. Obtaining PHI from a business associate will likely not be necessary in many instances when the business associate only has the same PHI as the covered entity or only has PHI that is not in a DRS. It may be a good exercise for covered entities to determine in advance which business associates will have PHI that does not fall within these categories so that they know which business associates to contact to obtain PHI when needed to respond to a request.

**FEES**

The FAQs reiterate and clarify the following issues related to fees that may be charged in response to a request for access:

- Covered entities may impose a reasonable, cost-based fee to provide an individual with a copy of his or her PHI, or to direct the copy to a designated third party.

- Fees may include only the cost of certain labor, supplies and postage. Labor fees are limited to the reasonable costs associated only with the labor for copying the PHI requested. Labor for copying includes only labor for “creating and delivering the electronic or paper copy” and does not include reviewing the access request, searching for, retrieving and otherwise preparing the information. Individuals may be charged for the costs of supplies for creating the paper copy (e.g., paper, toner) or electronic media (e.g. CD or USB drive); however, a covered entity may not require an individual to purchase portable media as individuals have the right to have their PHI e-mailed or mailed to them upon request. And, the actual cost of postage may be included when the individual requests the information be mailed.

- Covered entities must inform the individual in advance of the approximate fee that may be charged for the copy, including any associated fees that may impact the form, format or manner in which the individual requests to receive the copy.

- Covered entities may (i) use the actual cost, (ii) develop an average standard rate based on schedule of costs for labor or (iii) charge a flat fee provided the flat fee does not exceed $6.50. An average standard rate can be a per page fee only where the request is for a paper copy or the individual asks for the paper to be scanned into an electronic format. The OCR does not consider per page fees for copies of PHI maintained electronically to be reasonable.
• Covered entities may charge patients limited fees for providing copies of PHI but not for access to their PHI. Thus, a covered entity may not charge an individual to access his or her PHI through the View, Download and Transmit functionality of certified EHR technology.

• Coordination with state law in this area is essential. The FAQs reiterate that hospitals must charge the lower of the two rates set by HIPAA and state law. That is, if state law establishes a lower fee for a copy of a medical record then state law applies and HIPAA is preempted; if HIPAA establishes a lower fee then HIPAA applies and state law is preempted. Accordingly, in most cases it will be necessary to calculate the fee both ways to determine which formula yields a lower fee and that fee must be used.

• The fee limitations apply also to requests by an individual for a copy of PHI to be sent to a third party as directed by the individual under the individual’s right of access. But the fee limitations do not apply to requests for PHI from a third party based on a patient authorization.

• A covered entity may not withhold an individual’s PHI on the grounds that the individual has not paid his or her bill for health care services. Further, a covered entity may not apply the fee for a copy of the PHI received from an individual to the individual’s unpaid bill for health care services.

Our analysis

While the interpretation that only labor costs of “copying” the record, when in electronic format, may be included may seems overly restrictive as it does not allow for legitimate labor costs when producing copies of electronic records, OCR has made this interpretation clear and covered entities should ensure that labor costs for producing an electronic copy of PHI do not include costs of searching for, retrieving, and otherwise preparing the copy. Additionally, it is especially important to review state law on medical records fees. Because either HIPAA or state law can apply (whichever is less expensive), covered entities have little choice but to calculate the costs under each formula and then use whichever is lower.

ONC DATA BRIEF

In October 2015, the ONC released Data Brief 30 Trends in Consumer Access and Use of Electronic Health Information. That Data Brief is an interesting look at the metrics of patient access activity, providing national estimates of consumers’ access and use of their electronic health information based upon nationally representative surveys conducted from 2012 to 2014.

Information from the Data Brief shows that individuals utilizing electronic access to their medical records increased significantly – from 28 percent to 38 percent – from 2013 to 2014.

Approximately one-third of individuals who accessed their information electronically downloaded information from their online medical record in 2014, similar to the rate in 2013. In 2014, 33 percent of individuals used their online medical records to share information with at least one other party (e.g., family member, health care provider, someone else involved with their care), which was down from 44 percent in 2013. In both 2013 and 2014, about one in ten individuals used their online medical records to transmit their data to another system, such as a PHR or app.

