	<b>Title:</b> HIPAA - Responding to Breaches of Protected Health Information (PHI) Policy	<b>Review Frequency:</b> Annual	<b>Effective Date:</b> 03/22/2017
	<b>Document Category / Document Type</b> Cascaded / Policy	Doc Control No.	HS-313
		Revision Letter/No.	1

### 1.0 Purpose/Objectives.

It is the purpose of this Breach notification policy to provide guidance when an unauthorized or prohibited acquisition, access, use, or disclosure of unsecured protected health information ("PHI") occurs. This policy sets forth the University of New Mexico Health Sciences Center ("UNMHSC") Breach notification requirements in accordance with the Health Information Technology for Economic and Clinical Health ("HITECH") Act and its related regulations, "Breach Notification for Unsecured Protected Health Information."

The American Recovery and Reinvestment Act of 2009 ("ARRA") was signed into law on February 17, 2009. Title XIII of ARRA the HITECH Act. The HITECH Act in conjunction with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and their related regulations promulgated by the U.S. Department of Health and Human Services ("HHS") mandate that any form of individually identifiable health information be safeguarded appropriately so as to remain private and secure. When there is unauthorized acquisition, access, use, or disclosure of protected health information that has not been secured through technology or methodology specified by the Secretary for HHS, the UNMHSC is required to fulfill certain Breach notification requirements. The Breach of Unsecured Protected Health Information Regulation became effective September 23, 2009.

### 2.0 Scope.

This policy applies to All Health Sciences faculty and staff regardless of their department, unit, clinic, and college or facility affiliation. Health Sciences cascaded policies shall be sent to Health Sciences Components for their respective adoption, dissemination and implementation.

All UNMHSC workforce members and all workforce members of health care components of UNM that are under the jurisdiction of the HSC as designated in the UNM Board of Regents' Policy Manual, No. 3.8, "Institutional HIPAA Compliance Program".

### 3.0 Content.

- A. **Breach of Unsecured Protected Health Information:** A Breach of PHI means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.
- B. **Discovery of Breach:** A Breach of PHI or potential Breach of PHI shall be treated as discovered by the UNMHSC as of the first day the Breach is known to the UNMHSC or by exercising reasonable diligence would have been known to the UNMHSC. This includes Breaches by Business Associates of the UNMHSC.
  - 1. The UNMHSC shall be deemed to have knowledge of a Breach if such Breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or Business Associate of the UNMHSC.
  - 2. Following discovery of a potential Breach, the UNMHSC shall begin an investigation.
- C. **Breaches and Notification:** The UNMHSC is committed to the prevention of Breaches with respect to PHI. Suspected Breaches of unsecured PHI will be reviewed and assessed by the

HIPAA Privacy Officer and/or HIPAA Security Officer and other appropriate UNMHSC Officials (including, for example, the Office of University Counsel, UNMH IT Security, and Human Resources). The purpose of the assessment will be to determine the likelihood of "harm" (pursuant to HIPAA) arising from the actual or suspected Breach. The results of the assessment will be used to determine the actions to be taken in response to the actual or suspected Breach.

