POLICY
It is the policy of the University of Pennsylvania Health System (UPHS) to provide notification of any Breaches of Unsecured PHI in accordance with the requirements of the federal HITECH Act.

PURPOSE
The purpose of this policy is to describe steps that must be taken in the event of a Breach of Unsecured PHI, including providing notification of such Breach to:

- Each patient whose Unsecured PHI has been, or is reasonably believed to have been, Breached;
- The Secretary of the U.S. Department of Health and Human Services ("HHS"); and
- Prominent media outlets serving the state or jurisdiction if the Breach involves more than 500 residents of such state or jurisdiction

SCOPE
This policy is applicable to all components and entities of UPHS including but not limited to: the Hospital of the University of Pennsylvania ((HUP); an unincorporated operating division of The Trustees of the University of Pennsylvania (Trustees)); Radnor Surgery Center, a facility of HUP; Presbyterian Medical Center of the University of Pennsylvania Health System d.b.a. Penn Presbyterian Medical Center (PPMC); the Penn Digestive and Liver Health Center University city (PDLH), a facility of PPMC; The Pennsylvania Hospital of the University of Pennsylvania Health System (PAH); Chester County Hospital; Chester County Health and Hospital System; Wissahickon Hospice d.b.a Penn Care at Home; Clinical Practices of the University of Pennsylvania (CPUP); Clinical Care Associates; Clinical Health Care Associates of New Jersey, P.C., the Hospital of the University of Pennsylvania Reproductive Surgical Facility; Lancaster General Health (LG Health), Lancaster General Hospital (LGH), and Lancaster General Hospital Ambulatory Surgical Facility (LGHASF); Princeton Health; the Surgery Center of Pennsylvania Hospital; the Endoscopy Center of Pennsylvania Hospital; the Surgery Center at Penn Medicine University City, a facility of Penn Presbyterian Medical Center; all ambulatory care facilities (ACF) that are off campus departments of PPMC operating in New Jersey, and all divisions, facilities and entities within UPHS that have a CMS Certification Number (CCN) or that are operating under the license of a UPHS entity (collectively the "Entities") excluding the Perelman School of Medicine (PSOM) except where specifically noted.

This policy applies to all Breaches of unsecured PHI at UPHS.

IMPLEMENTATION
The responsibility for implementation of this policy rests with the UPHS Privacy Office

DEFINITIONS
Breach means access to PHI or the acquisition, use, or disclosure of PHI in a manner that is not permitted by HIPAA, unless a risk assessment demonstrates a low probability that the PHI was compromised.

Protected Health Information (PHI) is 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.

Unsecured PHI means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services. PHI that has been encrypted in keeping with UPHS Information Security standards is secured.

PROCEDURE

REPORTING AN ACTUAL OR SUSPECTED USE OR DISCLOSURE OF PHI

All UPHS staff, students, faculty, trainees, and volunteers are required to report any actual or suspected use or disclosure of PHI believed to be in violation of the HIPAA Privacy Rules to the UPHS Privacy Office.

DETERMINING WHETHER A BREACH OF UNSECURED PHI OCCURRED

Upon receiving a report of any actual or suspected unauthorized use or disclosure of PHI, the UPHS Privacy Office, in conjunction with the Entity Privacy Officer, the Office of General Counsel, and Information Security, when applicable, shall investigate the incident to determine if the incident resulted in a Breach of Unsecured PHI. Such investigation shall include a documented risk assessment that supports the final determination.

PROCEDURE IF A BREACH OF UNSECURED PHI OCCURRED

If it is determined that a Breach of Unsecured PHI occurred, UPHS shall provide notice of the Breach and maintain documentation of such notice as follows:

1. Notice to Patient

Written notice of Breach shall be provided to each patient whose Unsecured PHI has been Breached, or is reasonably believed to have been Breached, as follows:

- **Timing of Notice.** The notice shall be provided promptly and no later than sixty (60) days after discovery of the Breach. The Breach is considered to be discovered on the first day on which the Breach is known, or would have been known by exercising reasonable diligence to any person who is a Workforce Member or agent of UPHS (other than the person committing the Breach).
- **Manner of Notice.** The notice shall be sent by first-class mail addressed to the patient's last known address. Notice may be sent electronically if the patient has agreed to receive electronic notice and the agreement has not been withdrawn. If UPHS knows that the patient is deceased, UPHS shall provide written notice to the next-of-kin or personal representative of such patient if UPHS has the addresses

of those individuals. Notice may be provided in one or more mailings as additional information becomes available.

