The next meeting of the JACC will be held on Wednesday, February 3, 2016 at 10:00 am
Rome Commons Ballroom, Storrs
University of Connecticut & UConn Health
Joint Audit & Compliance Committee Meeting

Meeting Minutes from September 17, 2015

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

The meeting of the Joint Audit and Compliance Committee (JACC) was called to order at 10:03 a.m. by Trustee Nayden.

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

- C.G.S. 1-200(6)[E] – Preliminary drafts or notes that the University has determined the public’s interest in withholding outweighs the public’s 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 or the information contained therein pertaining to or communications privileged by the attorney-client relationship. [1-210(b)(10)]
- C.G.S. 1-200(6)[C] – Matters concerning standards, processes and codes not available to the public the disclosure of which would compromise the security of integrity of an information technology system. [1-210(b)(20)]


The Executive Session ended at 10:50 a.m. and the JACC returned to open session at 10:55 a.m.

There were no public comments.

**Tab 1 – Minutes of the Meeting**

**ON A MOTION** made by Trustee Nayden and seconded by Trustee Cantor the minutes of the May 7, 2015, JACC meeting were approved.
University of Connecticut & UConn Health
Joint Audit & Compliance Committee Meeting

Meeting Minutes from September 17, 2015

TAB 2 – Storrs & UConn Health Significant Compliance Activities
K. Fearney and I. Mauriello provided an update on significant compliance activities.

J. Pufahl updated the committee on the data exposure in the School of Engineering.

A. Cretors and P. McCarthy presented the committee with an update on NCAA Compliance activities as well as various topics impacting the NCAA.

C. Mitchell updated the committee on ICD-10 initiatives at UConn Health. K. Fearney provided an update for the Storrs campus.

Annual Audit and Compliance Plans – Storrs and UConn Health
C. Chiaputti provided the committee with the Storrs and UConn Health FY16 Audit Plans.

K. Fearney provided the committee with the Storrs FY16 Compliance Plan and I. Mauriello the UConn Health FY16 Compliance Plan.

ON A MOTION made by Trustee Kruger and seconded by Director Holt, both the audit and compliance plans were approved by the committee.

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 eight audits and had twelve audits ongoing during this reporting period. OACE completed three special projects.

The JACC accepted eight, as follows:

• Cash Handling,
• Medical Device Security,
• Health Management (HIM) – Patient Record Management JDH UMG,
• UConn Health Electronic Health Record (eHims),
• General University Fee (GUF) Funded Activity – Marching Band,
• Firewall Security,
• NCAA Compliance – Academic Performance, and
• Project Commissioning / Closeout Process.

The Student Health Services Clinical Systems audit was incorrectly posted to the Status of Audit Assignments.

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

Tab 4 – Auditors of Public Accounts
University of Connecticut & UConn Health
Joint Audit & Compliance Committee Meeting

Meeting Minutes from September 17, 2015

Tab 5 – External Engagements

ON A MOTION made by Trustee Nayden and seconded by Trustee Borges, the JACC approved the re-appointment of the accounting firm of McGladrey as independent auditors of UConn 2000 expenditures for FY15.

ON A MOTION made by Trustee Nayden and seconded by Trustee Cantor, the JACC approved the re-appointment of the accounting firm BKD to provide audit services for the year ending June 30, 2015.

Tab 6 – Informational / Educational Items

The committee was provided with the following:

• Compliance Newsletters – Storrs and UConn Health,
• Practical Guidance for Health Care Governing Boards on Compliance Oversight, April 20, 2015, and
• JACC Agenda Forecast.

There being no further business, ON A MOTION made by Trustee Nayden and seconded by Trustee Kruger, the meeting was adjourned at 11:30 a.m.

Respectfully submitted,

Angela Marsh

Angela Marsh
University of Connecticut
&
UConn Health

Joint Audit & Compliance Committee Meeting
SIGNIFICANT COMPLIANCE ACTIVITIES

STORRS

• **Protection of Minors Program** – A Minor Protection Coordinator has been hired and will begin mid-December. Introductory meetings for the program have occurred with union representatives at both UConn Storrs and UConn Health.

• **Policy Development** – the Board of Trustees adopted the Intellectual Property and Commercialization Policy on September 30, 2015.

• **Records and Information Management** – Educational efforts have begun with the College of Agriculture, Health and Natural Resources.

• **Compliance Listserv** – A new communication tool will be launched in early December to share important compliance information with approximately 100 administrative staff throughout the institution. The goal of the listserv is to enhance communications regarding new policies, annual compliance training and other important compliance initiatives with key staff in various departments, schools and colleges.

• **Faculty Consulting Oversight Committee** - The Faculty Consulting Oversight Committee is responsible for monitoring the University’s compliance with the Faculty Consulting Policies and Procedures. The Committee met on November 17th to discuss its annual report to the Board of Trustees and State Legislature.
UConn Health

- **Government Exclusion List Checking** – Monthly exclusion checking of all individuals employed or engaged in work for UConn Health began in September using a vendor. Protocols and processes necessary to address both potential and validated exclusions are being developed by an executive level compliance committee.

- **Overpayment refunds** –
  - Neurology testing billed by ineligible provider
  - Drugs billed with incorrect units / multiple units of administration

- **2015 Annual Compliance and HIPAA training** – launched in mid-October with deadline of mid-January 2016 for completion.

- **Department of Health & Human Services, Office of Inspector General Work Plan** – The 2016 Plan was posted by OIG in early November and has been reviewed by the Compliance Office. Discussions are planned with stakeholders on key components where they have responsibility for oversight of identified risk areas.
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>Dental Record Management</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>axiUm Dental System</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Leave Time Benefits</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Foundation Receipts and Disbursements – FY15</td>
<td>Storrs &amp; UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Student Health Services – Business &amp; Clinical Operations</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Student Health Services Clinical Systems</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>NCAA Compliance – Extra Benefits, and Camps &amp; Clinics</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Leave Time Benefits</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Firewall Security Audit</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>Grants – Cash Management</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Lab Safety</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Bioscience CT Initiative , Phase II – New Hospital</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Emergency Preparedness</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>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>Innovation Partnership Building (IPB)</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Human Subject Incentive Payments</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Stem Cell Audit – FY15</td>
<td>Storrs &amp; UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Transportation &amp; Parking Services</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Correctional Managed Health Care – Pharmacy</td>
<td>UH</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>Clinical Contracts</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><strong>TOTAL AUDITS (24)</strong></td>
<td></td>
<td>(01) Hold</td>
<td>(03)</td>
<td>(12)</td>
<td>(05)</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>Radiology</td>
<td>UH</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SHS Special Project</td>
<td>Storrs</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>TOTAL SPECIAL PROJECTS/CONSULTING (02)</strong></td>
<td></td>
<td>(00)</td>
<td>(00)</td>
<td>(01)</td>
<td>(01)</td>
</tr>
</tbody>
</table>
Open Overdue Items by Functional Area - Based on Original Due Date

- Storrs and Regional Campuses
- UConn Health
High Risk Overdue by Functional Area

Campus and Functional Area

# of Open Overdue High Risk Observations

- Bursar's Office
- Enrollment Services
- Environmental Health and Safety
- Information Technology
- Public Safety
- Public Safety
- Storrs and Regional Campuses
- UConn Health
Implemented

- High: 13
- Medium: 66
- Low: 51

Open OverDue Items by Risk Level

- High: 16
- Low: 50
- Medium: 134
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
University of Connecticut
Joint Audit and Compliance Committee (JACC)
Charter

Purpose

The primary function of the University of Connecticut and University of Connecticut Health Center Joint Audit and Compliance Committee (the “Committee”) is to assist the University of Connecticut Board of Trustees and the University of Connecticut Health Center Board of Directors in fulfilling their oversight responsibilities relating to (a) the integrity of the University’s financial statements and the systems of internal accounting control, (b) the effectiveness of the University’s compliance with performance of the Office of Audit, Compliance & Ethics functions, and the University’s compliance with legal and regulatory requirements, and (c) monitor oversight of the performance of the University’s Office of Audit, Compliance and Ethics (“OACE”). In so doing, it is the responsibility of the Committee to maintain free and open communication among the Committee members, management, the internal auditors, and compliance officers/staff of the University. The Committee shall take all appropriate actions to set the overall University tone for quality financial reporting, sound business risk practices, compliance with all applicable laws and regulations, and ethical behavior.

Membership

The Committee shall consist of seven members all of whom are independent of management and the University. Four members will be selected from the University of Connecticut Board of Trustees (BOT) and three members will be selected from the University of Connecticut Health Center Board of Directors of the University of Connecticut Health Center (UCHC). Members of the Committee shall be considered independent as long as they do not accept any consulting, advisory, or other compensatory fee from the University and are not affiliated persons of the University, its subsidiaries or management.

A majority of Committee members shall be “financially literate” and at least one member shall be a “financial expert.” Financial literacy is defined as being able to read and understand fundamental financial statements. Financial expert means a person who has an understanding of generally accepted accounting principles and financial statements, experience applying such principles, experience preparing or auditing financial statements, experience with internal controls, and an understanding of audit committee functions. In addition, the Committee should also have members with expertise in information technology and compliance.

Roles and Responsibilities

Internal Control

Assure that management is setting the appropriate tone in communicating the importance of internal control and ensuring that all individuals have an understanding of their roles and responsibilities.
responsibilities and also that the systems are in place and being followed to ensure appropriate compliance with internal control procedures.

Evaluate the extent to which internal and external auditors review computer systems and applications, the security of such systems and applications, and the contingency plan for processing critical business functions information in the event of a systems breakdown.

Determine whether internal control recommendations made by internal and external auditors have been implemented by management.

Ensure that internal auditors OACE personnel keep the Joint Audit and Compliance Committee informed about fraud, illegal acts, deficiencies in internal control, and other audit and compliance - related matters.

Financial Reporting

General

Review significant accounting and reporting issues, including recent professional and regulatory pronouncements, and understand their impact on the University’s financial statements.

Review significant financial reporting risks and exposures and the plans to minimize such risks.

Annual Financial Statements

Review the annual financial statements and determine whether they are complete and consistent with the information known to Committee members, and assess whether the financial statements reflect appropriate accounting principles.

Review the annual report before its release and consider whether the information is adequate and consistent with members’ knowledge about the University and its operations.

Compliance with Laws and Regulations

Review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up (including disclosure, repayment and disciplinary actions) on any fraudulent acts or other irregularities.

Periodically obtain updates from management, and the University’s counsel, regarding compliance issues and the overall compliance programs at the University.

Be satisfied that all regulatory compliance matters have been considered in the preparation of the financial statements and other required reports.

Review the findings of any significant compliance or audit examinations by regulatory or other outside agencies and the related organizational response.

The Office of Audit, Compliance and Ethics

Review and ensure that the University of Connecticut has the appropriate structure, staffing and capability to effectively carry out the internal audit, compliance and ethics responsibilities.
Concur in the appointment, replacement, reassignment, or dismissal of the Chief Audit & Compliance Officer.

Review and confirm the structure, priorities and key action plans of the audit, compliance and ethics functions.

**External Auditors**

Appoints, reviews contracts and approves fees of outside auditors.

Establishes policies that ensure management and trustee independence of outside auditors, including “reversing door” employment restrictions and prohibiting external auditors from providing management-consulting services, particularly with respect to information technology and systems.

**Other Responsibilities:**

Ensure that significant audit or compliance findings and recommendations made by the Office of Audit, Compliance & Ethics (OACE) staff, and external auditors, regulators, or other outside agencies, are received, discussed and acted upon in an appropriate and timely manner.

Review with the University’s counsel legal matters that could have a significant impact on the University’s financial statements.

Review and update the Joint Audit and Compliance Committee charter; receive approval of changes from the Board of Trustees.

Regularly update the Board of Trustees and Health Center Board of Directors on Committee activities, any key external audit issues or regulatory reviews, and make appropriate recommendations.

Review and approve the University’s standards of conduct and other compliance-related policy guidance.

**Resources and Authority**

The Committee is empowered to investigate any matter brought to its attention with full access to all books, records, facilities, and personnel of the University and the authority to engage independent counsel and other advisors as it determines necessary to carry out its duties.

**Meetings**

A majority of the members of the Committee will constitute a quorum for the transaction of business. The Committee shall maintain written minutes of its meetings, which will be filed with the Secretaries of the Board of Trustees and Health Center Board of Directors. Reports of all meetings will be made to the Board of Trustees and Board of Directors.

The Committee may request any officer, employee, outside counsel or external auditor to attend a meeting of the Committee or to meet with any members of, or consultants to, the Committee.
As part of its responsibility to foster open communication, the Committee shall provide sufficient opportunity for the internal auditors and compliance staff, and external auditors to meet privately with the Committee. At least annually, or as needed, the Committee shall meet separately with the Chief audit and compliance officer and management.

