Quarterly Compliance Report – Information Compliance

This report is for information only.

BACKGROUND

In November 2015, Elizabeth Cherry, Associate Vice Provost, Compliance and Risk Services, presented a report on the University’s new Structural Compliance Program. Over an 18-month cycle, the Board of Regents will receive a quarterly report from each of the six key institution-wide compliance areas:

- Research
- Health & Safety
- Financial
- Information
- Special Areas (e.g. global activities)
- Civil Rights/Employment

Attachments
1) University of Washington Information Compliance
2) UW Information Compliance Priority Item 1: Student Information and Health or Safety Emergencies
3) UW Information Compliance Priority Item 2: Internet of Things (IoT)
University of Washington Information Compliance

Overview

American public universities have long maintained a tradition of intellectual freedom, transparency, and open access to campus facilities. In today’s world, such access includes virtual access: every student and employee carries a computer (often in the form of a smartphone) and demands connectivity to the internet and to multiple university systems and data. Institutions must now monitor both internal systems and the external environment for threats, hacks, phishing scams, and malicious software.

Universities generate, access, acquire, store, and transmit more information than ever before and have become a frequent target for cyber attackers. The consequences of data breaches can be significant, presenting serious financial, reputational and compliance risks. Government regulators demand compliance with a network of intersecting laws and regulations that pertain to security and privacy. These wide-ranging federal and state laws are constantly evolving to keep pace with technological innovation, and cover personally identifiable information (PII), protected health information (PHI), HR data, student and financial aid data, medical and research data, financial information, and public records. Examples include the Federal Information Security Management Act (FISMA) and the Health Insurance Portability and Accountability Act (HIPAA).

The administrative realities of complying with these laws and regulations require significant staffing, training, and budgetary commitments for decentralized public research institutions like the University of Washington. The sheer magnitude of the compliance challenges, and associated complexities and costs, has led universities to contract with third parties to manage or hold sensitive information. These relationships introduce still more complexity into an environment where oversight and governance of information is essential to the institution’s sound functioning.

Information compliance affects every member of the UW community – faculty, staff, students, patients, alumni – and many members of the broader public and the media as well. UW units with information compliance functions include: Office of the Chief Information Security Officer (CISO), Office of Research, Office of Public Records and Open Meetings, Records Management Services, Internal Audit, Office of the University Registrar, Enrollment Management, Human Resources, Office of Academic Personnel, and UW Medicine.

Compliance Services facilitates and supports compliance work across the institution by providing a unifying framework for the University’s diverse compliance obligations and subject matter experts. The framework is based on seven elements that characterize effective compliance programs: 1) leadership and oversight, 2) standards of conduct, policies and procedures, 3) education and outreach, 4) monitoring and auditing, 5) receiving reports and investigating, 6) accountability, incentives and corrective action, and 7) response and prevention.
Compliance Services convenes the subject matter experts for facilitated assessments designed to identify strategies or initiatives that advance the maturity of the University’s compliance functions and emphasize continuous improvement.

**Assessment**

In July 2016, assessment sessions were held with Information compliance subject matter experts representing these areas: public records and open meetings, records management, student and financial aid data, alumni and donor data, human resources data, data safety agreements and data custodians, internal audit, employee benefits, and information technology and security, among them. Through those meetings, two priority items were identified for focused attention over the next 18 months: 1) the Family Educational Rights and Privacy Act’s health or safety emergency exception, which allows disclosure of personally identifiable information from an education record if, in connection with an emergency, knowledge of the information is necessary to protect the health or safety of the student or other individuals; and, 2) a burgeoning area, known as the “Internet of Things,” that presents new compliance challenges with regard to data security and privacy.

**The Information compliance assessment was led by:**

Kirk Bailey | Associate Vice President and Chief Information Security Officer, Office of the CISO
Elizabeth Cherry | Associate Vice Provost, Compliance and Risk Services
Sue Clausen | Chief Compliance Officer, UW Medicine, and Associate Vice President for Medical Affairs, UW