1. Internal Notification: Any UNMHSC workforce member who becomes aware of a suspected or actual Breach must immediately notify his or her supervisor, who must immediately notify the following officials: the HIPAA Privacy Officer and the HIPAA Security Officer. See Section 7 for Internal References and contact information.
2. Breach by Business Associate: In the event that a Business Associate becomes aware of a potential Breach, the Business Associate immediately must notify the office and official of the UNMHSC with whom the Business Associate contracted to perform the contracted service. The contacted UNMHSC official must then immediately notify the HIPAA Privacy Officer and the HIPAA Security Officer.
3. External Notification:
  - a. Required Notification to Affected Individuals: In the case of a Breach of unsecured PHI that is discovered by the UNMHSC, the UNMHSC shall notify each individual whose unsecured PHI has been or reasonably believed to have been acquired, accessed, used, or disclosed as a result of the Breach. The Privacy Officer shall be responsible for drafting the notification letter to each of the individuals identified as having been affected by a Breach, and all information related to the Breach necessary for drafting the notifications shall be made available to the Privacy Officer. Without unreasonable delay, but in no case later than sixty (60) calendar days after discovery of the Breach, the UNMHSC, through the appropriate office, shall take the following actions:
    - (i) Notice to Affected Individuals: Notify affected individuals (or next of kin if deceased) in writing by first class mail at the last known address of the affected individual (or by electronic communication if so indicated by the individual's the preferred method of communication) of the following information:
      - a) A brief description of the Breach, including the date of the Breach and the date of discovery;
      - b) A description of the types of PHI that were involved in the Breach;
      - c) Steps that individuals should take to protect themselves from potential harm resulting from the Breach;
      - d) A brief description of the UNMHSC's remedial measures in response to the Breach, including investigations, mitigation of losses and protection against further Breaches; and
      - e) Contact information for the UNMHSC, or its designated agent, including, as appropriate, a toll-free telephone number, e-mail address, website, or postal address where individuals can obtain additional information and make requests.
    - (ii) Substitute Form of Notice: If there is insufficient or no up-to-date contact information precluding direct written communication to an individual, then a substitute form of notice shall be provided.

If there is insufficient or out-of-date contact information for ten (10) or more individuals, the UNMHSC shall provide a toll-free telephone number where individuals can learn if they have been affected by the Breach by:

- a) Posting a notice of the Breach on the UNMHSC website as specified by the U.S. Department of Health and Human Services; or
  - b) Placing a notice in major print or broadcast media in geographic areas where the affected individuals are likely to reside.
- b. **Emergency Notice:** If the Privacy Officer or the Office of University Counsel deems that a Breach notification is urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other means is permitted, as appropriate, in addition to written notice.
- c. **Required Notification to Media:** Notice of a Breach shall be provided to prominent media outlets serving the state if the unsecured PHI of more than 500 residents of such state has been or is reasonably believed to have been acquired, accessed, used or disclosed as a result of a Breach.
- d. **Required Notification to the Secretary of the U.S. Department of Health and Human Services (HHS):** Notice shall be provided to the Secretary of HHS of a Breach of unsecured PHI for which Notice to an affected individual has been or will be provided.
- (i) If the Breach involves the data of 500 or more individuals, the Privacy Officer shall notify the Secretary of HHS in the manner as specified at [www.hhs.gov](http://www.hhs.gov) at the same time notice is made to the individuals.
  - (ii) Breaches that involve the data of fewer 500 individuals will be maintained in a log and the Breach information submitted annually to the Secretary, no later than 60 days after the end of the calendar year.
  - (iii) If a Breach involves "secure" PHI, no notification to HHS is required.
- e. **Law Enforcement Delay:** Notice to affected individuals shall be delayed if law enforcement informs the UNMHSC that disclosure of a Breach would impede a criminal investigation or jeopardize national security.
- (i) A request for delayed notification must be made in writing or documented contemporaneously by the UNMHSC in writing, including the name of the law enforcement officer making the request and the officer's agency engaged in the investigation.
  - (ii) The required notice shall be provided without unreasonable delay after the law enforcement agency communicates to the UNMHSC the law enforcement agency's determination that notice will no longer impede the investigation or jeopardize national or homeland security.
- D. **Documentation:** Documentation of a Breach incident shall be maintained for at least six (6) years after a Breach incident has been closed and any required notification sent.
- E. **Sanctions:** The UNMSHC shall have in place and apply appropriate sanctions for failure to comply with privacy policies and procedures.
- F. **Retaliation/Waiver:** The UNMHSC may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The UNMHSC may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