Adoption of Charter

Approved by the Joint Audit & Compliance Committee on 06/07/12
University of Connecticut
Office of the Audit, Compliance & Ethics
Charter

Authority
Whereas it is a primary function of the University of Connecticut Board of Trustees and University of Connecticut Health Center Board of Directors (hereinafter referred to collectively as the “Board”) to ensure effective control of the administration and operations of the University of Connecticut and University of Connecticut Health Center (hereinafter referred to collectively as the “University”), the Joint Audit and Compliance Committee (JACC) of the Board of Trustees mandates the establishment of the Office of Audit, Compliance and Ethics (OACE). It shall report functionally to the Chair of the JACC and report for administrative purposes only to the President.

These functions are prerogatives of the Chief Audit and Compliance Officer, which may not be infringed upon nor otherwise compromised. The Office of Audit, Compliance and Ethics shall be organized at the discretion of the Chief Audit and Compliance Officer for optimum effectiveness.

The Department OACE will have uninhibited access to all files, documents and related information (except as may be restricted by law).

Purpose
The purpose of OACE is to provide the Board and the President an independent appraisal of the adequacy and the effectiveness of the University’s system of internal administrative and accounting controls and the quality of performance when compared with established standards. Further, it is established to promote a University-wide culture of compliance and ethics. OACE also serves as the centralized office for compliance with Privacy laws and Freedom of Information Act requests. The primary objective is to assist the Board, the President and Senior University Administration in the effective discharge of their responsibilities.

Standards and Independence
The Internal Audit Department audit services function will operate generally within the guidelines of the Institute of Internal Auditors’ (IIA) Professional Practices Framework which includes the Definition of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing or other professional guidance as the Chief Audit and Compliance Officer determines appropriate as mandatory guidance. In addition, where applicable, the Division audit services will follow Generally Accepted Government Auditing Standards (GAGAS).

The Compliance Department compliance functions will operate within the guidelines of the various standards for conduct and professional practice for compliance professionals (e.g., Society for Corporate Compliance and Ethics Code of Professional Ethics) as the Chief Audit and Compliance Officer determines appropriate.

Department OACE staff will be members of appropriate professional associations and will participate in continuing education to remain current with best practices and emerging issues in the areas of audit, compliance and ethics.

Department OACE staff will be independent in fact and appearance by upholding the principles of integrity, objectivity, confidentiality and competency. Staff will be independent of the activities or

Commented [GD1]: These paragraphs were moved from the end of the charter to the front since they relate to the authority of OACE.

Commented [GD2]: Recommend removing these responsibilities. While we may continue to support these functions, ideally Privacy and FOIA should report to an operational entity within the University, not to OACE. These functions are not compatible with our role as an independent oversight activity. Neither of these roles is included in the JACC charter.

Commented [GD3]: We do not comply with all the guidelines of the IIA and probably do not want to. This wording allows us flexibility in our operating standards.

Commented [GD4]: I would like to move toward referring to internal audit and compliance as “services” rather than departments. We have already moved somewhat in this direction, Cheryl is the Director of Audit Services.
operations they review, they will not engage in any activity which would impair their independence of judgment, and they shall be independent of any other influence or control of any kind.

**Scope and Responsibility**

In consultation with the JACC, the Chief Audit and Compliance Officer shall plan, implement, report upon, supervise and be responsible for all internal auditing activities, consulting services, compliance activities, and associated personnel within the framework of this Charter. These functions are prerogatives of the Chief Audit and Compliance Officer, which may not be infringed upon nor otherwise compromised. The Office of Audit, Compliance and Ethics shall be organized at the discretion of the Chief Audit and Compliance Officer for optimum effectiveness. The Department will have uninhibited access to all files, documents and related information (except as may be restricted by law).

The Office of Audit, Compliance and Ethics (OACE) will fulfill its responsibility to the Board and the President by:

- Developing annual audit and compliance activity plans based on an on-going risk analysis which includes consideration of the University’s goals and objectives and the concerns of management and the Board.
- Providing audit and compliance coverage that consistently meets the needs and expectations of management.
- Following up on identified weaknesses, findings and recommendations from previous audit work and compliance reviews.
- Participating in a program of quality assurance designed to ensure the increasing professionalism of the department of OACE and the standard of the work performed.
- Performing consulting services including advisory and related service activities, the nature and scope of which are agreed upon and which are intended to add value and improve the University’s governance, risk management, and control processes without assuming management responsibility. Examples include counsel, advice, facilitation, training, and committee service.
- Promoting awareness of the University’s Code of Conduct, compliance risk, and the objectives of compliance activities through communicating with and educating the University community.
- Developing effective ways to mitigate compliance risk through collaboration with the University community and the implementation of appropriate monitoring plans.
- Acting as a liaison with the State of Connecticut Office of State Ethics and State Auditors of Public Accounts.

The scope of audit and compliance activities will include all controls, reports and operations of the University. OACE will examine and evaluate the following:

- The reliability and integrity of financial and operating information and the means used to identify, measure, classify and report information.
- The systems established to ensure compliance with policies, plans, procedures, laws and regulations that could have a significant impact on the University.
- The means of safeguarding assets and verifying their existence.
- The economy and the efficiency with which resources are employed.
- The extent to which the operations and programs of the University are consistent with its objectives and goals.
The extent to which information technology governance sustains and supports the University’s strategies and objectives.

The ethics objectives and activities of the University.

The potential for fraud and the management of fraud risk.

The Department, OACE, will help ensure that the University:

- Develops and implements effective training programs to ensure that employees are aware of, adhere to, and report potential violations of laws, regulations and policies and procedures;
- Investigates potential violations of laws, regulations, and policies;
- Establishes and publicizes a confidential safe harbor reporting mechanism to allow University employees and agents to report or seek guidance regarding potential or actual criminal or other non-compliant conduct without fear of retaliation; and, to receive and direct compliance issues for investigation and resolution;
- Develops innovative and effective ways to collaborate with the University community to mitigate compliance risk.

**Reporting Results**

The results of audit engagements and significant compliance assessments, the conclusions formed, and the recommendations made, are promptly reported to the appropriate personnel at the University. Significant issues are shared with the JACC and senior University administration and, as appropriate, the Executive Risk Management and Compliance Committees. OACE will report to the JACC periodically on the status of management’s corrective actions on reported deficient conditions.

Approved by the Joint Audit & Compliance Committee on 08/09/12

Commented [GD5]: I revised this to reflect the Federal Sentencing Guidelines terminology.

Commented [GD6]: I added this to provide for our reporting relationships.
UConn Health
Executive Risk Management and Compliance Committee
Charter

Role
The UConn Health Executive Risk Management and Compliance Committee (Committee) is appointed to provide direction and guidance to the UConn Health 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 UConn Health’s overall risk management program, focusing on UConn Health’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:

- Executive Vice President of Health Affairs (Chairman);
- Vice President for Research;
- Chief Administrative Officer;
- Chief Executive Officer, John Dempsey Hospital;
- Dean, School of Medicine;
- Dean, School of Dental medicine;
- Assistant Attorney General (non-voting);
- Senior Counsel (Counsel) (non-voting);
- Chief Information Officer;
- Vice President for Ambulatory Care;
- Chief Financial Officer; and
- Chief Audit and Compliance Officer (Executive Secretary to the Committee) (non-voting).

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 UConn Health 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 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 Health faculty and staff.
UConn Health
Executive Risk Management and Compliance Committee
Charter

(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 UConn Health managers to help ensure institution-wide compliance with relevant state and federal laws and to provide a safe working environment for the UConn Health community.
(4) Review and approve the role, responsibilities, and structure of the UConn Health health/safety, public safety, and compliance committees.
(5) Review and approve the designation of specific UConn Health health/safety, public safety, and compliance coordinators.
(6) Identify and assess health/safety, public safety, and compliance risks at UConn Health 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 significant identified risks, activities, and findings.
(12) Provide a forum for communication among the various units and programs within UConn Health for issues relevant to health/safety, public safety, and compliance.
(13) Perform any other activities consistent with this Charter and University, Schools, Hospital and Medical Staff 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
### 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>FY2015 engagement is underway.</td>
</tr>
<tr>
<td>RSM US LLP (RSM), formerly McGladrey LLP</td>
<td>Storrs, Regionals &amp; UConn Health</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.</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>FY2015 fieldwork is complete and BKD will present the draft report to the JACC at their December 1, 2015 meeting.</td>
</tr>
</tbody>
</table>
University of Connecticut
&
UConn Health

Joint Audit & Compliance Committee Meeting
### 2016 JACC Meeting Dates

<table>
<thead>
<tr>
<th></th>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wednesday, February 3, 2016</td>
<td>10:00 am – 12:00 pm</td>
<td>Rome Commons Ballroom, Storrs</td>
</tr>
<tr>
<td>2</td>
<td>Tuesday, May 17, 2016</td>
<td>10:00 am – 12:00 pm</td>
<td>Rome Commons Ballroom, Storrs</td>
</tr>
<tr>
<td>3</td>
<td>Wednesday, September 21, 2016</td>
<td>10:00 am – 12:00 pm</td>
<td>Rome Commons Ballroom, Storrs</td>
</tr>
<tr>
<td>4</td>
<td>Wednesday, December 14, 2016</td>
<td>10:00 am – 12:00 pm</td>
<td>Rome Commons Ballroom, Storrs</td>
</tr>
</tbody>
</table>
University of Connecticut & UConn Health

Joint Audit & Compliance Committee Meeting
Intellectual Property and Commercialization

The University encourages the development and commercialization of intellectual property invented, created and developed by faculty, students and staff. Intellectual property generally consists of patents, copyrights, trademarks and trade secrets. This policy sets out the University’s policies with respect to such intellectual property, including its ownership, protection and commercialization.

No policy of this nature can cover every possible scenario but it seeks to provide clarity on intellectual property and commercialization issues. The Office of the Vice President for Research (“OVPR”) is the entity primarily responsible for implementing and interpreting this policy, and is ready to work with faculty, staff and students to explain these policies and make determinations in specific cases.

This policy applies to faculty, staff and students at all University Campuses. Please review the full policy at http://policy.uconn.edu/?p=348.

Policy on Employment and Contracting for Service of Relatives

The employment or contracting for service of relatives in the same department or area of an organization may cause conflicts and serve as the basis for complaints concerning disparate treatment and favoritism as well as violations of the state’s Ethics statute.

The Policy on Employment and Contracting for Service of Relatives exists to protect against such conflicts and complaints and to provide for the ethical and legally consistent treatment of individuals with relatives seeking employment or who are employed by the University.

Please review the full policy at http://policy.uconn.edu/?p=357. For questions, contact the Office of Audit, Compliance & Ethics at (860) 486-4526 or the Office of Faculty and Staff Labor Relations at (860) 486-5684.

Reporting Compliance Concerns

The University’s REPORTLINE allows the University community an opportunity to report unethical or illegal activity any time of the day or night by calling a toll-free number at 1 (888) 685-2637.

Learn more about the REPORTLINE and additional reporting options at: http://audit.uconn.edu/reportline/.

The Office of Audit, Compliance & Ethics is available for assistance with questions on any University Policy.

The “Compliance Courier” is a quarterly newsletter issued by the Office of Audit, Compliance & Ethics. Each newsletter will provide updates on important compliance issues. For questions or concerns or to suggest future articles, please contact Kimberly Fearney at (860) 486-6195 or Kim.Fearney@uconn.edu.
Happy Holidays!

Now, what do I do about gifts?

Holiday Gift F.A.Q.s

Please use the following to assist you regarding the giving and receiving of gifts during the holidays:

**Q:** A vendor that frequently does business with the University just sent a large fruit basket to our office as a holiday gift. May we accept it or do we need to send it back?

**A:** A fruit or gift basket (valued at more than $10), while not acceptable if given to one person alone, may be accepted on behalf of an entire department or office if the per-person cost is less than $10.

**Q:** I was just invited by one of our vendors to their holiday party. May I attend?

**A:** Attendance at a vendor’s holiday party may be permissible, as long as employees are mindful that gifts of food and beverage must total less than $50 in a calendar year and items given as gifts from a vendor must total less than $10 in value with an annual total less than $50.

**Q:** May I spend $250 to pay for a holiday luncheon for my staff.

**A:** Yes, provided that the benefit for each subordinate is not more than $99.00.

**Q:** May my coworkers and I pool our money to give our supervisor a gift certificate worth $150?

**A:** No. Gifts from subordinated to supervisors cannot exceed $99.99. Pooling above that limit is not permissible. (Except when the “major life event” gift exception may be used. Holiday gifts do not fall within this exception.

**Q:** If I receive a gift from a vendor outside the permissible limits, may I donate it to charity?

**A:** Yes, as long as you do not accept any tax credit for donating the gift. It is suggested that you document the charitable donation. If the gift is not practical to donate, you may return it to the vendor or bring it to the office to share (following the guidance in the first F.A.Q above).