Related to the concerns expressed by OCR in this area, the Data Brief notes that 27 percent of individuals either didn’t believe they had a right or were unaware of their right to an electronic copy of their medical record.

Human Resources

Colleges Brace for Overtime Overhaul

Wall Street Journal – March 22, 2016

Schools across the country are bracing for a surge in personnel costs as they prepare for the Obama administration’s overhaul to overtime-pay rules.

Under the plan, Obama would increase the threshold under which salaried workers receive overtime pay from $23,660 to $50,440 making about 5 million U.S. workers newly eligible for overtime pay.
While the rule will apply to employers of all kinds, higher-education institutions say their missions and circumstances mean they’ll be hit in ways that other types of employers aren’t. School officials, who say they’re under pressure to keep a lid on tuition, have warned of cuts in student services, degree offerings and labor-intensive research on issues such as climate change and cancer.

The new requirements are creating a clash between two White House priorities: strengthening the middle class by raising pay for many workers and relieving tuition burdens on college students.

Given the administration’s desire to rein in student debt, many colleges question the wisdom of the details in the overtime-pay proposal, saying that doubling the salary threshold is too extreme, for example. “Adding additional financial burdens on higher education institutions does not make good fiscal sense,” Southeast Missouri State University told the Labor Department. The university said the rule could cause schools to curb bonuses and other benefits.

The rule reached its final stages of review last week when the Labor Department sent it to the White House’s Office of Management and Budget. That office will have 90 days to review it, including analyzing the costs and benefits, though that could be extended.

Administration officials say inflation has eroded the value of the existing threshold of $23,660 a year since it was last updated in 2004, leaving too few workers eligible for overtime pay while working more than 40 hours a week.

Universities are busy determining which workers will be affected and what their costs will be if regulators don’t scale back the proposal. Though professors and others who primarily teach are expected to be untouched by the rule under a longtime teaching exemption that still leaves a huge swath of staff.

To afford the cost of compliance, institutions say they’ll likely use a combination of raising salaries, paying overtime, and forbidding some work.

Research universities reliant on postdoctoral associates—academic employees and trainees who have earned Ph.D.s and take on labor-intensive projects to advance their careers—will feel a particular blow, say school officials who fund some of these positions with federal grants that have been stagnant or declining.

“It’s a finite bucket of money in higher education,” said David Blake, chairman of the public-policy group for the College and University Professional Association for Human Resources.

Information Security and Privacy

10 Lessons From FTC Guidance on Data Security

“Not if, but when.” These simple words are enough to keep corporate counsel, compliance officers and IT managers up at night when faced with the reality that their network will at some point be breached. This is no surprise given the spate of corporate breaches and unauthorized network intrusions reported in recent years as well as the costs, reputational harm and investigations and lawsuits that follow in their wake. While there are no silver bullets to stop breaches from occurring, understanding and following legal actions brought by regulatory agencies and heeding security guidance they issue could go a long way in preventing security lapses and unauthorized attacks.

There is no omnibus federal law that prescribes the level of security that companies must use to protect consumer information. Instead, Congress has identified certain categories of sensitive data that warrant regulation, such as health and financial information, and online information collected from children under 13, resulting in the Health Information Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Children’s Online Privacy Protection Act, respectively.

Each of the above laws (and their implementing regulations) to some extent dictates specific data security standards for companies that possess consumer information in these industries. But for the vast number of companies that do not fall within these categories, knowing what standards they are expected to employ to protect consumer information remains an elusive task. Notwithstanding this void, companies that fail to develop a comprehensive data security plan and implement at least some level of minimum security measures to protect consumer information remain vulnerable to attacks, lawsuits and regulatory investigations.
Enter the FTC

Companies that experience a data breach of some sort can expect to hear from the Federal Trade Commission shortly following the breach becoming public. The agency has brought over one hundred privacy and data security cases under its broad jurisdiction authority pursuant to Section 5 of the FTC Act (15 U.S.C. § 45), which empowers it to investigate and halt unfair and deceptive acts and practices in commerce.

