V.J. POLICY ON SECURITY OF ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

(Source: For Comment, Vice President for Information Systems and Computing, Almanac, February 22, 2005; approved, Almanac, April 5, 2005 *(*https://almanac.upenn.edu/archive/volumes/v51/n27/OR-phi.html*))*

HIPAA is a federal law that, among other things, focuses on protecting the privacy and security of personal health information (protected health information or PHI). This law affords certain rights to individuals regarding their PHI and imposes obligations upon many institutions that maintain such PHI. At Penn, the following entities are responsible for compliance with HIPAA privacy and security regulations: the University of Pennsylvania Health System (UPHS), the Perelman School of Medicine, the School of Dental Medicine, the Living Independently For Elders (LIFE) program, Student Health Services, and the Employee Health Benefits Plan, as well as workforce members of other Penn offices that, while offering support to these entities, access PHI (workforce members pertains to anyone assessing ePHI working with the University of Pennsylvania's Covered Components and their Shared SupportServices as an employee, volunteer, student or faculty member.).

While inextricably linked, the HIPAA security regulation is distinguished from the HIPAA privacy regulation in that it applies to electronic storage and transmission of PHI (ePHI), compared with the privacy regulation that applies to all forms of PHI and prescribes more detailed requirements for securing such data.

The ePHI security policy outlines minimum standards for ensuring the confidentiality, integrity, and availability of electronic protected health information received, maintained or transmitted by all University HIPAA Covered Components (those schools and units listed above), as well as other offices which support these entities, listed below as Support Services. Covered Components shall meet or exceed these standards by implementing the necessary administrative, physical or technical safeguards as appropriate based on their assessments of risk. Compliance by Support Services with these standards is limited to activities that directly involve the creation or receipt of ePHI in support of Covered Components and does not pertain to activities related to services provided to non-covered areas of the University.

Support Services include:

- Office of Regulatory Affairs
- Institutional Review Board (eight review boards)
- Office of General Counsel
- Office of Audit and Compliance
- University Archives and Records Center
- Office of Environmental Health and Radiation Services
- Office of Risk Management and Insurance
- Office of the President
- Office of the Provost
- Office of the Executive Vice President
- Office of Student Financial Services
- Office of Development and Alumni Relations
- Office of the Comptroller
- Office of Information Systems and Computing
- School of Nursing Office of Technology and Information Systems, Center for
- Nursing Research, and Office of Business and Finance
- VPUL Technical Support

Exclusions

Certain data is specifically excluded from coverage under HIPAA, most importantly:

1. Student records, except for student patient data maintained at Student Health Service;
2. Employment records, except for health benefits records; and
3. Information "de-identified" under HIPAA standards.

Exceptions

Exceptions to this policy must be documented and submitted for approval to the University Information Security Officer who shall consult with the Office of General Counsel. Appeals of decisions shall be referred to the Vice President of Information Services and Computing.

For a description of the administrative, physical and technical safeguards that should be undertaken, a definition of various terms used in the policy and a list of related policies, see page 4 - Almanac, February 22, 2005 (https://almanac.upenn.edu/archive/volumes/v51/n22/pdf_n22/022205.pdf).