Emergency Closing Policy

Winter is right around the corner... Are you familiar with the Emergency Closing Policy? There have been some changes. Please visit [http://policy.uconn.edu/?p=348](http://policy.uconn.edu/?p=348) for full details.

Records Management Initiative

Are you frustrated with the overwhelming amount of records and other files in your office? Did you know that you may not have to keep everything? The Office of Audit, Compliance & Ethics offers records management support. We can help you to navigate State and University record policies and procedures and work with you to build upon best practices. Together, we can free up some much needed space and reduce risks associated with storing sensitive information.

Contact Laurie Neal at 860-486-4805 for more information.
OCR is responsible for enforcing Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act (ADA) and Section 1557 of the Patient Protection and Affordable Care Act (ACA). Together, these Federal laws require hospitals, health care providers, clinics, medical practices and other entities who receive Federal financial assistance to provide services to persons with disabilities in a non-discriminatory manner. The services or aids that must be provided to ensure effective communication will depend on the abilities of the individual who is deaf or hard of hearing, the primary method used by the individual to communicate and the complexity and nature of the information being conveyed. Failure to ensure effective communication in such health care settings may lead to misinformation, inappropriate diagnosis and/or delayed or improper medical treatments.

UConn Health community members must obey Federal and state laws against discrimination. You must treat all members of the UConn Health community in a fair and equal manner. This means that UConn Health values diversity, assures equal access to all services, gives assistance with interpretation or translation services as necessary, and provides proper accommodations for any disabilities. For additional information on effective communication resources for health providers, please see the following resources:

- For Persons who are Deaf or Hard of Hearing: [http://www.hhs.gov/ocr/civilrights/resources/specialtopics/hospitalcommunication/edisability.html](http://www.hhs.gov/ocr/civilrights/resources/specialtopics/hospitalcommunication/edisability.html)
- For Persons with limited English proficiency: [http://www.hhs.gov/ocr/civilrights/resources/specialtopics/hospitalcommunication/lep.html](http://www.hhs.gov/ocr/civilrights/resources/specialtopics/hospitalcommunication/lep.html)
- From other HHS Agencies: [http://www.hhs.gov/ocr/civilrights/resources/specialtopics/hospitalcommunication/ecehhsprogandres.html](http://www.hhs.gov/ocr/civilrights/resources/specialtopics/hospitalcommunication/ecehhsprogandres.html)
- Disability and LEP Compliance Activities: [http://www.hhs.gov/ocr/civilrights/resources/specialtopics/hospitalcommunication/heccomplicanceactivities.html](http://www.hhs.gov/ocr/civilrights/resources/specialtopics/hospitalcommunication/heccomplicanceactivities.html)

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

---

**2015 Compliance Training is Underway!**

Mandatory Compliance annual education courses are now available online. Compliance and ethics education provides a foundation for understanding the many laws that govern our institution and applying pertinent regulations in our day to day work. Employees regularly deal with situations that have compliance or ethics implications and sometimes are faced with more serious concerns. Compliance knowledge and education are the first step toward ensuring compliant processes and making sound, ethical decisions.

To complete your assigned training, access the Saba Online Learning Center and following these steps:

1. Log in using your UConn Health Domain login name and password.
2. View “Current Enrollments” on the right side of the page for a listing of all assigned courses.
3. Click “Launch Now” to begin a course.
4. Once you have completed a course click the “Home” tab to view additional course assignments.

**Compliance education must be completed no later than January 21, 2016.**

For training questions please contact Ginny Pack at 860-679-1280 or pack@uchc.edu or Melanie O’Connor at 860-679-4180 or moconnor@uchc.edu

For Saba technical issues, please contact Chris Desjardins at 860-679-7577 or cdesjardins@uchc.edu or the UConn Health IT Helpdesk at 860-679-4400.
UConn Health Obligations When Dealing With a Reported Breach as Defined Under HIPAA

UConn Health is obligated as a covered entity under the HIPAA Privacy and Security Rules to address reported breaches, based on a risk assessment of at least the following factors: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated.1

UConn Health must provide the required notifications to patients and or the government if the breach involved unsecured protected health information. Unsecured protected health information is defined as protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

Additionally by law, notice to affected parties, should a reportable breach be determined must be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved.2

UConn Health also has the burden of proof to demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach and to maintain documentation of the evaluation. This documentation must include the risk assessment noted above either showing that there was a low probability that the Protected Health Information had been compromised or that the impermissible use or disclosure fell within one of the other exceptions in the definition of breach.

The HITECH Rule also established four categories of violations that reflect increasing levels of culpability and four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation, with a maximum penalty amount of $1.5 million annually for all violations of an identical provision. The $1.5 million is not a comprehensive maximum fine for a given category/year, but rather a maximum for all identical violations. The maximum fine is ultimately at the discretion of HHS and is dependent on how many different kinds of violations are found upon review by the Office of Civil Rights.

Violation Category—Section 1176(a)(1)

<table>
<thead>
<tr>
<th>VIOLATION</th>
<th>Each Violation</th>
<th>All such violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect—Corrected</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

1 45 CFR § 164.402
2 HITECH Sec. 13402 (d) (1)

For questions about HIPAA breaches please contact the Privacy Office at 860-679-4180 or email at privacyoffice@uchc.edu

REPORTLINE
1-888-685-2637
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:

- Athletics
- Information Security / Privacy
- Legal
- Research

Athletics

Lawsuit Accuses UConn Coach of Bullying and Allowing Hazing

*Connecticut Law Tribune* – September 8, 2015

A former University of Connecticut women's hockey player has sued her former coach, alleging that he allowed the student to be hazed by the older players and created a hostile environment that caused her to become depressed.

The lawsuit claims Shannon Godin was the subject of emotional distress and negligence at the hands of her coach during her freshman year. Actually, she claims, the poor treatment started before her arrival at UConn in the fall of 2014.

In late January 2014, while Godin was still in high school in Ontario, Canada, UConn Coach Christoper MacKenzie called Godin's parents to tell them he had seen video of Godin's latest game and that she played "terribly," according to the lawsuit. He went on to tell the Godins that she "was not going to be able to keep up, that she would not fit in, that she would lose her scholarship, that she would hate UConn, and that she would hate coming to the rink."

According to the lawsuit, he then called Godin and told her the same. Godin and her parents explained that she did not play well because it was suspected that she had mononucleosis, which was later confirmed.

In August 2014, Godin arrived in Storrs and she played her first game in September. However, she did not play for the next 10 games, allegedly because MacKenzie did not like her.

What's more, the lawsuit alleges, MacKenzie knew about and allowed a culture of hazing to exist within the team.

"Defendant MacKenzie's mistreatment of Shannon cause her to suffer severe emotional distress which was compounded by defendant MacKenzie allowing the senior members on the team to bully and haze Shannon and force her to a 'Rookie Night' where she was forced to drink alcohol and wear sexually inappropriate and degrading clothing," according to the lawsuit, filed by her attorney, James F. Sullivan, of Howard, Kohn, Sprague & FitzGerald in Hartford. "The senior members forced the freshman to drink alcohol on other occasions until they puked and/or passed out."

Godin claims she was hospitalized for binge drinking on Nov. 7, 2015, after being "egged on" by the seniors to keep drinking. According to the lawsuit, MacKenzie was well aware of the "culture of drinking" on the team.

Even before the lawsuit was filed, UConn said its Office of Community Standards conducted an investigation after receiving a complaint this past spring about "hazing-like activities" by the women's hockey team. "The activities included excessive drinking and participation in potentially embarrassing activities," according to Stephanie Reitz, a UConn spokeswoman. "The Office of Community Standards further found that aside from this one event, there was no indication that the upperclassmen were attempting to intimidate others during the year or otherwise had any expectation that members of the team engage in drinking alcohol."

That investigation also found that none of the coaches "endorsed, encouraged or had prior knowledge of Rookie Night," Reitz said.

Additionally, the lawsuit alleges MacKenzie, who is entering his third season at UConn, would talk about his "European-style underwear," which "sickened and disgusted" Godin.
After her first winter break, Godin opted to return to Connecticut and try and do better in the spring semester. According to the lawsuit, she improved her grades, played in 15 games for the team and drank no alcohol. However, in March, MacKenzie told Godin that he would not be renewing her scholarship.

The events of Godin's first year "traumatized" her, according to the lawsuit. "The prospect of returning to UConn makes her cry as does the mention of defendant MacKenzie," according to the lawsuit. "She used to love hockey and now she has no interest in playing. She has lost her confidence in herself."

The university has a campus wide anti-hazing policy. "Hazing is defined as an act which endangers the mental or physical health or safety of a student, or which destroys or removes public or private property for the purpose of initiation, admission into, affiliation with, or as a condition for continued membership in a group or organization," according to the policy.

The university's athletics department had no comment on the lawsuit and referred inquiries to the university.

This is the only sports-related hazing complaint UConn is currently facing, according to Reitz, though the university has dealt with several hazing incidents within the Greek life on campus in the past several years.

"The Division of Athletics has reviewed and discussed the critical issue of hazing and the conduct responsibilities of student-athletes with every returning fall sports team and will continue this practice with all intercollegiate teams," according to Reitz. "In addition, the Division of Athletics is bringing in an outside consultant to conduct training related to hazing. This training will be provided to all of the university's student-athletes, not just those members of the women's hockey team."

Information Security / Privacy

Another Network Outage at Rutgers Leads to Frustration Among Professors and Students

*Chronicle of Higher Education* – September 30, 2015

When a cyberattack brought down Rutgers University’s computer network on Monday morning, Melissa Aronczyk found out via a text from the IT department.

An assistant professor of journalism and media studies, Ms. Aronczyk wasn’t on the New Jersey campus during the outage. But she knew that her students, who use the university’s network to complete their assignments and communicate with their professors, couldn’t get access to their work.

The attack, which started at about 10 a.m. and lasted into the afternoon, is the fourth to hit the university since November 2014. After last year’s attacks, Rutgers spent $3 million to tighten its security — which is one of the reasons the institution raised tuition and fees 2.3 percent this year, according to NJ.com.

"My first thought was, ‘Not again,’” Ms. Aronczyk said, "especially after the school spent so much money over the summer to try to make our system more robust."

After she received the text from IT, Ms. Aronczyk read about the hacker who claimed responsibility for the attacks. Known as Exfocus, the hacker was also allegedly behind attacks last spring.

When Ms. Aronczyk checked her Twitter feed, her students seemed frustrated. They thought Rutgers had taken care of the problem.

Since the attacks began, someone claiming to be Exfocus has spoken out over the Internet, and even has a Twitter account. "This is the third time I have launched DDoS attacks against Rutgers," Exfocus wrote in a post on Pastebin during an attack in April. "Every single time, the Rutgers infrastructure crumpled like a tin can under the heel of my boot."

All of the attacks are classified as distributed denial-of-service attacks. That’s when a hacker takes control of a network of computers, and then uses those computers to flood a network with traffic.

"DDoS attacks tend to be personally motivated," said Kim Milford, executive director of the Research and Education Networking Information Sharing and Analysis Center at Indiana University at Bloomington. "You rarely have to worry that the data is breached. It’s just a really big annoyance."
In an interview this year with the e-commerce blogger Dimitry Apollonsky, Exfocus said he or she was being paid with Bitcoin by someone with a grudge against the university. And according to E.J. Miranda, a Rutgers spokesman, no data have been compromised by the attacks.

The Federal Bureau of Investigation is helping state and local authorities investigate the attacks. Mr. Miranda declined to comment on the FBI’s involvement in the latest one, saying only that the law-enforcement investigation is continuing.

The attacks shut down Rutgers’s access to the Internet as well as to Sakai and eCollege, two systems students use to connect to homework and examinations, the International Business Times reports.

A Short Shutdown

The Rutgers network stabilized by mid-afternoon on Monday, making the shutdown one of the shortest of the last few months. An attack this past spring, which took place during exams, lasted days.

During the spring attack, Ms. Aronczyk created a separate Gmail account to communicate with her students and to administer her final exam. She programmed her email account to send out the final-exam questions whenever students sent her an email, in case they weren’t able to see them through the Rutgers network.

"We bypassed the Sakai system entirely," she said. She is considering creating a course website separate from the Rutgers network, in case of another attack.

Denial-of-service attacks are difficult to prevent, said Ms. Milford. "There is no one-size-fits-all solution for this sort of thing." During the Rutgers incident, she said, everything was interrupted: Access to the Internet, email, and class resources were all compromised, "which is pretty massive when you’re trying to teach and you can’t get to the resources."

But even if universities continue to see such attacks, Ms. Milford doesn’t think that the consequences will get much worse.