The FTC’s privacy enforcement docket has historically involved companies that failed to abide by their posted privacy policies, which the agency claims violated the FTC Act for being a deceptive trade practice. But the FTC has also brought cases against companies that have failed to take adequate precautions to protect consumer information, alleging that such failure was unfair to consumers, since they could not reasonably avoid the harm that may result from such inadequacies.

But therein lies the rub. How can the FTC claim that a company has not adequately protected consumer information if it and Congress have not given industry specific guidance to follow?

Two companies took the FTC to task on this issue by challenging the agency’s authority to bring data security enforcement cases in the absence of clear and prior guidance. Both of these cases have recently reached resolution, with differing, though logical, results.

Last summer, the U.S. Court of Appeals for the Third Circuit upheld a district court’s finding that the FTC does have the authority to review and scrutinize a company’s data security practices under Section 5 of the FTC Act. The FTC sued Wyndham Worldwide Corporation in federal district court in December 2012 for failing to employ reasonable and appropriate protections for consumer information, which resulted in several data breaches and caused “the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers’ accounts, and more than $10.6 million in fraud loss.”

Wyndham moved to dismiss the action by challenging the FTC’s authority to bring claims under Section 5 in the absence of specific and particular data security standards. The district court rejected Wyndham’s motion and the Third Circuit affirmed.

Three months later an FTC administrative law judge ruled against the agency in a case involving a cancer-screening laboratory’s failure to adequately protect sensitive consumer information. The ALJ dismissed the agency’s August 2013 complaint alleging that LabMD failed to employ “reasonable and appropriate” data security for consumer information, which “caused, or is likely to cause substantial injury to consumers.” Like Wyndham, the FTC investigation followed several breaches by LabMD that collectively exposed personal information of approximately 10,000 consumers. The FTC’s complaint alleged that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network, and company documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves.

The complaint concluded that LabMD’s alleged failure to employ such measures amounted to an unfair trade practice under the FTC Act by causing, or being likely to cause, substantial harm to consumers that is not reasonably avoidable by consumers or outweighed by benefits to consumers or competition. The ALJ disagreed, finding that “FTC complaint counsel had failed to carry its burden of proving that LabMD’s alleged failure to employ reasonable data security constitutes an unfair trade practice, because complaint counsel failed to prove that the allegedly unreasonable conduct caused or was likely to cause substantial injury to consumers.” He added, “At best, Complaint Counsel has proven the ‘possibility’ of harm, but not any ‘probability’ or likelihood of harm. Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) [of the FTC Act] requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case.”

This matter is far from over, since the FTC has appealed the decision to the full FTC Commission, which will likely result in the decision being overturned. But the ALJ’s finding does fall in line with a string of cases questioning whether regulatory investigations and class actions are appropriate where no harm resulted from an actual or potential data breach.

While these decisions may appear conflicting, they address very different issues and are in fact mutually exclusive. Wyndham involved actual proven consumer harm whereas LabMD did not. Query whether the Third Circuit and the
lower court would have upheld the FTC’s authority to prosecute inadequate security practices in the absence of provable and discernible harm. The lack of harm was very much the centerpiece issue for the FTC’s ALJ in LabMD. Regardless of the final outcome of these cases, companies that collect and maintain consumer information, particularly sensitive information such as account numbers, must develop and implement sound data security policies and procedures designed to prevent unauthorized breach and intrusion. In the absence of statutory prescriptions to follow, the FTC has published a document that many consider to be a treasure map to the FTC’s secret vault of security expectations.

This document, titled “Start with Security: A Business Guide,” follows a series of FTC workshops and papers involving privacy and data security. It highlights the following 10 practical lessons that can be drawn from over 50 data security cases the agency has brought over the last decade.

1. The FTC urges companies to factor security into every aspect of their business, especially when developing data collection, retention and use policies. Specifically, companies should not collect unneeded personal information, should only retain collected information for as long as needed, and should not use such information for unnecessary purposes.