**4.0 Responsibilities.**

<b>RESPONSIBILITIES</b>	
<b>Position/Title/Group</b>	<b>Requirements/Expectations/Duties</b>
Privacy Office	- Conduct investigation following the discovery of a Breach - Determine the necessity of Emergency, Law Enforcement, Media and government notices. - Responsible for drafting notification letters.
HCS Workforce Member	Must immediately notify his/her supervisor upon becoming aware of a Breach
HCS Workforce Supervisor	Must immediately notify HIPAA Privacy Officer and the HIPAA Security Officer of Breach
Business Associate	Must immediately notify the office and official of the UNMHSC with whom the Business Associate contracted to perform the contracted service.
UNMMHSC Contract Official	Must immediately notify the HIPAA Privacy Officer and the HIPAA Security Officer of Breach.
UNMMHSC	Shall notify each individual whose unsecured PHI has been or reasonably believed to have been acquired, accessed, used or disclosed as a result of the Breach within 60 calendar days.

**5.0 Records. Applicability/Retention.**

All UNMHSC workforce members and all workforce members of health care components of UNM that are under the jurisdiction of the HSC as designated in the UNM Board of Regents' Policy Manual, No. 3.8, Institutional HIPAA Compliance Program.

**6.0 External Reference(s).**

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA").
- Health Information Technology for Economic and Clinical Health ("HITECH") Act, ARRA Title XIII, Subtitle D.
- U.S. Department of Health and Human Services Breach Notification for Unsecured Protected Health Information Regulation, 45 CFR § 164.400 et seq.
- HIPAA Privacy Rule, Security Rule, and Enforcement Rule, 45 CFR Parts 160 and 164.

**7.0 Internal Reference(s).**

- Privacy Office 272-1493 or [HSC-Privacy@salud.unm.edu](mailto:HSC-Privacy@salud.unm.edu)
- HSC IT Security 272-1696 or [HSC-ISO@salud.unm.edu](mailto:HSC-ISO@salud.unm.edu)
- UNMH IT Security 272-5657 or [ITSecuirtyplan@salud.unm.edu](mailto:ITSecuirtyplan@salud.unm.edu)
- UNM Board of Regents' Policy Manual, No. 3.8, Institutional HIPAA Compliance Program

**8.0 Definitions.**

**Breach:** an acquisition, access, use, or disclosure of protected health information in a manner not permitted under (45§ 164.402) subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
- (iii) Whether the protected health information was actually acquired or viewed; and

- (iv) The extent to which the risk to the protected health information has been mitigated.

The term "Breach" does not include:

- (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
- (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
- (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

**Business Associate:** A Business Associate is a party with whom the UNMHSC enters into a contract in order to perform a service that the UNMHSC otherwise would perform for itself. Pursuant to HIPAA, the contract is called a "Business Associate Agreement" ("BAA"). The Business Associate "steps into the shoes" of the UNMHSC with regard to the responsibility to protect PHI, including responsibility to report a Breach to the UNMHSC.

**Disclosure:** Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of PHI outside of the entity holding the information.

**Individual:** The person who is the subject of the PHI.

**Protected Health Information:** Protected Health Information ("PHI") is information created by a health care provider, health plan, or health care clearinghouse that identifies an individual or provides a reasonable basis to believe the information can be used to identify the individual and that relates to:

- (i) The past, present, or future physical or mental health or condition of an individual; (ii) The provision of health care to an individual;
- (iii) The past, present, or future payment for the provision of health care to an individual; and
- (iv) that is transmitted or maintained in any form or medium, including electronic information.

**Reasonable Diligence:** Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

**Unsecured Protected Health Information:** As defined within the Breach of Unsecured Protected Health Information Regulation, unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary for the U.S. Department of Health and Human Services in guidance issued under the HITECH Act.

**Workforce Member:** Consistent with HIPAA and for purposes of this policy, "workforce member" means employees, volunteers, students, trainees, and other persons whose conduct, in the performance of work for the UNMHSC or a Business Associate of the UNMHSC, is under the direct control of the UNMHSC or the Business Associate, whether or not they are paid by the UNMHSC or the Business Associate.