She added that her center's technical-advisory group plans to meet with institutions that have suffered denial-of-service attacks recently, to see if they can come up with new solutions collaboratively.

Boston Children’s CIO Talks DDoS Threats, Lessons Learned

HCCA Regional Conference – September 11, 2015

At the Health Care Compliance Association’s regional conference in Boston, Dr. Daniel Nigrin, Boston Children’s Hospital (BCH) Senior Vice President and CIO, went into great detail about the distributed denial of service (DDoS) attacks the hospital experienced in 2014. Though no BCH patient data was ever accessed, the organization had to shut down some of its Web pages and some patients and medical personnel were unable to access online accounts, including email.

A group self-styled “Anonymous” posted details of the BCH external website, such as its IP address and web server infrastructure information, in response to the hospital's diagnosis and treatment of a 15-year-old girl removed from her parent's care by the Commonwealth of Massachusetts. Anonymous began DDoS attacks that initially the hospital was able to address. However, the attacks ramped up to approximately 40 times the normal traffic and BCH had to bring in a third-party provider to help address the traffic. Nigrin said “If there was any lesson learned, it was that we need to take these potential threats seriously and I’m thankful for the fact that we did.”
“After [the early attacks], we went through what I called “cat and mouse” changes where we would make network changes and they would follow with a new DDoS tactic. This meant that they could tell we were adjusting to new strategies and they would accommodate those modifications. We were fearful that more was coming and it did.

“There was a massive uptick in DDoS volume from the Anonymous hackers on the Friday before the 2014 Boston Marathon. As a result, Nigrin said Boston Children’s engaged a third party vendor to assist with the attacks because it was no longer able to accommodate the volume of traffic. “Without their assistance in filtering traffic, we would have been paralyzed,” he said.

But the attacks weren’t limited to DDoS; there were direct penetration attacks on exposed ports and web sites and a barrage of malware-infected email. In response, the hospital took down all externally facing sites and shut down the email system for 24 hours while reinforcing employee education on phishing attacks.

The ultimate solution came from Anonymous itself. As Anonymous Twitter activity showed threatening messages from other Anonymous accounts, the @YourAnonNews account tweeted “To all the ‘Anons’ attacking the CHILDREN’s HOSPITAL in the name of Anonymous – IT IS A HOSPITAL: STOP IT.” After that, the DDoS and other attacks slowly began to dissipate.

Lessons learned

Nigrin said both he and the organization have quite a few takeaways. “[Now] I don’t think that because we’re a healthcare organization, we’re above or immune to these attacks,” he said. Here are a few areas of focus following the attacks:

DDoS counter measures – Nigrin explained that having the infrastructure and planning in place to deal with these types of threats it is important.

Inventory – Knowing which systems depend on internet access and having contingency plans is also crucial. Because the Boston Children’s EHR system is locally hosted, it remained up and running without the internet. But it still had to explain to staff why they couldn’t send prescriptions to pharmacies without email, which Nigrin said was tricky.

Importance of email – In the event the internet is down, the organization needs to have other communication forms as well, such as secure SMS.

New security initiatives – Nothing drives new security projects like an incident, so may as well take advantage of the opportunity, right?

“There were some items that our security team had been pushing for years, such as web proxies. Even if clinical staff and researchers were concerned about the burden, that’s too bad. We implemented 3-4 new security measures in the span of about 48 hours. Don’t wait until you’re in the middle of a fire drill to push these initiatives through, because they will pay off in the end.”

Securing teleconference meetings – Nigrin said to leave no stone unturned, as hackers can plug into insecure teleconferences if the password is included in the meeting invite itself. BCH had the uncomfortable experience of discovering that Anonymous hackers were listening in to their teleconferences.

Signal v. noise – At various points over the few weeks of attacks, Nigrin said that it became hard to separate the events that really were important from the ones that were mainly the result of heightened sensitivity from the incident.

Rehearse Now for Cyberattacks and Be Ready for the Real Thing

*Corporate Counsel* – September 1, 2015

Playacting isn’t just for the human resources department anymore. Diane Reynolds of Taft Stettinius & Hollister suggests rehearsing responses to potential data attacks. “Hacking used to be the domain of college-aged geeks, but those days are past,” she says. “Cyber criminals across the globe are concocting new ways to penetrate the security of organizations, to wreak havoc on data and steal everything from intellectual property to customer information.”

Compounding the issue is the growing prevalence of the Internet of Things. Estimates say that by 2020 between 26 billion and 50 billion devices will be embedded. Reynolds warns that the way IoT technology stores data on the cloud
can be problematic for privacy. Indeed, a study by Hewlett-Packard Co. predicts that 70 percent of the most common IoT devices contain vulnerabilities, such as password security and encryption flaws, says Reynolds.

She suggests that aside from theatrics, organizations study data, forensics and regularly refresh their strategies, make cybercrime a priority at board level and stay current on the latest hacking trends, that is, until the machines can do it themselves.

Legal

University of Nebraska at Kearney to Pay $140,000 in Therapy-Dog Lawsuit

The University of Nebraska at Kearney will pay $140,000 and change its policies to settle a lawsuit, brought by the U.S. Justice Department, alleging that it violated federal law by not allowing students living in university housing to keep assistance animals. Under the new policy, the Associated Press reports, students will be able to apply for “reasonable accommodations,” and may require a doctor’s note.

The settlement stems from the case of a former student, Brittany Hamilton, who said the university did not allow her to keep in university housing her dog Butch, whom she said helped her deal with anxiety and depression. The Justice Department argued that the denial was a violation of the Fair Housing Act. A federal judge ruled for the student in 2013.

The university insists it did not break the law. The campus’s chancellor, Douglas A. Kristensen, told the AP the settlement would allow the university to avoid a trial.

Research

Drastic Changes Proposed for Clinical Research Rules

The U.S. Department of Health and Human Services (“HHS”) and fifteen other Federal Departments and Agencies have announced a proposal to update the Federal Policy for the Protection of Human Subjects known as the “Common Rule,” originally promulgated in 1991. A Notice of Proposed Rulemaking (“NPRM”), published on September 2, 2015, seeks comments on the proposal, which includes some dramatic changes for researchers. According to HHS, the NPRM is intended to strengthen protections for human subjects while at the same time facilitating important research. Additionally, the changes recognize that the volume and landscape of research involving human subjects has changed considerably since 1991, including increased use of sophisticated analytic techniques for use with human biospecimens and the growing use of electronic health data and other digital records to enable very large data sets to be analyzed and combined in novel ways. Here are some highlights:

1) Informed Consent Process Updates. The NPRM proposes to improve the informed consent process by eliminating unduly long consent forms that bury important information. Additionally, there is a proposal for increasing transparency by requiring a one-time, public posting of consent forms.

2) Restrictions on the Use of Stored Biospecimens. HHS believes that research participants prefer to be asked for their consent before their biospecimens are used for research. Accordingly, the NPRM proposes to require informed consent for the use of stored biospecimens for secondary research (for example, leftover blood or tissue samples), even if the samples will be de-identified. The consent would be obtained by means of broad consent (i.e., consent for future, unspecified research studies) to the storage and eventual research use of leftover biospecimens.

3) New IRB Review Requirements. The NPRM proposes to make changes to the IRB review process, so that the level of IRB review is proportional to the level of risk presented by a particular study. Additionally, HHS proposes excluding from IRB review certain categories of activities that should be deemed not to be research, are inherently low risk, or where protections similar to those usually provided by IRB review are separately mandated.
4) **New Exemption Categories.** The NPRM proposes to add new categories of exempt research. Additionally, HHS proposes the creation of a web-based decision tool for determining exempt status. Use of the tool by investigators would be viewed as an appropriate determination of exempt status, in contrast to requiring an IRB to make the exemption determination, which is the current best practice.

New exemption categories would include:

- research involving benign interventions with adult subjects;
- research involving educational tests, surveys, interviews or observations of public behavior when sensitive information may be collected, provided that data security and information privacy protections policies are followed;
- secondary research use of identifiable private information originally collected as part of a non-research activity, where notice of such possible use was given; and
- storing or maintaining biospecimens and identifiable private information for future, unspecified secondary research studies, or conducting such studies, when a broad consent template to be promulgated by the Secretary of HHS is used, information and biospecimen privacy safeguards are followed, and limited IRB approval of the consent process used is obtained.

5) **Limited Availability of Consent Waiver for Secondary Research.** The NPRM proposes waiver of consent for research involving biospecimens (regardless of identifiability) will occur only changing the conditions and requirements for waiver or alteration of consent so that in very rare circumstances.

6) **Cooperative IRB Review Requirement.** The NPRM includes a mandate that U.S. institutions engaged in cooperative research rely on a single IRB.

7) **Elimination of the Continuing Review Requirement for Certain Studies.** The NPRM proposes eliminating the continuing IRB review requirement for studies that undergo expedited review and for studies that have completed study interventions and are merely analyzing data or involve only observational follow-up in conjunction with standard clinical care.

8) **Expanded Scope of Common Rule Applicability.** Currently, the Common Rule applies to federally-funded human subject research. The NPRM proposes extending the scope of the rule to cover all clinical trials, regardless of funding source, conducted at a U.S. institution that receives federal funding for non-exempt human subjects research.

Comments on the NPRM must be received within 90 days following publication of the NPRM in the federal register, which is expected to be on September 8, 2015. Researchers or sponsors relying on access to data and tissue banks or existing tissue samples should consider commenting given the numerous NPRM provisions affecting this type of research.

---

**Federal Plan to Modernize Medical Trials’ Rules Would be Boon to Universities**

*Chronicle of Higher Education* – September 2, 2015

After more than four years of work, the finish line appears to be in sight for a government wide process to modernize the rules governing human participation in medical trials. The results appear to offer substantial benefits for many university researchers.

The U.S. Department of Health and Human Services issued a 519-page set of regulations on Wednesday, the result of work with 15 other federal departments and agencies dating to 2011. The document represents the first comprehensive overhaul of the regulations in three decades.

The revised rules would make several key policy changes. They would simplify the consent-authorization paperwork given to people who volunteer for medical studies, allow studies that involve multiple universities and trial sites to undergo just a single ethical review, and exclude from those reviews a range of low-risk uses of study subjects, such as interviews and surveys.

The changes stem from a recognition that research practices — and public expectations of what it means to participate in a medical trial — have shifted substantially since federal rules in this area were first put into effect, in 1991, said
Kathy L. Hudson, deputy director for science, outreach, and policy at the National Institutes of Health, which helped lead the policy revisions.

"These aren’t rules to protect people," Ms. Hudson said, describing the government’s new way of regarding so-called human-subjects protection rules. "These are rules that can help guide the relationship between researchers and research participants, and help guide the design and conduct of research."

The rules are expected to save time and money for universities, their institutional review boards, and researchers in the social sciences, who have chafed at needing board approvals for projects that involve human subjects but pose little or no risk to them.

Redirecting Resources

Questions about the adequacy of human-subject consent forms led to tensions last year between two units of the Department of Health and Human Services — the NIH and the Office for Human Research Protections. At issue was a medical study designed to determine the proper amounts of oxygen to be given to premature babies. Previous experience had suggested that too little oxygen could increase the risk of death, while too much could lead to blindness.

Some parents whose babies suffered harm or death suggested afterward that they weren’t clear on the risks and procedures in the study. The NIH and the study’s lead institution, the University of Alabama at Birmingham, faced criticism from the OHRP, which said the experiment and its methods appeared not to have been fully explained to parents at some locations.

The proposal issued on Wednesday — with the endorsement of both NIH and OHRP leaders — intends to simplify the consent forms by requiring plain-English descriptions of expected risks and benefits, while leaving to appendixes the details that might be understood only by a lawyer.

"It puts in place a number of provisions" that make sure that the consent forms "will do a much better job in terms of informing them," said the OHRP’s director, Jerry A. Menikoff.

Improving Patient Safety

The new regulations would cover virtually all medical trials, regardless of their financial support, that are conducted at any American institution that receives federal money. But first the rules must pass through a 90-day comment period before being published in a final form. They would then take effect one year later.

Two provisions would take effect only after three years. One is the rule that would allow a single institutional review board to approve studies at multiple locations. The other is a change in procedures for handling medical specimens. That policy would forbid subsequent studies to reuse specimens without the express consent of each donor, but it would encourage making language that conveys such patient approval a standard feature of consent forms.

The lengthiness of the four-year process, which led some to predict the rules would never be finished, was due to the need to coordinate the changes through more than a dozen federal agencies and various interest groups, said Philip E. Rubin, an adjunct professor of surgery at Yale University who helped draft the rules during his earlier service at the White House’s Office of Science and Technology Policy.

The final rules should improve patient safety by directing regulatory resources where they are most needed, Mr. Rubin said. "When hospitals and universities and other institutions are paying so much attention to that, then they’re not taking the time to pay attention to what they need to do, and they’re overburdened, so it’s great to see that rebalancing."