- **Content of Notice.** The notice shall be written in plain language and shall contain the following information: (A) a brief description of the incident, including the date of the Breach and the date of the discovery of the Breach if known, (B) a description of the types of Unsecured PHI involved in the Breach (rather than a description of the specific PHI), (C) any steps the patient should take to protect himself or herself from harm resulting from the Breach, (D) a brief description of what UPHS is doing to investigate the Breach, to mitigate the harm to the patient and to protect against future occurrences, and (E) contact procedures for the patient to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address.
- **Substitute Notice.** If there is insufficient or out-of-date contact information for a patient that precludes written notice to such patient, as soon as reasonably possible after such determination, UPHS shall provide notice reasonably calculated to reach the patient as described below. A. If there is insufficient or out-of-date contact information for fewer than ten (10) patients, notice may be provided by e-mail, telephone or other means. B. If there is insufficient or out-of-date contact information for ten (10) or more patients, notice shall (1) be in the form of either a conspicuous posting for ninety (90) days on UPHS's website home page or conspicuous notice in major print or broadcast media in geographic areas where the affected patients likely reside, and (2) include a toll-free number that remains active for at least ninety (90) days so that the patient can learn whether his or her Unsecured PHI was included in the Breach. C. Substitute notice need not be provided if the affected patient is deceased and UPHS has insufficient or out-of-date contact information for the next of kin or personal representative of the patient.
- **Additional Notice in Urgent Situations.** If UPHS determines there is potential for imminent misuse of the Unsecured PHI in connection with a Breach, UPHS may provide information regarding the Breach to patients by telephone or other means, as appropriate, in addition to providing the required written notice as described above.

2. Notice to HHS

In addition to notifying the patient as described above, UPHS also shall notify HHS of the Breach of Unsecured PHI. Such notification shall be provided as follows: (i) If the Breach involves 500 or more patients, UPHS shall notify HHS of the Breach contemporaneously with providing the notice to the patient and in a manner specified by HHS on its website. (ii) If the Breach involves less than 500 patients, UPHS shall maintain a log or similar documentation of the Breach and shall provide the required documentation to HHS no later than sixty (60) days after the end of each calendar year in the manner specified by HHS on its website.

3. Notice to Media

Unless contrary instructions from law enforcement are received (see Section 5(d) below), if a Breach involves more than 500 residents of a state or jurisdiction, in addition to notifying the patient and HHS, UPHS also shall notify prominent media outlets serving the state or jurisdiction. Such notice shall be provided promptly

and in no case later than sixty (60) calendar days after discovery of the Breach. The notice shall contain the same information included in the notice to the patient.

4. Law Enforcement Delay

If a law enforcement official informs UPHS that the notice to patients, HHS or the media described above would impede a criminal investigation or cause damage to national security, UPHS shall:

- If the statement is in writing and specifies the time for which a delay is required, delay the notification for the specified time; or
- If the statement is made orally, document the statement, including the identity of the official, and delay the notification for no longer than thirty (30) days from the date of the oral statement, unless during that thirty (30) day time period, the official provides a written statement requiring a different notification timeframe.

DOCUMENTATION OF BREACH NOTICE

UPHS shall maintain the documentation related to the provision of notice to patients, HHS, the media, if applicable, and any communication from law enforcement related to the delayed notification, if applicable, for at least six (6) years from the date notice was provided.

STATE LAW

If the laws of the state(s) in which the applicable UPHS entity operates have more stringent requirements than those set forth in this policy, UPHS will comply with the most restrictive applicable law, statute, or regulation.

SUPERSEDES:	ISSUED BY: Lauren Steinfeld Lauren B. Steinfeld Assistant Vice President, Audit, Compliance and Privacy Chief Privacy Officer, Penn Medicine