

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 11	Patient Privacy Policies	Effective:	February 2010
Section 11.1	General Oversight Policies	Revised:	
Policy 11.1.1	Notification of Privacy and Security Breaches	Responsibility:	Assistant Vice President for Regulatory Affairs & Compliance

NOTIFICATION OF PRIVACY AND SECURITY BREACHES

Overview

The UT Health Science Center at San Antonio (Health Science Center) is required to report all breaches of protected health information and personally identifying information to the Department of Health & Human Services (HHS). A report of all breaches involving less than 500 individuals per incident is required annually. Breaches involving 500 or more individuals have additional notification requirements as outlined in this policy. This policy outlines the reporting responsibilities and potential penalties to both the Health Science Center and/or employees if breaches are not appropriately handled in accordance with federal regulatory requirements and institutional policies.

Policy

Whenever a breach of protected health information and personally identifying information occurs, the employee should immediately notify their supervisor, who will notify the institutional Privacy Officer in the Office of Regulatory Affairs & Compliance at (210) 567-5212. If the supervisor is not available, the employee should contact the Privacy Officer.

In addition, if personally identifying information is lost or stolen, a report should be made with the proper law enforcement authorities where the incident occurred and with University Police.

Each employee is required to cooperate with institutional officials in identifying what information was stolen and/or compromised. By federal regulations, an individual whose information was breached shall be notified by the Privacy Officer within sixty (60) days following a discovery of a breach.

Definitions

BREACH: Generally is an impermissible use or disclosure under the HIPAA Privacy Rules that compromises the security or privacy of protected health information (PHI), and personally identifiable information (PII), such that the use or disclosure poses a significant risk of financial, reputational, or other harm to an affected individual. Information can be in the form of paper, faxes, an electronic device, including laptops and portable devices (including USB devices) or even

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 11	Patient Privacy Policies	Effective:	February 2010
Section 11.1	General Oversight Policies	Revised:	
Policy 11.1.1	Notification of Privacy and Security Breaches	Responsibility:	Assistant Vice President for Regulatory Affairs & Compliance

disclosure through inappropriate conversations. A breach is the unauthorized acquisition, access, use or disclosure of PHI and PII.

BUSINESS ASSOCIATES: A business associate is a person or entity who provides certain functions, activities, or services for or to the Health Science Center, involving the use and/or disclosure of protected health information. This includes but is not limited to, lawyers, auditors, third party administrators, healthcare clearinghouses, data processing firms, billing firms, and other covered entities. A business associate is not a Health Science Center employee.

PERSONAL HEALTH INFORMATION (PHI): Individually identifiable health information, including demographic data, that is maintained in any medium that related to:

- The individual’s past, present or future physical or mental health or condition
- The provision of health care to the individual, and/or
- The past, present, or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

PERSONALLY IDENTIFYING INFORMATION (PII): Individual personal information, such as Social Security number, driver’s license or identification number, date of birth, address, phone number or other personal information.

REASONABLE CAUSE: Circumstances that would make it unreasonable for the University, despite the exercise of ordinary business care and prudence, to comply with the provision violated.

REASONABLE DILIGENCE: Business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

WILLFUL NEGLECT: Conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 11	Patient Privacy Policies	Effective:	February 2010
Section 11.1	General Oversight Policies	Revised:	
Policy 11.1.1	Notification of Privacy and Security Breaches	Responsibility:	Assistant Vice President for Regulatory Affairs & Compliance

Determining if a Breach Occurred

It is the responsibility of all supervisors and employees to immediately report any breaches. The Privacy Officer, along with other institutional officials, will determine if a breach of information has indeed occurred.

All stolen and lost electronic devices shall be reported to the appropriate officials as defined in this policy.

Any inadvertent or unauthorized access, use or disclosure of information will be evaluated and analyzed to determine when individuals whose information was breached need to be notified.

Exceptions to Breach Notifications

In accordance with federal regulations, there are some exceptions when an individual(s) does not need to be notified of a breach. However, this determination will be made by the Privacy Officer and Legal Affairs.

The University has the burden of proving why a breach notification was not required and must document why impermissible use or disclosure fell under one of the exceptions.

Breach Notification Requirements

The Privacy Officer must provide notification of a breach of unsecured protected health information to affected individuals, the Secretary of the United States Department of Health & Human Services, and in certain circumstances breaches affecting more than 500 individuals, to the media. Also, business associates must notify the Privacy Officer that a breach has occurred. Below is a summary of the required notifications that will be handled by the Privacy Officer in coordination with appropriate institutional officials.

Individual Notice

The Privacy Officer must notify affected individuals following the discovery of a breach of unsecured protected health information. The Privacy Officer must provide the individual(s) notice in written form by first-class mail. If the University has insufficient or out-of-date contact information for 10 or more individuals, the Privacy Officer must provide substitute individual notice by providing the notice on the home page of the Web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the University has

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 11	Patient Privacy Policies	Effective:	February 2010
Section 11.1	General Oversight Policies	Revised:	
Policy 11.1.1	Notification of Privacy and Security Breaches	Responsibility:	Assistant Vice President for Regulatory Affairs & Compliance

insufficient or out-of-date contact information for fewer than 10 individuals, the Privacy Officer may provide substitute notice by an alternative form of written, telephone, or other means.

The individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the University is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information. The notifications will be signed by the senior leadership (Vice President, Dean, Chair, Director) where the breach occurred along with the Privacy Officer. Additionally, a substitute notice provided via Web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the University to determine if their protected health information or personally identifying information was involved in the breach.

Media Notice

The University that experiences a breach affecting more than 500 residents of a state or jurisdiction is, in addition to notifying the affected individuals, is required to provide notice to prominent media outlets serving the state or jurisdiction. The University would provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Notice to United States Department of Health & Human Services

In addition to notifying affected individuals and the media, when appropriate, the Privacy Officer must notify the Secretary of the United States Department of Health & Human Services (Secretary) of breaches of unsecured protected health information. The Privacy Officer will be required to provide this notification by submitting an electronic breach notification. If a breach affects 500 or more individuals, the Privacy

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 11	Patient Privacy Policies	Effective:	February 2010
Section 11.1	General Oversight Policies	Revised:	
Policy 11.1.1	Notification of Privacy and Security Breaches	Responsibility:	Assistant Vice President for Regulatory Affairs & Compliance

Officer must notify the Secretary without unreasonable delay and in no case later than 60 days following the breach. All notification requirements will be handled by the Privacy Officer in the Office of Regulatory Affairs & Compliance.

Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the University following the discovery of the breach. To the extent possible, the business associate should provide the University with the identification of each individual affected by the breach, as well as any information required to be provided by the University in its notification to affected individuals.

Potential Penalties for Breaches

The United States Office of Civil Rights can assess penalties for breach violations. The following tiers of penalties are cited in the Act. An individual employee and the institution may be held liable for not protecting information.

Category A: The individual did not know they violated the regulations, and was exercising reasonable diligence and would have not known they violated the regulations. The penalty could be \$100 for each violation, and may not exceed \$25,000 in a calendar year.

Category B: Violations due to reasonable cause and not to willful neglect. The penalty could be \$1,000 for each violation, and may not exceed \$100,000 in a calendar year.

Category C: Violations due to willful neglect and was eventually corrected. The penalty could be \$10,000 for each violation, and may not exceed \$25,000 in a calendar year.

Category D: Violations due to willful neglect and not corrected. The penalty could be \$50,000 for each violation, and may not exceed \$1,500,000 in a calendar year.

In addition to the federal penalties, the State Attorney General may also levy fines and file a civil action on behalf of the individuals harmed.