Both the Association of American Universities and the Association of American Medical Colleges have supported key elements of the changes but said they would need time to review the entire proposal before commenting on its specific provisions.
SUMMARY

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

- Campus Safety
- Compliance Programs
- Information Security / Privacy
- Legislation

Campus Safety

10 Are Dead, 7 Wounded, in Shooting at Community College in Oregon

The Chronicle of Higher Education – October 1, 2015

Ten people died and seven more were wounded in a shooting spree on Thursday at Umpqua Community College, in Roseburg, Oregon, law-enforcement officials said.

In a news conference on Thursday afternoon, Sheriff John Hanlin of Douglas County, Oregon, said that three of the seven were critically injured, the Associated Press and other news outlets reported.

Federal authorities confirmed Thursday evening that the gunman, identified as 26-year-old Chris Harper Mercer, was among the 10 fatalities. The gunman, who lived in a nearby town, was killed by officers who were responding to his attack.

Law-enforcement officials provided no further details about Mr. Mercer or information about his motive. But one witness to the attack said he had demanded that people in one classroom state their religion before he opened fire, the AP reported.

The New York Times reported that the first 911 call came at 10:38 a.m. Pacific time (1:38 p.m. Eastern). The college, which enrolls roughly 2,000 students in a rural area about 175 miles south of Portland, Oregon, went on lockdown. Officers exchanged gunfire with the shooter when they arrived on the scene, Sheriff Hanlin said.

The Times later reported that a law-enforcement official had said the gunman had three weapons, including at least one long gun. “He appears to be an angry young man who was very filled with hate,” the Times quoted the official as saying.

A former president of the college, Joe Olson, told the AP that the institution has only one police officer on duty at a time and that the officer is unarmed.

According to the college’s safety and security policy, “possession, use, or threatened use of firearms” on the campus is prohibited.

A visibly angry and frustrated President Obama said in a televised statement on Thursday evening that mass shootings have become so routine that “we’ve become numb to this.” He challenged voters to make gun safety a priority, saying, “If you think this is a problem, then you should expect your elected officials to reflect your views.”
Compliance Programs

The Yates Memo – A Warning to Execs and Employees

“...corporations are structured to blur lines of authority and prevent responsibility for individual business decisions from residing with a single person.” The same day, Principal Deputy Assistant Attorney General for the Criminal Division Marshall Miller told the Global Investigation Review Program that “corporations do not act criminally, but for the actions of individuals. The Criminal Division intends to prosecute those individuals, whether they’re sitting on a sales desk or in a corporate suite.”

Last month, these warnings were solidified as Department of Justice policy with the publication of Deputy Attorney General Sally Yates’ Memorandum, “Individual Accountability for Corporate Wrongdoing.” The Yates Memo, which is addressed to DOJ attorneys and the FBI, requires the Department to “fully leverage its resources to identify culpable individuals at all levels in corporate cases,” (emphasis added), and outlines “six key steps to strengthen our pursuit of individual corporate wrongdoing,” including:

1. To be eligible for any cooperation credit, corporations must provide to the Department all relevant facts about the individuals involved in corporate misconduct.

2. Both criminal and civil investigators should focus on individuals from the inception of the investigation.

3. Criminal and civil attorneys handing corporate investigations should be in routine communication with one another.

4. Absent extraordinary circumstances, no corporate resolution will provide protection from criminal or civil liability for any individuals.

5. Corporate cases should not be resolved without a clear plan to resolve related individual cases before the statute of limitations expires and declinations as to individuals in such cases must be memorialized.

6. Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual’s ability to pay.

Yates followed the announcement of the memo with a speech the next day, in which she commented that “corporate misconduct isn’t all that different from everything else DOJ investigates and prosecutes. Crime is crime. And it is our obligation at the Justice Department to ensure that we are holding lawbreakers accountable regardless of whether they commit their crimes on the street corner or in the boardroom.”

The Yates Memo constitutes a further development in the DOJ’s longstanding efforts to apply principles of federal prosecution in cases involving corporate wrongdoing. While the Yates Memo focuses on individual accountability for corporate wrongdoing, it follows a series of memos by previous Deputy Attorneys General.
(DAG) clarifying when and whether to require *corporate accountability* based on individual wrongdoing. The Holder Memo (1999); the Thompson Memo (2003); the McNulty Memo (2006) and the Filip Memo (2008), all, have outlined the various factors to be considered in deciding whether to charge a corporation based on the acts of its agents, or individual employees. These factors have always included the nature and extent of the corporation’s cooperation in the investigation, *including its willingness to cooperate in the investigation of its agents and individual employees*.

The difficulties in holding individuals responsible for the company’s conduct, where, as former AG Eric Holder remarked a year ago, “responsibility remains so diffuse, and top executives so insulated, that any misconduct could again be considered more a symptom of the institution’s culture than a result of the willful actions of any single individual,” remain. Even in the DOJ’s $900 million settlement with GM, announced the same week as the release of the Yates Memo, the US Attorney acknowledged the difficulty of finding evidence of individual criminal intent, saying that “a particular person may have had only partial knowledge, and contributed in a chain of actions.” However, the Yates Memo makes it clear that the DOJ has made surmounting these difficulties a priority.

**DOJ Fraud Section Retains Hui Chen as Compliance Counsel Expert**


The *Department of Justice (DOJ)* Fraud Section has retained Hui Chen as a “full-time compliance expert.” Ms. Chen comes to the position with compliance counseling experience in the technology, banking, and pharmaceutical sectors. She served as Microsoft Corporation’s director of legal compliance for the Greater China area. She also served as assistant general counsel at Pfizer Inc. in its compliance division, where she conducted compliance investigations that focused on the company’s operations in Europe, Asia, Latin America, and the Middle East. Most recently, Ms. Chen served as the global head for anti-bribery and corruption at Standard Chartered Bank. Ms. Chen also has prosecutorial experience. From 1991–1994, she served as a trial attorney in the DOJ’s criminal division as part of the Attorney General’s Honors Program, after which she served as an Assistant US Attorney at the US Attorney’s Office in the Eastern District of New York.

In a speech on November 2 regarding Ms. Chen’s position, Assistant Attorney General (AAG) Leslie Caldwell noted that “many banks and financial institutions operate all over the world” and highlighted that DOJ hired a compliance counsel “who has the experience and expertise to examine a compliance program on a more global and a more granular level.” AAG Caldwell also set forth the compliance counsel’s duties, which will include assessing the compliance programs of companies under investigation and testing “whether the compliance program truly is thoughtfully designed and sufficiently resourced to address the company’s compliance risks, or essentially window dressing.” Ms. Chen will also “help guide Fraud Section prosecutors when they are seeking remedial compliance measures as part of a resolution with a company.” According to AAG Caldwell, DOJ seeks to ensure that “appropriate compliance enhancements are included when they are needed” while avoiding imposing “unrealistic, unnecessary or unduly burdensome requirements on companies.”

AAG Caldwell highlighted that DOJ’s retention of a compliance counsel was not an “indication that the department is moving toward recognizing or instituting a ‘compliance defense,’” but would instead continue to review companies’ compliance programs “as one of the many factors to be considered when deciding whether to criminally charge a company or how to resolve criminal charges.” According to AAG Caldwell, DOJ’s “hiring of a compliance counsel should be an indication to companies about just how seriously we take compliance.”
Information Security/Privacy

SEC Cybersecurity Guidance

In April the US Securities and Exchange Commission’s Division of Investment Management released its Cybersecurity Guidance document to help “protect confidential and sensitive information related to…business activities.”

While focused on investment companies, the guidance is short and principle-based and is of value to all types of business enterprise. The guidance includes the following:

- Conduct a periodic assessment of:
  1) the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;
  2) internal and external cybersecurity threats to and vulnerabilities of the firm’s information and technology systems;
  3) security controls and processes currently in place;
  4) the impact should the information or technology systems become compromised; and
  5) the effectiveness of the governance structure for the management of cybersecurity risk. An effective assessment would assist in identifying potential cybersecurity threats and vulnerabilities so as to better prioritize and mitigate risk.

- Create a strategy that is designed to prevent, detect and respond to cybersecurity threats. Such a strategy could include:
  1) controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation, and system hardening;
  2) data encryption;
  3) protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events;
  4) data backup and retrieval; and
  5) the development of an incident response plan. Routine testing of strategies could also enhance the effectiveness of any strategy.

- Implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures.

Legislation

Automatic Enrollment for Health Plans Has Been Repealed


Budget legislation signed into law by President Barack Obama on November 2, 2015, the Bipartisan Budget Act of 2015, repeals the controversial automatic enrollment provision under the Affordable Care Act (ACA).

Section 18A of the Fair Labor Standards Act (FLSA), added by the ACA, directed employers with more than 200 full time employees to automatically enroll new full time employees in one of the employer’s health benefits plans (subject to any waiting period authorized by law), and to continue the enrollment of current employees in a health benefits plan offered through the employer. This requirement, which had yet to take effect, was riddled with concerns and questions regarding how these employers would effectuate administration.

The Budget Bill also sharply increased the amount of premiums employers pay to the Pension Benefit Guaranty Corporation.
SUMMARY

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

- Campus Safety
- Compliance Programs
- Controlled Substances
- Information Security / Privacy
- Legislation
- Stark Law
- Ig Nobel

Campus Safety

10 Are Dead, 7 Wounded, in Shooting at Community College in Oregon

*The Chronicle of Higher Education* – October 1, 2015

Ten people died and seven more were wounded in a shooting spree on Thursday at Umpqua Community College, in Roseburg, Oregon, law-enforcement officials said.

In a news conference on Thursday afternoon, Sheriff John Hanlin of Douglas County, Oregon, said that three of the seven were critically injured, the Associated Press and other news outlets reported.

Federal authorities confirmed Thursday evening that the gunman, identified as 26-year-old Chris Harper Mercer, was among the 10 fatalities. The gunman, who lived in a nearby town, was killed by officers who were responding to his attack.

Law-enforcement officials provided no further details about Mr. Mercer or information about his motive. But one witness to the attack said he had demanded that people in one classroom state their religion before he opened fire, the AP reported.

*The New York Times* reported that the first 911 call came at 10:38 a.m. Pacific time (1:38 p.m. Eastern). The college, which enrolls roughly 2,000 students in a rural area about 175 miles south of Portland, Oregon, went on lockdown. Officers exchanged gunfire with the shooter when they arrived on the scene, Sheriff Hanlin said.

The *Times* later reported that a law-enforcement official had said the gunman had three weapons, including at least one long gun. “He appears to be an angry young man who was very filled with hate,” the *Times* quoted the official as saying.

A former president of the college, Joe Olson, told the AP that the institution has only one police officer on duty at a time and that the officer is unarmed.

According to the college’s safety and security policy, “possession, use, or threatened use of firearms” on the campus is prohibited.

A visibly angry and frustrated President Obama said in a televised statement on Thursday evening that mass shootings have become so routine that “we’ve become numb to this.” He challenged voters to make gun safety a priority, saying, “If you think this is a problem, then you should expect your elected officials to reflect your views.”
Compliance Programs

The Yates Memo – A Warning to Execs and Employees

JDSupra Business Advisor – October 7, 2015

“The buck needs to stop somewhere where corporate misconduct is concerned,” said Attorney General Eric Holder in a September 17, 2014 speech to NYU School of Law. He went on to say that “corporations are structured to blur lines of authority and prevent responsibility for individual business decisions from residing with a single person.” The same day, Principal Deputy Assistant Attorney General for the Criminal Division Marshall Miller told the Global Investigation Review Program that “corporations do not act criminally, but for the actions of individuals. The Criminal Division intends to prosecute those individuals, whether they’re sitting on a sales desk or in a corporate suite.”

Last month, these warnings were solidified as Department of Justice policy with the publication of Deputy Attorney General Sally Yates’ Memorandum, “Individual Accountability for Corporate Wrongdoing.” The Yates Memo, which is addressed to DOJ attorneys and the FBI, requires the Department to “fully leverage its resources to identify culpable individuals at all levels in corporate cases,” (emphasis added), and outlines “six key steps to strengthen our pursuit of individual corporate wrongdoing,” including:

1. To be eligible for any cooperation credit, corporations must provide to the Department all relevant facts about the individuals involved in corporate misconduct.
2. Both criminal and civil investigators should focus on individuals from the inception of the investigation.
3. Criminal and civil attorneys handing corporate investigations should be in routine communication with one another.
4. Absent extraordinary circumstances, no corporate resolution will provide protection from criminal or civil liability for any individuals.
5. Corporate cases should not be resolved without a clear plan to resolve related individual cases before the statute of limitations expires and declinations as to individuals in such cases must be memorialized.
6. Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual’s ability to pay.