**Subject matter experts:**

David M. Anderson | Executive Director, Health Sciences Administration
Barbara Benson | Director and University Records Officer, Records Management Services
Chuck Benson | Assistant Director, Facilities Services
Richard Cordova | Executive Director, Internal Audit
Elizabeth Coveney | Associate Vice President, HR Administration and Information Systems, Human Resources
Laura Dorsey | Senior Technology Manager, Engineering and Sciences, CoMotion
Walt Dryfoos | Associate Vice President, University Advancement
Katy Dwyer | Executive Director, Benefits, Human Resources
Cris Ewell | Chief Information Security Officer, UW Medicine
Helen B. Garrett | University Registrar and Chief Officer of Enrollment Information Services, Office of the University Registrar
Joe Giffels | Associate Vice Provost for Research Administration and Integrity, Office of Research
Kay Lewis | Assistant Vice President for Enrollment and Executive Director of Financial Aid and Scholarships
Jackie Mynarski | Associate Athletic Director, Compliance, Intercollegiate Athletics
Ann Nagel | Director and Associate CISO, Office of the Chief Information Security Officer
Lori Oliver | Director of Legal and Business Affairs, UW Medicine and Associate Vice President for Medical Affairs, UW
Summary of Priority Items

Priority Item 1: Student Information and Health or Safety Emergencies
The Family Educational Rights and Privacy Act (FERPA) generally prohibits colleges and universities from disclosing personally identifiable information about a student from education records without the student’s consent. However, FERPA does provide a number of exceptions when disclosure may be permitted even without a student’s consent. One example is in connection with a health or safety emergency, e.g. when a student may be a threat to her/himself, or a threat to others. An institution’s failure to provide appropriate warning about a student who poses a danger can have significant legal and, more importantly, safety ramifications.

Student Life and the Office of the University Registrar will lead an effort to establish clear criteria and procedures for releasing student information in connection with a health or safety emergency, and to review existing University policies to determine appropriate alignment with federal and state laws and regulations.

Priority Item 2: Internet of Things (IoT)
Complex industrial control systems (an aspect of the Internet of Things, or IoT) that collect and share data using sensors, software and the internet are found across campus. These systems control building access, power, lights, water, networked printers, heating/ventilation/air conditioning (HVAC), and more. Due to their reliance on connectivity, they introduce vulnerabilities into existing data security and privacy management mechanisms. This can affect the University’s ability to control access to data, protect health and safety, and ensure compliance with information security and privacy laws and regulations.

To better manage IoT, University stakeholders will: recommend that ongoing, institution-wide IoT oversight be established; identify and mitigate vulnerabilities in existing technologies in use across campus; establish a strategic framework to guide operational decision-making for new buildings or renovation projects; and encourage awareness of and compliance with laws and regulations.

Additional Reading

University of Washington Information Compliance

Priority Item 1: **Student Information and Health or Safety Emergencies**

**Challenge Statement**

The Family Educational Rights and Privacy Act (FERPA) generally prohibits colleges and universities from disclosing personally identifiable information about a student – except for designated “directory information,” which includes physical and email address, phone number, dates of attendance, date of birth, and other personal and academic information – without the student’s consent. However, when a student is a threat to her/himself, or a threat to others, an institution may disclose personally identifiable information from an education record of a student without the student’s consent, if the information is necessary to protect the health or safety of the student or others. An institution’s failure to provide appropriate warning about a student who poses a danger can have significant legal and, more importantly, safety ramifications.

**Context**

FERPA is a federal privacy law that protects students’ education records, as well as personally identifiable information contained in such records. An education record is any record, regardless of its format, that is directly related to a student and maintained by the institution or by a party acting on behalf of the institution.

Student information is available and accessible to many faculty and staff across the institution, all of whom must be made aware of FERPA protections regarding education records that contain such information. Training and education on safeguarding student information, and the circumstances under which it can be released (for example, at the request of the student or in response to a subpoena or public records request), is routinely provided to UW departments and schools.

There is less awareness, however, with regard to FERPA’s health or safety emergency exception, which permits disclosures without student consent when necessary to protect the health or safety of the student or others in an emergency. In the case of an articulable and significant threat, a school official may release student information from the education record to appropriate parties in order to protect the welfare of the student or other individuals. This exception to FERPA’s consent requirement is limited to the period of the emergency and only extends to information needed in connection with the emergency. It does not allow for a blanket release of personally identifiable information from a student’s education record.