- a. A person is acting under the authority of the UNMHSC if he or she is acting on its behalf.
- b. A person may include a Business Associate or an employee of a Business Associate

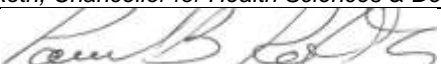
**9.0 Key Words.**

Breaches; Health Insurance Portability and Accountability Act (HIPAA); Protected Health Information (PHI)

**10.0 Attachments.**

Attachment A. Examples of Breaches of Unsecured Protected Health Information

**11.0 Approval Authority.**

APPROVAL and Information			
Item	Contact Information	Date	Reviewed / Approved
Document Owner	Privacy Office, Laura Putz, Privacy Officer, 272-1493		
Committee	Executive Compliance Committee		Approved
Office	HSC Office of University Counsel		Reviewed
Official Approver	Paul B. Roth, Chancellor for Health Sciences & Dean of School of Medicine.		Approved
Official Signature		3/22/2017	
	Document Origination Date	10/2010	
	Document Effective Date	3/22/2017	

**12.0 Document History.**

HISTORY LOG				
Date and Date Type: (Specify: Origination, Effective or Retired Date) In addition: Add Review Date when effective date does not change due to no major updates.	New Revision/ Letter/#:	Title of Document:	Description of Change(s):	Approved By: Print Name/Title
10/2010, Origination Date	Original	Responding to Breaches	Original	
3/22/2017, Effective Date	Version I	Responding to Breaches of Protected Health Information (PHI)	<ul style="list-style-type: none"> <li>• Clarifies that internal notification and Breach by Business Associate should be reported to the HIPAA Privacy Officer and the HIPAA Security Officer.</li> <li>• Updates definition of breach.</li> <li>• Updates requirements of external notification.</li> <li>• Corrects typos.</li> <li>• Removes redundant definitions and/or statements</li> <li>• Removes Privacy Breach Notification Process Flow Chart.</li> <li>• Updates Examples of Breaches of Unsecured Protected Health Information</li> </ul>	Dr. Paul Roth, Chancellor for Health Sciences
5/31/2018, Reviewed. Effective Date remains 3/22/2017 as there were only minor edits.	Revision 1	HIPAA - Responding to Breaches of Protected Health Information (PHI) Policy	<ul style="list-style-type: none"> <li>• Reformatted using Universal Template</li> <li>• Created the Responsibilities box, using information from existing content.</li> </ul>	Dr. Paul Roth, Chancellor for Health Sciences
11/1/2019, Reviewed. Effective Date remains 3/22/2017 as there were only minor edits.	Revision 1	HIPAA - Responding to Breaches of Protected Health Information (PHI) Policy	<ul style="list-style-type: none"> <li>• Update Regent Policy reference.</li> <li>• Updated Document Owner.</li> </ul>	N/A

## ATTACHMENT A

## Examples of Breaches of Unsecured Protected Health Information

- Missing or stolen laptop containing unsecured protected health information
- Workforce member accessing PHI for information about co-workers, friends, or family members out of curiosity, i.e., without a medical or business-related purpose
- Misdirected FAX of patient records to the incorrect patient
- Misdirected FAX of PHI to a local business instead of the requesting provider's FAX
- Discharge documents of one patient given to another patient
- Prescription document intended for Patient #1 given to Patient #2
- Billing or credit card information of Patient #1 sent to Patient #2
- Briefcase containing patient information stolen from auto
- Lost flash drive containing PHI about individuals participating in a clinic study
- Medical record documents left unattended in cafeteria
- Explanation of Benefits (EOB) sent to the wrong entity
- Lost mobile device with patient-identifying photos
- Papers containing protected health information found scattered along the roadside
- Intentional and non-work related access by staff member of neighbor's health information
- Medical records or other PHI lost in mailing process and never received