Yates followed the announcement of the memo with a speech the next day, in which she commented that “corporate misconduct isn’t all that different from everything else DOJ investigates and prosecutes. Crime is crime. And it is our obligation at the Justice Department to ensure that we are holding lawbreakers accountable regardless of whether they commit their crimes on the street corner or in the boardroom.”

The Yates Memo constitutes a further development in the DOJ’s longstanding efforts to apply principles of federal
prosecution in cases involving corporate wrongdoing. While the Yates Memo focuses on *individual accountability* for corporate wrongdoing, it follows a series of memos by previous Deputy Attorneys General (DAG) clarifying when and whether to require *corporate accountability* based on individual wrongdoing. The Holder Memo (1999); the Thompson Memo (2003); the McNulty Memo (2006) and the Filip Memo (2008), all, have outlined the various factors to be considered in deciding whether to charge a corporation based on the acts of its agents, or individual employees. These factors have always included the nature and extent of the corporation’s cooperation in the investigation, *including its willingness to cooperate in the investigation of its agents and individual employees.*

The difficulties in holding individuals responsible for the company’s conduct, where, as former AG Eric Holder remarked a year ago, “responsibility remains so diffuse, and top executives so insulated, that any misconduct could again be considered more a symptom of the institution’s culture than a result of the willful actions of any single individual,” remain. Even in the DOJ’s $900 million settlement with GM, announced the same week as the release of the Yates Memo, the US Attorney acknowledged the difficulty of finding evidence of individual criminal intent, saying that “a particular person may have had only partial knowledge, and contributed in a chain of actions.” However, the Yates Memo makes it clear that the DOJ has made surmounting these difficulties a priority.

**DOJ Fraud Section Retains Hui Chen as Compliance Counsel Expert**


The *Department of Justice (DOJ)* Fraud Section has retained Hui Chen as a “full-time compliance expert.” Ms. Chen comes to the position with compliance counseling experience in the technology, banking, and pharmaceutical sectors. She served as Microsoft Corporation’s director of legal compliance for the Greater China area. She also served as assistant general counsel at Pfizer Inc. in its compliance division, where she conducted compliance investigations that focused on the company’s operations in Europe, Asia, Latin America, and the Middle East. Most recently, Ms. Chen served as the global head for anti-bribery and corruption at Standard Chartered Bank. Ms. Chen also has prosecutorial experience. From 1991–1994, she served as a trial attorney in the DOJ’s criminal division as part of the Attorney General’s Honors Program, after which she served as an Assistant US Attorney at the US Attorney’s Office in the Eastern District of New York.

In a speech on November 2 regarding Ms. Chen’s position, Assistant Attorney General (AAG) Leslie Caldwell noted that “many banks and financial institutions operate all over the world” and highlighted that DOJ hired a compliance counsel “who has the experience and expertise to examine a compliance program on a more global and a more granular level.” AAG Caldwell also set forth the compliance counsel’s duties, which will include assessing the compliance programs of companies under investigation and testing “whether the compliance program truly is thoughtfully designed and sufficiently resourced to address the company’s compliance risks, or essentially window dressing.” Ms. Chen will also “help guide Fraud Section prosecutors when they are seeking remedial compliance measures as part of a resolution with a company.” According to AAG Caldwell, DOJ seeks to ensure that “appropriate compliance enhancements are included when they are needed” while avoiding imposing “unrealistic, unnecessary or unduly burdensome requirements on companies.”

AAG Caldwell highlighted that DOJ’s retention of a compliance counsel was not an “indication that the department is moving toward recognizing or instituting a ‘compliance defense,’” but would instead continue to review companies’ compliance programs “as one of the many factors to be considered when deciding whether to criminally charge a company or how to resolve criminal charges.” According to AAG Caldwell, DOJ’s “hiring of a compliance counsel should be an indication to companies about just how seriously we take compliance.”
Controlled Substances

NIH Releases Comprehensive Resource to Help Address College Drinking

*NIH News* – September 22, 2015

CollegeAIM, a new resource to help college officials address harmful and underage student drinking, is now available. The CollegeAIM (Alcohol Intervention Matrix) guide and website was developed by the National Institute on Alcohol Abuse and Alcoholism, part of the National Institutes of Health.

The centerpiece of CollegeAIM is a comprehensive and easy-to-use matrix-based tool that will help inform college staff about alcohol interventions and guide college staff to evidence-based interventions. CollegeAIM is the result of a multi-year collaboration and an extensive review of the scientific literature. It is unique in the breadth of research covered by its analysis, and the number and expertise of its contributors.

“Despite our collective efforts to address it, high-risk drinking remains a significant and persistent problem on U.S. campuses,” said George Koob, Ph.D., NIAAA director. “While college officials have numerous options for alcohol interventions, they are not all equally effective. CollegeAIM can help schools choose wisely among available strategies, boosting their chances for success and helping them improve the health and safety of their students.”

CollegeAIM compares and rates nearly 60 types of interventions on effectiveness, anticipated costs and barriers to implementation, and other factors. Interventions are classified as either environmental-level strategies or individual-level strategies. Environmental-level strategies target the campus community and student population as a whole; while individual-level strategies focus on individual students, including those in higher risk groups such as first-year students, student-athletes, and members of Greek organizations. With CollegeAIM, school officials can learn how their current strategies compare to other evidence-based alternatives; discover possible new strategies to consider; and select a combination of approaches that best meets the particular needs of their students and campus.

The top tier of CollegeAIM – higher effectiveness – includes eight individual and five environmental strategies. In general, they represent a range of counseling options and policies related to sales and access.

“This new matrix-based instrument is one of the most thoroughly vetted and user-friendly summaries of intervention strategies I have seen in decades,” said Jonathan Gibralter, Ph.D., president of Wells College in Aurora, New York, and chair of the NIAAA College Presidents Working Group to Address Harmful and Underage Drinking.

“There is a pressing need for a clear, unbiased tool to help colleges make informed decisions,” Dr. Gibralter said. “College administrators are in a critical position – to serve as catalysts to influence a school’s social atmosphere and make choices that improve the health and safety of students. And we believe the CollegeAIM guide and website will help.”

Underage drinking, as well as harmful drinking among students of legal drinking age, continues to be a major problem on U.S. campuses. Researchers estimate that each year 696,000 college students are assaulted by another student who has been drinking, 97,000 students report experiencing alcohol-related sexual assault or date rape and 1,825 students die from alcohol-related injuries.

The CollegeAIM guide and related resources, along with additional information on harmful and underage college drinking, are available at [www.collegedrinkingprevention.gov](http://www.collegedrinkingprevention.gov).

The National Institute on Alcohol Abuse and Alcoholism, part of the National Institutes of Health, is the primary U.S. agency for conducting and supporting research on the causes, consequences, prevention, and treatment of alcohol abuse, alcoholism, and alcohol problems. NIAAA also disseminates research findings to general, professional, and academic audiences. Additional alcohol research information and publications are available at [www.niaaa.nih.gov](http://www.niaaa.nih.gov).

Information Security/Privacy
Thousands of Critical Medical Devices Exposed Online

*eSecurity Planet* - October 01, 2015

At the DerbyCon security conference in Louisville, Kentucky, security researchers Scott Erven and Mark Collao recently stated that thousands of critical medical devices are connected to the Internet and vulnerable to attack, *The Register* reports.

At one unnamed U.S. healthcare organization with 12,000 staff and 3,000 physicians, Erven and Collao said, more than 68,000 devices are exposed online, including 21 anaesthesia systems, 488 cardiology systems, 67 nuclear medical systems, 133 infusion systems, 31 pacemakers, 97 MRI scanners, and 323 picture archiving and communications devices.

The researchers discovered the linked devices through the Shodan device search engine. "Once we [started] changing [search terms] to target speciality clinics like radiology or podiatry or pediatrics, we ended up with thousands with misconfiguration and direct attack vectors," Erven said.

MRI and defibrillator machine honeypots (a honeypot consists of data that appears to be a legitimate part of the site but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers) placed by Erven and Collao attracted 55,416 successful SSH and Web logins and 299 malware payloads. As a result, they said, it's reasonable to assume that there are infected medical devices connecting to command and control servers on a regular basis.

"These devices are getting owned repeatedly, and now that more devices and hospitals are Wi-Fi enabled, it's pretty prevalent," Collao said, *SC Magazine* reports. "Next time you're in a hospital and you're getting hooked up to a machine and you see Ethernet going into a wall, it makes you think twice -- is this connected to a command and control server somewhere?"

"The Internet of Things is already here, and some of its denizens are already in critical condition," Tripwire director of IT security and risk strategy Tim Erlin told *eSecurity Planet* by email. "Embedded devices are nothing new, and the expansion of Internet connectivity has turned networked embedded devices, from energy to healthcare, into internetworked embedded devices. As the forward end of the industry works to bring the 'things' to the Internet, the Internet has already been brought to the 'things' that were out there."

"With embedded devices, it's often not as simple as applying the latest updates," Erlin added. "When those devices interact directly with a human being in a therapeutic task, it’s even more complicated to make changes. This isn't a challenge that’s likely to go away. It's likely to get worse, and make headlines, when someone hacks a medical device to make a point."

**SEC Cybersecurity Guidance**

In April the US Securities and Exchange Commission’s Division of Investment Management released its *Cybersecurity Guidance* document to help “protect confidential and sensitive information related to…business activities.”

While focused on investment companies, the guidance is short and principle-based and is of value to all types of business enterprise. The guidance includes the following:

- Conduct a periodic assessment of:
  1) the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;
  2) internal and external cybersecurity threats to and vulnerabilities of the firm’s information and technology systems;
  3) security controls and processes currently in place;
  4) the impact should the information or technology systems become compromised; and
  5) the effectiveness of the governance structure for the management of cybersecurity risk. An effective assessment would assist in identifying potential cybersecurity threats and vulnerabilities so as to better prioritize and mitigate risk.
Create a strategy that is designed to prevent, detect and respond to cybersecurity threats. Such a strategy could include:

1) controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation, and system hardening;

2) data encryption;

3) protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events;

4) data backup and retrieval; and

5) the development of an incident response plan. Routine testing of strategies could also enhance the effectiveness of any strategy.

Implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures.

Legislation

Automatic Enrollment for Health Plans Has Been Repealed


Budget legislation signed into law by President Barack Obama on November 2, 2015, the Bipartisan Budget Act of 2015, repeals the controversial automatic enrollment provision under the Affordable Care Act (ACA).

Section 18A of the Fair Labor Standards Act (FLSA), added by the ACA, directed employers with more than 200 full time employees to automatically enroll new full time employees in one of the employer’s health benefits plans (subject to any waiting period authorized by law), and to continue the enrollment of current employees in a health benefits plan offered through the employer. This requirement, which had yet to take effect, was riddled with concerns and questions regarding how these employers would effectuate administration.

The Budget Bill also sharply increased the amount of premiums employers pay to the Pension Benefit Guaranty Corporation.

Stark Law

Compensation for Employed MDs Who Lost Money Led to Hospital’s $69M Settlement

Report on Medicare Compliance - September 21, 2015

Because of their patient referrals, the paychecks of nine physicians employed by North Broward Hospital District were fat even though their practices lost money, a quid pro quo that allegedly violated the Stark law and led to a $69 million false claims settlement, the Department of Justice (DOJ) said Sept. 15.

The lawsuit originally was filed by whistleblower Michael Reilly, M.D., who said he was offered an employment contract by North Broward Hospital District in Fort Lauderdale, Fla., which does business as Broward Health and includes 30 facilities. Reilly, an orthopedic surgeon, turned the employment offer down and filed a false claims lawsuit. He alleged North Broward paid the physicians above fair-market value and at rates that weren’t commercially reasonable and took into account the volume or value of patient referrals from 2004 on. DOJ intervened in the lawsuit at the end for the purpose of settling it. North Broward did not admit liability in the settlement.

The complaint paints a detailed picture of the money going in and out of the physician practices and how much revenue they generated for Broward Health. This was itemized in “margin reports,” alleged the complaint. “Throughout the employment period of each physician, Broward Health has tracked and monitored the value and volume of referrals from each physician in contribution Margin Reports,” the complaint alleged. “If the value and
volume of referrals did not offset the excessive physician compensation, then Broward Health pressured particular physicians with deficient referrals for increased referrals to Broward Health hospitals and clinics.”

DOJ has a problem with hospitals losing money on referring physicians under the Stark law. It isn’t commercially reasonable to take a loss, the argument goes, and arrangements between entities that provide designated health services (e.g., hospitals) and referring physicians must be commercially reasonable to qualify for an exception to the Stark law *(RMC 3/16/15, p. 1)*.