2. Companies should limit access to personal information to only those employees and vendors who need it.

3. Companies should require persons with access to personal data to use strong and effective passwords and employ encryption devices when the nature of the data warrants stronger protection.

4. Companies should maintain sensitive personal information securely throughout its life cycle, both when in storage and when in transit.

5. They should design networks to separate internal networks containing consumer information from the Internet and employ intrusion detection software to monitor for malicious activity.

6. Given the explosive growth of telecommuters and vendors that remotely access company networks, companies should secure endpoint security by requiring strong passwords and antivirus software on all remote computers and devices.

7. They should employ security sensitivities in all new product development so that engineers and developers consider current and future product uses and scaling. Companies should also consider the platform guidelines on which the products may be run and accessed.

8. Businesses should require third-party service providers to implement appropriate security measures commensurate with the work they will perform and the data to which they will have access and should monitor their activity.

9. They should keep antivirus and third-party software updates current, implement required patches as quickly as possible, and take network vulnerability warnings seriously.

10. Finally, they should apply the same level of sensitivity and diligence to office hardware and paper files as they would electronic files. Specifically, companies should develop and implement security policies for the storage of files and hardware while on and off company premises as well as the destruction of such materials when no longer needed.

Data breaches are the new reality. As hackers continue to develop technological capabilities faster than data protection specialists can, and companies increasingly allow remote access to corporate networks by employees and vendors, it is virtually impossible to protect these networks from unauthorized attacks. But, following the FTC’s guidance outlined above will go a long way in preventing such events from occurring. In the event of a breach and a follow-on FTC inquiry, being able to show that this guidance was followed might stave off a full regulatory investigation and consent agreement. And better yet, following the guidance just makes good business sense.
Another hospital system targeted by possible ransomware cyber-attack

Briker.com – March 30, 2016

MedStar Health, which operates 10 hospitals in Maryland and Washington, D.C., has become the latest hospital system victimized by a cyber-attack on its medical records system.

On Tuesday, March 29, it was reported in the Washington Post that the system was “crippled” by a virus and was forced to shut down its records system on Monday. The newspaper also reported that the attack was causing delays in treatment and diversion of patients. Information that was not confirmed by the hospital system indicated that the attackers were holding the system’s records hostage, demanding 45 bitcoins (approximately $19,000) to release the data. The FBI said it was investigating whether the unknown hackers demanded a ransom to restore systems. The hospital system stated that it had acted quickly to contain the virus and had found no evidence that information had been stolen by the attackers.

Unfortunately, this is at least the third such attack on hospital systems in recent months, following the attacks on Hollywood Presbyterian Medical Center in California and Methodist Hospital in Kentucky.

PwC Report: Cybercrime on the Rise

Corporate Counsel – February 29, 2016

Cybercrimes like data breaches are getting lots of attention these days. But does the average company need to worry about them? The answer is a resounding yes, according to a survey from Pricewaterhouse Cooper, which found that cybercrime has become the second most common type of economic crime.

Of the 6,000 executives across the world who participated in the survey, 38 percent reported that their organizations dealt with economic crime in the last 48 months. Cybercrime increased big time, with 32 percent reporting an incident in the last two years. That’s an 8 percent increase from a year ago. Cybercrime was up and is now the second-most-reported type of economic crime (asset misappropriation is No. 1).

Cybercrimes can cause major losses, according to the report. Of the respondents affected by cybercrime, about 15 percent reported losses of more than $1 million; 2 percent reported losses in excess of $100 million.

Despite this potential for losses, many boards of directors aren’t focusing on cybercrime. Globally, just 27 percent of boards request information about the company’s state of cyber-readiness more than once a year, the report found.