**Mitigation Plan**

Working together, Student Life and the Office of the University Registrar will lead an effort to:

- Establish clear criteria and procedures for releasing student information related to a health or safety emergency, including documenting the articulable and significant threat that formed the basis for the disclosure, and the parties to whom the information was disclosed.
- Coordinate with offices that identify and assess students of concern, and those that provide mental or physical safety support services, including SafeCampus, Health & Wellness, Counseling

ATTACHMENT 2
Center, Disability Resources for Students (DRS), Youth Programs Development and Support, Housing & Food Services, and others.

- Review existing University policies to determine appropriate alignment with federal and state laws and regulations regarding the disclosure of student information in connection with a health or safety emergency.

Project Leads
Helen B. Garrett | University Registrar and Chief Officer of Enrollment Information Services, Office of the University Registrar
Ellen B. Taylor | Associate Vice President for Student Life

Relevant Laws and Regulations

Federal

State
- Mental Illness (Exemptions from liability): Chapter 71.05.120 RCW
- Medical Records – Healthcare Information Access and Disclosure (Mental health services, confidentiality of records – Permitted disclosures): Chapter 70.02.230 RCW; see also Chapter 70.02.050(1)(c).
University of Washington Information Compliance

Priority Item 2: Internet of Things (IoT)

**Challenge Statement**

Complex industrial control systems that collect and share data using sensors, software and the internet are found across campus. These systems control building access, power, lights, water, networked printers, heating/ventilation/air conditioning (HVAC), and more. Due to their reliance on connectivity, these systems may introduce weakness into the institution’s existing data security and privacy management mechanisms. As a result, individuals with bad intent who are able to compromise industrial control systems can gain access to other UW information systems and data. Vulnerabilities in these systems can affect the institution’s ability to control access to data, protect health and safety, and ensure compliance with information security and privacy laws and regulations.

**Context**

Internet of Things (IoT) refers not only to industrial control systems, but also to vehicles, machines and devices that collect, send and exchange data via the internet. IoT can support efficiency and innovation in public safety, healthcare, research, and teaching and learning. However, if these complex systems are not implemented with caution and careful planning, the return on investments in IoT functions may not be realized, and exposure to cyber-related risk can increase significantly. Technology is advancing at a very fast rate and being integrated into University buildings and operations without a standardized approach or plan for evaluation, selection, implementation, maintenance, and monitoring.

Decisions about use of technology and vendors for industrial control systems are being made independently by administrative and academic units across campus, but impacts to the institution as a whole are significant. For example, a new building with multiple IoT systems has implications that affect Capital Planning and Development, Information Technology (IT), Facilities Services, as well as multiple end-user departments. Each new system that connects to existing University infrastructure, especially those maintained by third-party vendors, potentially creates a new point of vulnerability.

IoT is a major concern, not only for the UW and other universities across the country, but also for private industry. Regulators have taken note. The Federal Trade Commission (FTC) released a report in January 2015, titled *Internet of Things: Privacy and Security in a Connected World*, which identifies potential security and safety risks related to IoT. Numerous regulations that mandate data security and breach notification already exist; additional laws and regulations responding to IoT-related issues may be forthcoming.

**Mitigation Plan**

There is no single, comprehensive solution to address IoT-related concerns, and avoidance of IoT systems is not practicable. Risks can be mitigated, however, with a coordinated approach to selection, procurement, installation and maintenance of these systems. To that end, key stakeholders will:
• Recommend that ongoing, institution-wide IoT oversight be integrated into an existing governance group like the Privacy Assurance and Systems Security (PASS) Council or the Information Security and Privacy Board (ISPB). The IoT oversight group will:
  o Acquire a clear understanding of technologies currently in use across campus.
  o Develop a plan to mitigate vulnerabilities in existing systems, establish a strategic framework to guide operational decision-making for new buildings or renovation projects, and encourage awareness of and compliance with laws and regulations.
  o Identify ownership of and responsibility for IoT systems throughout their lifecycle, with a particular focus on those that span multiple units and departments, and those managed by third-party vendors.
  o Include representatives from Facilities Services, UW-IT (central and local), Capital Planning and Development, Office of Planning and Management, Procurement Services, end-user groups, and others to be determined.

Project Leads
Kirk Bailey | Associate Vice President and Chief Information Security Officer, Office of the CISO
Chuck Benson | Assistant Director, Facilities Services

Sample of Relevant Laws and Regulations
Federal

State
• Personal Information – Notice of Security Breaches (Public Records Act): Chapter 42.56.590 RCW