“The settlement shows DOJ is aggressively pursuing physician employment under the Stark law,” says Tony Maida, former deputy chief of the administrative and civil remedies branch at the HHS Office of Inspector General. “There are many legitimate reasons why a hospital may not break even on a physician, such as bringing a needed specialty to the community or nonclinical work that the physician is going to do. Documenting what went into making the compensation decisions is critical to explaining it to the government later — and assume that you will need to explain at some point,” says Maida, with McDermott, Will & Emery in New York City.

The complaint explained the alleged imbalance between compensation and revenue. For example, in 2011, the complaint alleged the employed orthopedic surgeons generated $3,229,793 in collections, and their practice overhead was $5,712,239. “The percent of the practice group overhead to collections was 176 percent,” the complaint contended. Halfway through the year, Broward Health figured the net loss from the orthopedic group was $2,482,446. “The excessive compensation of the employed orthopedic surgeons was on pace to generate losses of $4,964,892,” the complaint alleged.

But the whistleblower alleged the health system didn’t mind because there were other benefits to employing the physicians, according to the complaint. “Broward Health tracked hospital profits from inpatient referrals by its employed orthopedists in the amount of $1,341,280 and hospital profits from outpatient referrals by its employed orthopedists in the amount of $2,318,359,” the complaint alleged.

Broward Health allegedly did a thorough analysis of the value and volume of referrals from each orthopedic surgeon. For example, in 2009, the health system was looking at a net loss of $814,007 on one of the orthopedic surgeons. Broward Health paid him $1,424,356.85, about $300,000 more than the 90th percentile for orthopedic surgery-sports medicine, according to a Medical Group Management Association salary survey, says the complaint. Broward Health agreed to this in anticipation of referral revenues, which were tracked and monitored in secretive reports, the complaint alleged.

The whistleblower describes similar arrangements with other orthopedic surgeons and with cardiologists. “There is one major reason for Broward Health’s excessive compensation of such physician practice groups to generate massive losses: profits from referrals to Broward Health hospitals and clinics,” the complaint alleged.
One message from this case is that “it’s a high-risk proposition” to use revenue from hospital admissions, ancillaries and other services to justify physician compensation, says Denver attorney Jeffrey Fitzgerald, with Polsinelli. “In this case, the allegation was that the hospital revenue — designated health services — was connected to the physician compensation structure in a manner that was not allowed under Stark,” he says.

However, there’s a little too much fuss about the so-called secret reports, Fitzgerald says. Almost every hospital tracks its revenue by department and physician. “How could you run a business without tracking its revenue? There is a legitimate and commonplace need to understand and track sources of hospital revenue, including from employed physicians. But the risk increases if these data are used to justify physician salaries,” he says. Part of the solution is to silo data. “I tell my clients they can run productivity reports on their physicians and analyze hospital revenue on a per-physician basis.” But the reports shouldn’t be shared with or used by the people who make decisions about physician compensation.

And documents that track profitability of captive physician practices shouldn’t include data related to hospital productivity or per-physician hospital revenue, Fitzgerald notes.

He calls these “complicated issues,” and while the allegations in the North Broward case should be taken “with a grain of salt,” it’s impossible to dismiss the fact that a health system settled for a whopping $69 million over nine physicians. “Maybe it’s time to revisit the overbearingness of Stark,” Fitzgerald says.

Washington, D.C., attorney Linda Baumann, who represents North Broward, emphasized that the allegations against her client “are just allegations; they are not proven at all.” She noted the health system cooperated with the government and settled to avoid litigation. Rather than spending more money on legal fees, the system wanted to be able to focus on patient care. “I certainly wouldn’t say the fact that a hospital employs physicians and doesn’t make a profit on their professional fees is clear evidence of payment for referrals,” notes Baumann, with Arent Fox. But fighting it out in court is impossibly expensive, as Tuomey Healthcare in South Carolina learned (RMC 8/3/15, p. 3).

Ig Nobel Prizes

Just in case you missed them, the Ig Nobel prizes awarded in 2015 included the following:

**DIAGNOSTIC MEDICINE PRIZE** — Diallah Karim [CANADA, UK], Anthony Harnden [NEW ZEALAND, UK, US], Nigel D'Souza [BAHRAIN, BELGIUM, DUBAI, INDIA, SOUTH AFRICA, US, UK], Andrew Huang [CHINA, UK], Abdel Kader Allouni [SYRIA, UK], Helen Ashdown [UK], Richard J. Stevens [UK], and Simon Kreckler [UK], for determining that acute appendicitis can be accurately diagnosed by the amount of pain evident when the patient is driven over speed bumps.


**PHYSICS PRIZE** — Patricia Yang [USA and TAIWAN], David Hu [USA and TAIWAN], and Jonathan Pham, Jerome Choo [USA], for testing the biological principle that nearly all mammals empty their bladders in about 21 seconds (plus or minus 13 seconds).


**PHYSIOLOGY and ENTOMOLOGY PRIZE** — Awarded jointly to two individuals: Justin Schmidt [USA, CANADA], for painstakingly creating the Schmidt Sting Pain Index, which rates the relative pain people feel when stung by various insects; and to Michael L. Smith [USA, UK, THE NETHERLANDS],
for carefully arranging for honeybees to sting him repeatedly on 25 different locations on his body, to learn which locations are the least painful (the skull, middle toe tip, and upper arm) and which are the most painful (the nostril, upper lip, and umm...other parts of the anatomy.)


LITERATURE PRIZE — Mark Dingemanse [THE NETHERLANDS, USA], Francisco Torreira [THE NETHERLANDS, BELGIUM, USA], and Nick J. Enfield [AUSTRALIA, THE NETHERLANDS],

for discovering that the word "huh?" (or its equivalent) seems to exist in every human language — and for not being quite sure why.

REFERENCE: "Is 'Huh?' a universal word? Conversational infrastructure and the convergent evolution of linguistic items," Mark Dingemanse, Francisco Torreira, and Nick J. Enfield, PLOS ONE, 2013. [a video accompanies the paper.]
Six Lessons Learned in Managing the Risk of Minors on Campus

Candace Collins JD
Praesidium, Inc.

Richard Dangel Ph.D.
Praesidium, Inc.

Aaron Lundberg LMSW
Praesidium, Inc.
Children are the world’s most valuable resource and its best hope for the future.

—JOHN F. KENNEDY (1917-1963),
POLITICIAN AND 35TH PRESIDENT OF THE UNITED STATES
Six Lessons Learned in Managing the Risk of Minors on Campus

| Candace Collins JD, Richard Dangel Ph.D., and Aaron Lundberg LMSW, Praesidium, Inc. |

Abstract: As estimates of the number of minors served on college and university campuses increase, schools are taking a proactive approach to protect underage visitors to their campuses. This article reviews obstacles faced by institutions when developing policies and procedures to deal with minors on campus and ways that risk managers can overcome these obstacles.

Introduction

Some statistics indicate that one-in-four girls and one-in-six boys are sexually abused before the age of eighteen.1 Ten percent of students may be exposed to sexual misconduct before completing high school,2 and there has been a significant increase in peer-to-peer sexual abuse in recent years.3 And while most parents warn their children about “stranger danger,” the majority of the time the offender isn’t a stranger at all, but rather someone known by the child or family.4

Over the past decade or so, most major youth-serving organizations, including the YMCA, Boys and Girls Clubs, and Big Brothers Big Sisters, have made significant progress in keeping minors in their programs safe from sexual abuse by employees, volunteers, and other program participants. Churches, schools, camps, childcare programs, and social-service agencies have made similar strides. But in the aftermath of the 2011 Jerry Sandusky child sexual abuse scandal that rocked the higher-education community, colleges and universities across the nation began realizing that they were not fully aware of just how big and dangerous a risk they were embracing in offering programs for minors. In the wake of this realization, universities across the nation have been hard at work to evaluate, develop, and implement system-wide changes. And through this work, many universities discovered that seemingly simple questions such as “How many minors do we serve on campus? In which programs are we serving minors? What safeguards do we have in place to protect minors?” are not so easily answered.

Many universities began by attempting to quantify their exposure but quickly realized they lacked a process to identify and track all youth-serving programs, and were unable to determine the actual number of minors served. Those universities that were able to get an estimate were surprised—even shocked—to realize that they actually served far more minors than university students. Between summer camps, recreation events, childcare, laboratory research, mentoring programs, 4-H, campus tours, and community outreach, the numbers kept growing.

Many universities also realized they had several similar programs operating in very dissimilar ways. For example: two camps, one an athletic camp and the other a recreation-center camp, both served similar groups of minors yet used completely different policies, procedures, employee- and volunteer-screening methods, and youth-supervision standards. Likewise, universities found that community outreach programs varied within and across departments, and many programs that served minors were unaware that they were required to comply with state licensing standards related to staffing ratios and employee- and volunteer-screening, selection, and training requirements.

Today, university awareness of this risk has increased tremendously and most have begun systematically addressing the exposure. These authors have worked with numerous universities—large and small, state and private—to help them assess and manage this exposure, and together we’ve learned six important lessons.
Lesson 1: Universities embrace a myriad of risks, each competing for attention and resources.

Universities face a myriad of challenges today. The explosion of MOOCs, competition for funding, skyrocketing student loans, national rankings, student dating violence, and increased federal regulation and oversight are only a few. The risks associated with serving minors on campus must compete for attention and resources.

Nevertheless, the need to manage this risk is a pressing issue. Instead of a short-term response, universities should think about an over-arching cultural shift. This means that a successful rollout and implementation of a minors-on-campus initiative requires a long-term investment from diverse leadership. Not everyone will be equally interested or committed, which is why universities should build a team of influential stakeholders early on and appoint an individual torchbearer to maintain momentum.

One example of a struggle we hear about often involves athletic departments and some level of push back on screening and training. These departments are often large, serve lots of minors, generate lots of money, and carry significant political power on campus. But imagine the ramifications of an entire department refusing to comply with an institutional position, choosing instead to act on its own authority. To avoid an entire department or group of faculty members resisting new policies and procedures, it is important to ensure that the interests of all groups are represented in the implementation process by including representatives from key departments in the decision making.

Lesson 2: Universities strive to develop the fewest policies that reasonably manage the most risks.

The first step we see universities taking is developing a campus-wide policy that meets industry standards and regulations. Some universities have individual policies for individual issues such as background checks, training, interactions with minors, and reporting. The challenge is how to create a broad enough policy that has teeth and also realistically applies to all programs.

While each university must find its own balanced approach that fits within its campus culture, we recommend that universities develop two types of policies to address minors: campus-wide policies and program-specific policies. Campus-wide policies are designed to create a minimum standard for all university programs that serve minors. These policies apply broadly and may cover a significant percentage of the exposures the university faces. The more risks that can be managed with the fewer policies, the better. At the same time, program-specific policies are designed to manage the specific risks of various program types and to ensure that similar programs operate in similar, consistent ways.

What difference does it make? Imagine university policies that prohibit meeting alone with one minor, or transporting minors. That sounds easy enough and may greatly reduce the risk of child sexual abuse. In fact, these policies may work well for everyone who runs campus tours and swim lessons. But what about a crew camp that travels to a local boating club for practice, a science summer camp that takes museum field trips, or a music lesson that needs to be one-on-one? A one-size-fits-all, universal policy doesn’t always work for every program that serves minors.

Campus-wide Policies

There are recognized industry standards and regulations that apply broadly to everyone in all programs at a university. Campus-wide policies strive for balance on the level of detail, but err on the side of broad inclusion. They are designed to address global issues that apply to anyone who works with or around minors, including screening, training, and reporting, and they include a zero-tolerance statement.

Screening

One of the most well-established standards among youth-serving organizations is background checks. The screening process is the first line of defense in limiting access to minors, and, in implementing new policies, most universities immediately start thinking about their background-check process.

But effective screening requires more than just background checks. While completing a background check is the industry standard these days, only a very small percentage of offenders have a criminal record. We recommend that universities include additional safeguards, such as standardized applications, face-to-face interviews,
reference checks, and an overall screening process specifically designed to assess for abuse-risk behavior.

The campus-wide policy should address key screening procedures that apply to anyone who works with or around minors. This includes not just faculty, staff, student employees, and interns, but also volunteers and chaperones.

**Training**

Industry standards also indicate that anyone who works with or around minors should complete some level of abuse-prevention training. The campus-wide policy sets forth these abuse-prevention training requirements. Again, this includes more than just employees—volunteers must also be trained. The next section outlines in greater detail what this training encompasses; however, from a policy perspective, universities should stipulate training be completed before individuals may work with minors—or very soon after they start—and be annually refreshed. In addition a variety of methods to maintain awareness throughout the year should be implemented.

**Reporting**

Universities need to create centralized reporting procedures to ensure responses are prompt and effective. Many universities have already started this process by centralizing mandatory reporting procedures for suspicions and allegations of abuse. This type of reporting is vital to ensure prompt and appropriate responses, which can potentially decrease the consequences of abuse. Equal importance to address in a centralized reporting policy are procedures for reporting suspicious or inappropriate behavior and policy violations and procedures for reporting minor-to-minor sexual behaviors.