International Students

Final Rule on Improving and Expanding Training Opportunities for F-1 Nonimmigrant Students with STEM Degrees and Cap-Gap Relief for All Eligible F-1 Students


Final rule published in the Federal Register by the Department of Homeland Security amending its F-1 nonimmigrant student visa regulations on optional practical training (OPT) for students with degrees in science, technology, engineering, or mathematics (STEM) from accredited U.S. higher education institutions. The final rule allows F-1 STEM degree students pursuing twelve months of OPT in the United States to extend the training period by 24 months. The rule also includes "Cap-Gap" relief for any F-1 student who has filed a timely H-1B petition and request for change of status. The final rule will go into effect on May 10, 2016.
NOTICE Act Compliance

$1.55 million settlement underscores the importance of executing HIPAA business associate agreements

Bricker - March 16, 2016

In response to the growing trend of hospitals keeping patients in outpatient status with observation services rather than admitting them as inpatients, Congress, last year, passed a law requiring hospitals and critical access hospitals (CAHs) to give each Medicare patient who receives extended observation services notice regarding the patient’s status. Starting August 6, 2016, hospitals are required to inform patients who are hospitalized more than 24 hours that they are outpatients of the hospital or CAH receiving observation services, not hospital inpatients. This requirement comes from the Notice of Observation Treatment and Implication for Care Eligibility (NOTICE) Act that was signed into law on August 6, 2015. Under the law, patients must be informed that they are in observation status, both orally and in writing, no later than 36 hours after the patient begins receiving observation services. The written notice must also explain:

- that the patient is an outpatient receiving observation services and is not an inpatient of the hospital;
- the reason for being in observation status; and
- the implications of such status both for cost-sharing in the hospital (Part B cost-sharing versus Part A) and for subsequent eligibility for coverage in a skilled nursing facility if the patient does not have a qualifying inpatient stay.

The patient, or a person acting on the patient’s behalf, must sign the notice acknowledging receipt. If the patient/representative refuses to sign acknowledging that the notification was given, the hospital staff member who presented the notice must sign the notice, certifying that the notification was given and the time and date that such notification was presented. The staff member’s name and title must also be included.

Centers for Medicare & Medicaid Services (CMS) is expected to issue regulations implementing this new requirement, but, as of the date of this bulletin, those regulations have not yet been issued. However, because the law is self-implementing to be effective one year from enactment, hospitals must comply with this new requirement effective August 6, 2016, even if no regulations have been published by that date. This means that hospitals should be working now to develop the notice that will be given to patients and any policies/procedures needed to ensure that the notice is provided in a timely manner in accordance with the law. Once CMS issues regulations, hospitals may have to revise their notices and/or policies and procedures to the extent that the regulations impose additional requirements.

Risk Management

Protiviti and NC State University ERM Survey Reveals Top Business Risks

Corporate Compliance Insights – March 23, 2016

More organizations are realizing that additional risk management sophistication is warranted given the fast pace at which complex risks are emerging, according to results of the fourth annual joint survey assessing the current risk environment by global consulting firm Protiviti and the Enterprise Risk Management (ERM) Initiative at the North Carolina State University Poole College of Management.

Released today, Executive Perspectives on Top Risks for 2016 (www.protiviti.com/TopRisks) summarizes the concerns of 535 Board members, C-suite and other top-level executives around the world and across industries. In the survey, respondents rate the significance of 27 risk issues for the coming year, spanning three risk categories: macroeconomic, strategic and operational.

Regulatory change and heightened regulatory scrutiny is the number one risk cited by survey respondents for the fourth consecutive year, highlighting its dominance on the minds of Board members and executives worldwide. The majority (60 percent) of respondents believe this risk will continue to have a significant impact on their organizations, indicating business executives remain highly concerned about the effect of the regulatory landscape on their strategic direction.
The Top 10 Risks for 2016

The following are the top 10 risks identified in the annual Board member and executive risk survey, along with the percentages of respondents who identified each risk as having a “significant impact” on their business:

1. Regulatory changes and regulatory scrutiny may heighten, noticeably affecting the manner in which products or services will be produced or delivered (60 percent)

2. Economic conditions in markets currently served may significantly restrict growth opportunities for the organization (60 percent)

3. The organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt its core operations and/or damage its brand (57 percent)

4. The organization’s succession challenges and ability to attract and retain top talent may limit its ability to achieve operational targets (52 percent)

5. Ensuring privacy/identity management and information security/system protection may require significant resources for the organization (53 percent)

