Message from the University's Privacy Officer

HIPAA Best Practices and New FERPA Policy

In September and October 2024, the U.S. Department of Health and Human Services – Office for Civil Rights announced multiple civil penalties in excess of $200,000 against medical providers in connection with ransomware attacks and alleged violations of the HIPAA Security Rule. The settlements highlight the importance of safeguarding electronic personal health information and serve as an opportunity to remind our University community about HIPAA at Pitt and the importance of student privacy.

Statistically, ransomware and hacking are the primary cyber-threats in health care. Since 2018, there has been a 264% increase in large breaches reported to OCR involving ransomware attacks. A review of recent ransomware attacks prompted OCR to issue recommendations and best practices reminders. The good news is that Pitt is in step with these recommendations. Next to each reminder, the Privacy Office has included a link or references to available University services and resources.

- Review all vendor and contractor relationships to ensure business associate agreements are in place as appropriate and address breach/security incident obligations. On an ongoing basis, the Privacy Office collects Business Associate Agreements and reviews them annual to ensure that they address obligations in the event of a breach or security incident.
- Integrate risk analysis and risk management into business processes; conducted regularly and when new technologies and business operations are planned. Our Office of Risk Management and Pitt IT Security help to ensure that departments and units across the University integrate risk analysis and complete vendor security risk assessment for new technologies and operations.
- Pitt IT Security ensures that audit controls are in place to record and examine information system activity.
- Implement regular review of information system activity. Pitt IT Security conducts ongoing monitoring of all system activity under its control.
- Duo Multifactor Authentication ensures that only authorized users are accessing ePHI.

- Encrypt ePHI to guard against unauthorized access to ePHI. Pitt's covered components encrypt ePHI (more on this below).
- Incorporate lessons learned from incidents into the overall security management process.
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security. All new Pitt employees are required to complete security awareness training and our PHI workforce members and covered components annually receive additional training in privacy and security.

HIPAA at Pitt

The University is considered a Hybrid Entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As a Hybrid Entity, the University Privacy Officer routinely identifies specific units to be Covered Components required to meet specific privacy and security standards under HIPAA in the delivery of health care, paying for health care, and providing operational support for health care services. Pitt's Covered Components include Student Health Services, the School of Dental Medicine, the University Dental Clinic, and the University Health Plan. The University's HIPAA Policy and Procedure offer more details about the University's compliance with HIPAA.

The Intersection of HIPAA and FERPA

As an institution of higher education, the Family Educational Rights and Privacy Act (FERPA) impacts our students, staff, and faculty on a daily basis and generally applies to students more broadly than HIPAA. FERPA is more protective of student-privacy as it broadly defines education and treatment records and generally requires written consent of the student before disclosure may be made.

In April of 2024, the University updated it FERPA Policy and Procedure. The Privacy Office is working with the University Registrar to establish a comprehensive FERPA compliance program, which will include annual training for all staff and faculty. Existing resources and forms can be found on the University Registrar's FERPA page. As we work to update FERPA compliance practices, please do not hesitate to contact the Privacy Office at compliance@pitt.edu with any questions or concerns. In addition, the Pitt Concern Connection can be used to report unauthorized disclosure of confidential information and other privacy concerns.

Thank you for your cooperation and commitment to protecting the privacy and security of our University community.

Laurel Gift
University Privacy Officer