Implementing a campus-wide reporting procedure for unacceptable behaviors that may not rise to the level of abuse helps universities identify problem individuals and address issues before an allegation of abuse is made. A reporting procedure for minor-to-minor behaviors further aids in the process of determining whether a child is simply having a bad day or is exhibiting behavior that may exceed the level of services provided by the program.

Including all three of these reporting procedures in the campus-wide policy provides universities with an opportunity to continually assess the need for additional safety measures and training.

**Zero Tolerance**

In an effort to set the right tone and culture, the system-wide policy ideally includes a zero-tolerance statement prohibiting abuse. Including a code of conduct is another way to provide a broad description of behaviors that are always prohibited when working with minors. These may include a prohibition on drugs, alcohol, and pornography in the presence of minors or during program operation.

**Program-specific Policies**

Program-specific policies help maintain consistency across similar programs by addressing varying risks that may exist in different types of programs. Note that a university does not need five thousand sets of policies to address five thousand individual programs. Rather, it may group programs together (day camps, student teachers, community outreach, overnight events, international programs, etc.) and implement consistent, program-specific guidelines that address more detailed issues such as interactions, boundaries, and high-risk activities.

**Interactions and Boundaries**

Whether it’s an offender grooming a child or behavior leading to a false allegation of abuse, poorly defined boundaries usually contribute to high-risk situations. To an outsider, both interactions may look the same. Without clear guidelines, individuals may interact with minors based on their own perceptions and personal comfort level. Specific policies set the bandwidth of acceptable behavior so that everyone in the program knows what constitutes a reportable offense. Not all policy violations constitute abuse, but putting everyone on the same page makes the reporting process less personal and refocuses the attention on safety.

Within each program type, develop guidelines for appropriate and inappropriate interactions between adult and minor participants. Consider addressing physical affection, verbal interactions, and whether and under what circumstances employees and volunteers may have contact outside of the program, communicate electronically or through social media, or give gifts to minors.
High-Risk Activities

Different programs have different activities and risks that are uniquely associated with abuse and false allegations. For instance, tutoring and mentoring programs may involve situations with more privacy and one-on-one interactions than other programs. Alternatively, a day camp may include an off-site activity or field trip with potential for interactions with the general public and uncontrolled environmental factors. Other high-risk situations include bathroom and locker-room activities, transportation, activities associated with water and swimming, overnight activities, and activities with mixed age groups. Develop guidelines for managing these high-risk activities as they relate to programs.

Lesson 3: Universities struggle to determine who should be background-checked and trained.

Universities have known for some time that they have an obligation to complete background checks on some individuals. However, because not all individuals on campus have the same level of access to minors in university programs, we receive a lot of questions about how to determine who should be background-checked and trained. Universities typically want to know how the screening and training process differs for different types of individuals: faculty who rarely interact with minors, employees who provide direct supervision for minors in a program, janitors, volunteers, contractors, etc. These decisions naturally present challenges. Cost may be a significant factor, and multiple stakeholders with differing opinions may be involved in the decision-making.

Unfortunately, there is not one answer that fits every university and every situation. However, there are a few guidelines a university can follow. First, follow all state and federal regulations. Second, the key is to let access to minors—not just title, employment, or contract status—guide the decisions.

State and National Laws

Several state and federal laws may govern who at a university should be background-checked, trained, and who is a mandatory reporter. Be aware of these laws and any licensing regulations that may affect a program.

Assessing Access

Assess access to minors by evaluating how each individual or group of individuals may interact with minors based on frequency, duration, level of supervision, and nature of the relationship.

- How frequently does the individual work around or interact with minors? Is it a one-time event or every day?
- What is the duration of the individual’s interactions? Is it a one-time, one-hour event or an entire summer?
- Are the individual’s interactions always supervised by another adult or are they one-on-one with minors?
- What is the nature of the relationship between the individual and the minors in the program? Does the individual merely supervise an area during a campus event that has minors, or are they getting to know individual minors and families while advising or tutoring?

Applying the above criteria may reveal surprising needs for additional screening and training. For example, a janitor at a recreation center may work around minors every day—sometimes when they are dressing and showering. A student teacher may work with minors for the duration of a school year. A professor in a lab may have unsupervised access in isolated or restricted areas of campus. All of these situations require more than just cursory thought on the issue of background checks and training.

When in doubt, err on the side of caution and increase the level of screening and training.

Lesson 4: Universities must rely on a multifaceted approach to deliver the right training to the right people at the right time.

Training on abuse prevention has become industry standard and is federally mandated in some instances. Some training must be generic enough that it is useful for anyone who interacts with minors, while other training must be program-, job-, or role-specific. For example, everyone who interacts with minors needs to know how to identify warning signs of offenders, high-risk behaviors, and proper reporting procedures. This knowledge base requires training in a variety of formats to reinforce key points.
However, universities face unique challenges due to the large number of individuals involved in programming and the roles they play at different times of year. Therefore, an effective training-delivery system must ensure that the right training gets to the right people at the right time. The training must include preventative content and program-specific information that is timely, easy to use, and holds everyone accountable.

Right Content
Not all abuse-prevention training is created equal. Some programs primarily focus on identifying signs and symptoms that a child has been abused or how to report abuse. Though these topics are important, these types of training programs fail to teach how to prevent abuse. The right training incorporates preventative, not just reactive, measures. Preventative training establishes a culture of awareness and involvement at all levels.

Program-Specific
Universities operate all kinds of programs, many of which have unique risks. The training for these programs should be specific to these risks, whether it’s a day camp, aquatic program, tutoring, overnight trip, or summer coaching. One training is unlikely to fit all program types.

Timely
The training must be delivered in such a way that individuals can access it prior to their interactions with minors, or very soon after. Training after an incident may help with future knowledge, but it doesn’t address events that have already occurred.

Ease of Use
Everyone is busy and technological glitches are no fun. To maximize the training experience, individuals must be able to easily enroll, schedule, and complete training courses.

Accountability
Individuals must be accountable for their training requirements. This means that universities need the ability to track who has completed what training and when.
To create a strong learning culture, consider using a blended training-delivery system, with both online and in-person components. For instance, leadership may benefit more from in-person training. These individuals may include campus leaders, deans, department chairs, program directors and assistant directors. Employees, interns, and volunteers may benefit more from online training. The ease and convenience of online training allows these users to complete training during a time that works best for them.
Campus-wide policies and general information are often communicated through online training modules. Supplemental information for program types can be delivered online or in-person. Supervisors should also consider incorporating in-person training components to reinforce knowledge retention and maintain awareness.

Lesson 5: Universities need to contractually manage relationships with vendors who serve or who have access to minors on campus
Contractors often have access to or serve minors in a variety of capacities, and universities need to ensure these individuals are operating with at least minimum safeguards. Universities also need assurances that contractors are not registered sex offenders. This means that how universities deal with contractors, vendors, facility rentals, and other situations involving third-party contracts is equally important in preventing sexual abuse of minors and minimizing organizational risk. We have found that many universities struggle to find the right balance in their relationships with contractors. For instance, they don’t want the wrong people involved with programs on campus or minors running around campus with zero supervision, but they also don’t want to negate the risk-shifting benefits of a contractual arrangement. To address these concerns, consider using a four-by-four approach: identify four
types of ownership and address four key issues.

Programs that serve minors typically fall into four ownership categories, most of which involve an outside entity: (1) the university solely owns and operates the program; (2) the university jointly operates the program with another organization; (3) the university contracts with another organization to provide the program; (4) another organization uses the university’s facilities to operate the program independently from (and having no affiliation with) the university.

When universities do not solely own or operate programs, other individuals (often with no university affiliation) may interact with minors. It’s not uncommon for parents and participants to associate the university’s name with a particular program that serves minors even when the university doesn’t actually operate, sponsor, or host the event, whether it’s a summer camp run by a coach operating under his own limited-liability company or a local book club hosted by community sponsors. Before signing a contract or facility-use agreement, universities must address the following four issues with all necessary internal departments (risk management, contracts and procurement, office of general counsel, etc.): (1) screening; (2) training; (3) supervision; (4) insurance coverage.

**Screening**

Universities may know the background check requirements for their employees and volunteers, but what about the outside organization and its employees and volunteers? How are these individuals who interact with minors screened? At a minimum, ensure that the individuals who supervise and are responsible for minors submit to a national background check and a national sex offender registry search.

**Training**

How are individuals who interact with minors trained by the contractor? The university will want to ensure that everyone interacting with minors receives abuse-prevention training similar to that described above, and knows the applicable policies and procedures.

**Supervision**

What are the contractor’s policies and procedures governing supervision of minors and high-risk areas? Ide-

ally, the agreement should include a provision requiring the contracting organization to have its own supervision requirements pertaining to minors and specify that failure to do so may result in termination of the agreement. Some of the key supervision areas that the contractor should address include:

- adult-to-minor ratios;
- supervision of bathroom and changing activities;
- supervision of activities associated with water use (pools, showers, bathing areas, swimming, etc.);
- supervision of overnight activities; and
- supervision during transition and free times.

**Insurance Coverage**

Which entity is going to cover the risk of loss and the cost of defense if necessary? In addition to the standard indemnity provision, request that the other organization provide a defense in the event of an incident and agree to name the university as an additional insured on its sexual abuse and molestation coverage. Recent ISO form changes affecting the availability of additional-insured coverage place greater significance on the terms contained in third-party contracts, further highlighting the need for legal counsel’s involvement in the process.

**Lesson 6: International programs that serve minors bring unique risks.**

Not all university programs that involve minors operate domestically. Some operate internationally or bring international minors to domestic university programs. Behavioral norms may differ, language barriers may impair communication, and living arrangements may introduce risks. Also, minors sometimes do things away from home that they might not otherwise do, and the university may own all of these challenges.

To overcome these challenges, universities must require well-defined policies, training, and education for everyone; strict monitoring and supervision; and clear procedures for and awareness of reporting channels. Take a closer look at any partner organizations or host families to determine the policies and procedures under which they operate.

**Conclusion**

It may seem as though abuse of a minor could never
happen on your campus—and we hope that it never does. But one incident of abuse is one too many. Implementing large-scale change takes work, and we hope these lessons and recommendations will help universities face current challenges and continue moving forward with a safer environment for everyone.

Universities cannot rely on screening, policies, training, reporting mechanisms, and other safeguards in isolation. It takes a system-wide approach. More importantly, post-2011, the entire higher-education community started a conversation about minors on campus. And while this conversation may change over time, we hope that it never stops. The protection of minors and institutional reputations depend on the continued evolution of this discussion.

About the Authors

Candace Collins works with a variety of clients to assess risk, investigate incidents, and train organizations in abuse prevention.

Prior to joining Praesidium, Collins practiced law for more than ten years, focusing on insurance and corporate defense. She also served as an Assistant Attorney General for the State of Texas, with an emphasis in consumer protection, long-term care facilities and group homes. She graduated cum laude from Texas A&M University with a degree in business management and obtained a juris doctorate from Texas Wesleyan University School of Law.

Dr. Richard Dangel holds advanced degrees from The University of Kansas and The University of Michigan. He is a doctoral level licensed child psychologist with more than 25 years of experience in abuse risk management, quality assurance, and program evaluation. Dr. Dangel has been a tenured full professor at The University of Texas at Arlington, published three books and dozens of scientific articles, and delivered more than 1,500 papers and workshops around the world.

In addition to his work at Praesidium, Dr. Dangel has served on the Editorial Board of the Journal of Child Sexual Abuse, National Research Advisory Boards of the YMCA of the USA and Father Flanagan’s Boys’ Town, and on the boards of numerous philanthropic organizations. He has also served as a consultant to Chartis, Lexington, Lloyd’s of London, The Redwoods Group, Willis, and Church Pension Group advising underwriters and claims managers about managing and underwriting abuse risk coverage in organizations. Dr. Dangel has written curriculum for more than 30 specialized online training courses on the subject of abuse prevention in organizations.

As Praesidium’s COO and Vice President of Account Services, Aaron Lundberg LMSW works with administrators and executive directors of large-scale human service organizations across the United States to develop, implement, and monitor abuse prevention policies and training programs. In addition to his work with clients, Lundberg leads Praesidium’s team of Account Managers.

Lundberg specializes in the study and prevention of sexual abuse in organizational settings. With a bachelor’s degree in psychology from Texas Tech University and a master’s degree in social work from the University of Texas at Arlington, he has conducted extensive research in the etiology, scope, and prevention of abuse in residential treatment centers. Since joining Praesidium in 2001, Lundberg has assessed, analyzed, and consulted on multiple cases of sexual abuse within a wide range of organizations. He has trained thousands of direct care workers, supervisors, administrators, and parents in preventing the sexual abuse of children and vulnerable adults.

Endnotes