6. Rapid speed of disruptive innovations and/or new technologies within the industry may outpace the organization’s ability to compete and/or manage the risk appropriately, without making significant changes to its business model (51 percent)

7. Resistance to change may restrict the organization from making necessary adjustments to the business model and core operations (49 percent)

8. Anticipated volatility in global financial markets and currencies may create significantly challenging issues for the organization to address (50 percent)

9. The organization’s culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect core operations and achievement of strategic objectives (45 percent)

10. Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in the organization’s existing customer base (46 percent)

“The results of our latest survey show that key stakeholders’ expectations regarding the need for greater transparency about the nature and magnitude of organizations’ risks continue to be high,” said Patrick Scott, Protiviti EVP of Industry Groups.

“Pressures from Boards, volatile markets, intense competition, demanding regulatory requirements, new technologies and other dynamic forces are leading to increasing calls for management to design and implement effective risk management capabilities to identify and assess organizations’ key risk exposures, with the goal of reducing them to an acceptable level,” said Jim DeLoach, a managing director with Protiviti.

Two new risks made it onto this year’s top 10 list: the rapid speed of disruptive innovations and/or new technologies within the industry (#6) and anticipated volatility in global financial markets and currencies (#8). These newly identified concerns bumped two former risks off the top 10 list: concern over the ability to manage an unexpected crisis that could impact reputation (#8 in 2015) and the ability to meet performance expectations relative to competitors (#10 in 2015).

“Interestingly, we found Boards of Directors, CEOs and other members of the executive team report differing views of the top risk exposures facing their organizations,” said Dr. Mark Beasley, Deloitte Professor of Enterprise Risk Management and NC State ERM Initiative director. “The level of impact of risk concerns among Board members is noticeably less risky compared to the executive team, who see the outlook for the next 12 months as more risky. These findings suggest there is a strong need for discussion and dialogue between management and the Board to ensure the organization is focused on the right emerging risk exposures.”
Stark Law Compliance

U.S. Supreme Court deals a blow to all payer claims databases

*Bricker* - March 2, 2016

All payer claims databases, which have been set up in 20 states and are seemingly an invaluable and inevitable tool in many payment reform initiatives, were dealt a blow by the U.S. Supreme Court in a March 1, 2016, decision finding them unlawful if run by state law. In a case styled *Gobeille v. Liberty Mutual Insurance Co.*, the Supreme Court found a Vermont law requiring all health plans to report data on paid claims to be pre-empted by federal regulation under ERISA.

Vermont is one of 20 states that has enacted legislation and is operating or implementing all payer claims databases. Vermont’s law required all health plans with Vermont members, or with non-Vermont members who received care in Vermont, to report medical claims data, pharmacy claims data, member eligibility data, provider data and other information. According to federal law, however, ERISA pre-empts “any and all State laws insofar as they may now or hereafter relate to any employee benefit plan.” Courts have upheld this pre-emption so as to assure uniformity in the regulation of health plans and protect plans from being subject to different regulation that may be imposed by any or all of 50 different states. Since ERISA already regulates the reporting, disclosure and record-keeping requirements for plans, the Supreme Court found that Vermont’s law requiring the reporting of claims and eligibility data to be pre-empted by ERISA’s regulation, even if ERISA does not currently require the same type of information gathering Vermont sought.

Spurred by payment reform and the rapidly-increasing size of electronic medical record information available, all payer claims databases have emerged as important tools for plans, providers and states alike. States that have not yet enacted legislation have been considering it. In Ohio, for instance, the governor’s 2016-2017 budget bill as introduced in February 2015 included creation of “the Ohio all-payer health claims database.” The final bill as enacted, however, did not include the language.

The concept of an all-payer claims database is not likely to go away, but its enactment will now have to come from federal law. In fact, in its decision disallowing Vermont’s law, the Supreme Court noted that the Secretary of Labor “may be authorized to require ERISA plans to report data similar to that which Vermont seeks.” When and what that law looks like will depend on elections and congressional developments that will take months, perhaps years, to play out.