Perelman School of Medicine at the University of Pennsylvania
Policy & Procedure Manual

Data Protection Policy – Storage and Transmission of PHI and Other Personally Identifiable Information

ACADEMIC COMPUTING
Policy Number: ACADCOMP-001
Date Approved: 2/3/2017

I. PURPOSE

The purpose of this policy is to ensure that HIPAA "protected health information" or "PHI" and other personally identifiable information ("PII") is protected in storage and transmission by appropriate safeguards.

II. SCOPE

This policy applies to all PHI and other PII used by members of the PSOM workforce including faculty, staff, researchers, students, and collaborators internal to the University of Pennsylvania. Requirements equivalent to those below should also apply to external collaborators working with PSOM's PHI or other PII through agreements and/or other conditions of collaboration.

III. POLICY

Data Storage

PHI and other personally identifiable information must be stored using one of the following mechanisms:

- Institutionally secured and managed network drive
- Institutionally secured and managed encrypted device
- Institutionally approved third-party computing environment

If compliance with the above policy statement is not possible, an exception may be granted based on business need and as approved by an information security professional within Penn Medicine Information Services.[1]

[1] In the Perelman School of Medicine, Penn Medicine Academic Computing Services ("PMACS") is the recognized arm of Penn Medicine Information Services.

Transmission/Temporary Storage:

All transmission of PHI and other personally identifiable information must be performed using one of the following:

- Use of encrypted portable drive
- Via a secure encrypted file transfer

Transmission mechanisms noted above must use a Penn Medicine Information Services authorized encryption solution.

Please Note: E-mail is often not secure and can be easily misdirected. Make all efforts to reduce the sensitivity of information shared via e-mail.

IV. DEFINITIONS

Institutionally Secured and Managed Network Drive:

A network drive/departmental file share that is secured and managed by a regular, full-time Penn Medicine staff member with a designated IT position within Penn Medicine Information Services.

Institutionally Secured and Managed Device:

A physical device including a laptop, desktop, tablet, phone, or other electronic device that is secured and managed by Penn Medicine Information Services in accordance with applicable regulations and institutional requirements for storage of electronic protected health information. At a minimum, these devices must be encrypted.

Institutionally approved third-party computing environment:

A third-party computing environment, such as a cloud services provider, that has been institutionally reviewed and approved. Such approval may be conditioned on the existence of contractual agreements and a security review to ensure appropriate protections.

Protected Health Information (PHI)

Information that is created or received by UPHS and relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient; and that

identifies the patient or for which there is a reasonable basis to believe the information can be used to identify the patient. PHI includes information of persons living or deceased. The following components of a patient's information also are considered PHI: a) names; b) street address, city, county, precinct, zip code; c) dates directly related to a patient, including birth date, admission date, discharge date, and date of death; d) telephone numbers, fax numbers, and electronic mail addresses; e) Social Security numbers; f) medical record numbers; g) health plan beneficiary numbers; h) account numbers; i) certificate/license numbers; j) vehicle identifiers and serial numbers, including license plate numbers; k) device identifiers and serial numbers; l) Web Universal Resource Locators (URLs); m) biometric identifiers, including finger and voice prints; n) full face photographic images and any comparable images; and o) any other unique identifying number, characteristic, or code.

Personally Identifiable Information

Information that can be used, alone or in combination with other available information, to identify an individual.

V. WHO SHOULD KNOW THIS POLICY?

- Department Chairs and Directors of Centers and Institutes
- Department, Center, and Institute Business Administrators
- Perelman School of Medicine Faculty, Staff, Students and other affiliates
- Dean's Staff
- Health System Administrators

VI. CONTACTS

Dean, Perelman School of Medicine
Phone: (215) 898-6796
FAX: (215) 573-2030
Vice Dean, Administration and Finance, Perelman School of Medicine
Phone: (215) 898-3655
FAX: (215) 898-0994
Associate CIO of Technology & Infrastructure, Penn Medicine
Phone:
(215) 614-0271 (Office)
(215) 349-8442 (Fax)

Data Protection Policy – Storage and Transmission of PHI and Other Personally Identifiable Information	ISSUED BY: Kathy Jameson 2/3/17 Dean, Perelman School of Medicine Date