CRR: Information Security: Acceptable Use

Compliance Risk Areas

Compliance Risk Areas	Related Governing Laws, Rules, Regulations, or University Policies
• General Compliance with Policies	• Administrative Policy: Internal Access to and Sharing University Information • Administrative Policy: Reporting and Notifying Individuals of Information Security Breaches • Administrative Policy: Information Security Risk Management • Administrative Policy: Information Security • Administrative Policy: Data Security Classification • Administrative Policy: Acceptable Use of Information Technology Resources
• Administrative Safeguards	• Health Insurance Portability and Accountability Act (HIPAA) • Gramm-Leach Bliley Act (GLBA) • Family Educational Rights and Privacy Act (FERPA) • Payment Card Industry Data Industry Standard (PCI DSS)
• Physical Safeguards	• HIPAA

	• GLBA • FERPA • PCI DSS
• Technical Safeguards	• HIPAA • GLBA • FERPA • PCI DSS
• Risk Management Framework and Assessments	• Federal Information Security Management Act (FISMA) • HIPAA • GLBA
• Business Associates/Vendors	• HIPAA • GLBA • PCI DSS
• Information Security Breaches and Security Incidents	• HIPAA • GLBA • FERPA • PCI DSS
• Acceptable Use	• Electronic Communications Privacy Act • Digital Millennium Copyright Act

Cost of Compliance Measurement Questions

1. How many full-time employees (FTEs) are dedicated to compliance-related activities in this area?

2. What is spent annually, on average, to perform the compliance-related activities conducted by Information Security? Please include only those items that require the purchase or goods or services from an outside entity such as outside consulting services, equipment purchases, non-routine supplies, or fees.
3. Please list all training required to maintain University compliance in this subject area. For each training requirement:
    a. Identify the primary source of the requirement as (1) federal or state law, (2) administrative regulations, or (3) University policy. (e.g., Conflict of Interest training is required under federal code of federal regulations for investigators conducting research funded by a Public health Service agency)
    b. Identify category (ies) of employees (e.g., faculty, P&A, etc.) required to take the training.
    c. Estimate the number of employees in each category required to take the training.
    d. Identify the frequency (e.g., quarterly, annually) and the length of the training (e.g., 1.5 hours).
4. Estimate the number of employees system-wide who are subject to the compliance requirements in this area.
5. Excluding time required to meet training requirements addressed in Question 3 above, please estimate the time required annually for these employees to comply with other compliance requirements (e.g., record keeping, monitoring, testing, reporting).

General Policy and Procedure questions

1. Who is the Security officer in charge of Information Security?
2. Is the following a complete list of University policies on Information Security:
    a. Administrative Policy: Internal Access to and Sharing University Information
    b. Administrative Policy: Reporting and Notifying Individuals of Information Security Breaches
    c. Administrative Policy: Information Security Risk Management
    d. Administrative Policy: Information Security
    e. Administrative Policy: Data Security Classification

f. Administrative Policy: Acceptable Use of Information Technology Resources

3. Has the University granted any exceptions to the Information Security policies?
4. Do these policies (and corresponding information security program) meet the administrative, technical, and physical safeguards requirements of HIPAA and GLBA?
5. Describe or attach the sanctions policy or process against workforce members who fail to comply with information security policies and procedures.
6. Has Information Security received any Audit findings in the past three years? Were those findings addressed?

Administrative Safeguards

1. Does the University have a policy and procedure in place to ensure that all workforce members have appropriate access to electronic protected health information (PHI)?
2. How often does the University conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (PHI) held by the parts of the University that are considered a "covered entity" under HIPAA?
    a. Describe the process for identifying risks and vulnerabilities and how the University adopts security measures to address them.
    b. Describe or attach the procedures implemented to regularly review records of information system activity.
3. Does the University perform periodic technical and nontechnical evaluations, based initially upon the standards implemented under the HIPAA rule and, subsequently, in response to environmental or operational changes affecting the security of electronic PHI?
4. Describe the University procedure for disposing customer information and PHI in an appropriate way.

Physical Safeguards

1. Describe the policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surrounding of a specific workstation or class of workstation that can access electronic PHI.

2. Describe the physical safeguards for all workstations that access electronic PHI or other private – highly restricted data to restrict access to authorized users.
3. Does the University keep an inventory of all authorized and unauthorized devices?
    a. Does the University periodically conduct audits of the inventory?
    b. Does the University security test and configure new devices before placing them onto a University network?
4. Does the University keep a list of units that are significantly engaged in financial activities that involve the collection or utilization of customer financial information?
    a. Where is the sensitive customer information stored?
    b. Who has access to the customer information?
5. Describe University procedures for the receipt and removal of hardware and electronic media that contain electronic PHI or other private – highly restricted data?
    a. What is the process for final disposition of this data and/or the hardware of electronic media in which it is stored?
    b. What is the process for removal of this data from the media before the media is available for re-use?

Technical Safeguards

1. Describe the hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.
2. Has the University implemented procedures to protect electronic PHI from improper alteration or destruction?
3. Has the University implemented procedures to verify that a person or entity seeking access to electronic PHI is the one claimed?
4. Has the University implemented technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network?
5. What steps does the University take to ensure the secure transmission of customer information to comply with GLBA and PCI DSS?
6. Describe the firewalls or other mechanisms that the University employs to protect its

network.

Risk Management Framework and Risk Assessments

1. Has the University implemented the 6-step NIST framework developed as part of FISMA?
    a. What is the process for determining information security categorization?
    b. Once a category is determined, what is the process for selecting baseline security controls?
    c. What is the process for implementing the security controls?
2. Describe the University's process to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity. Does the process include consideration of risks that include:
    a. Employee training and management;
    b. information systems, including network and software design, as well as information processing, storage, transmission and disposal;
    c. detecting, preventing and responding to attacks, intrusions or other systems failures
3. Describe the University's process to design and implement information safeguards to control the risks that the University identifies through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
4. Describe the University's process to evaluate and adjust the information security program in light of the results of testing and monitoring; any material changes to operations or business arrangements; or any other circumstances.

Business Associates and Vendors

1. What steps does the University take in requiring service providers to implement and maintain safeguards to meet GLBA and/or PCI DSS?
2. What steps does the University take in requiring business associates to comply with HIPAA standards?

Breaches and Security Incidents

1. Attach or describe the University's policies and procedures for dealing with breaches and security incidents.
2. How many breaches are reported to Information Security annually on average?
3. Does the University employ oversight and/or audit procedures to detect improper disclosure or theft of customer information?
4. Describe the University's vulnerability scanning process to discover new vulnerabilities.

Acceptable Use

1. Describe the training process for University employees to comply with the University's Acceptable Use of Information Technology Resources policy.
2. Does the University conduct regular checks and trainings to ensure employee understanding of Acceptable Use after the initial training? Describe this process.
3. How many reports of copyright infringement has Information Security received over the past year? How were those reports resolved?
4. Describe the security controls in place for information technology resources used for University business.
5. How does Information Security monitor compliance with the Acceptable Use policy?
6. Does the University have a policy or otherwise monitor employees who telecommute?