Chapter 11	Patient Privacy Policies	Effective:	February 2010
Section 11.1	General Oversight Policies	Revised:	February 2016
Policy 11.1.1	**Notification of Privacy and Security Breaches**	Responsibility:	Chief Compliance Officer 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) 567-2014. 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 acquisition, access, use or disclosure under the HIPAA Privacy Rules that compromises the security or privacy of protected health information (PHI), and personally identifiable information (PII). Information can be in the form of paper, faxes, an electronic device, including laptops and portable devices (including USB devices) or even disclosure through inappropriate conversations.

A breach is the unauthorized acquisition, access, use or disclosure of protected health information and personally identifying information.

BUSINESS ASSOCIATES: A business associate is a person or entity, including their subcontractors, who provide 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, health information organizations, E-prescribing Gateways, and other covered entities. A business associate is not a Health Science Center employee.

GENETIC INFORMATION: Genetic tests of the individual or of the individual's family members and about diseases or disorders manifested in an individual's family members.

PROTECTED HEALTH INFORMATION: 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 genetic information of the individual
- 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.

Protected health information does not include individually identifiable health information of persons who have been deceased for more than 50 years.

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

Chapter 11	Patient Privacy Policies	Effective:	February 2010
Section 11.1	General Oversight Policies	Revised:	February 2016
Policy 11.1.1	**Notification of Privacy and Security Breaches**	Responsibility:	Chief Compliance Officer for Regulatory Affairs & Compliance

REASONABLE CAUSE: An act or omission that by exercising reasonable diligence would have known it violated a provision, but did not act with willful neglect.

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

SUBCONTRACTOR: A person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such business associate.

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

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.

The Privacy Officer will use the HIPAA Risk Assessment Analysis Tool when needed to determine if a breach occurred.

Chapter 11	Patient Privacy Policies	Effective:	February 2010
Section 11.1	General Oversight Policies	Revised:	February 2016
Policy 11.1.1	**Notification of Privacy and Security Breaches**	Responsibility:	Chief Compliance Officer for Regulatory Affairs & Compliance

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. The individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.

Substitute Notice

If the University has insufficient or out-of-date contact information for fewer than 10 individuals, or if some notices are returned as undeliverable, the Privacy Officer may provide substitute notice by an alternative form of written notice, by telephone, or other means. In the event of 10 or more individuals, either with out of date contact information or undeliverable returned notices, then the University will provide substitute notice through either a conspicuous posting for a period of 90 days on the Health Science Center's home page or conspicuous notice in a major print of broadcast media in geographic areas where the individuals affected by the breach likely reside. The University will provide a toll-free phone number in the notice, active for 90 days, where an individual can learn whether their unsecured protected health information may be included in the breach.

Additional Notice in Urgent Situations

In any case deemed by the University to require urgency because of possible imminent misuse of unsecured protected health information, the University may provide information to individuals by telephone or other means, as appropriate, in addition to the methods of individual written notification.

Deceased Individual Notice

If the University knows that the individual is deceased and has the address of the next of kin or personal representative of the deceased individual, written notification will be sent by first-class mail. In the case where out-of-date contact information yields notices returned as undeliverable, verification will be attempted than the obligation ends.

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 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.

Law Enforcement Delay

A temporary delay of notification is required in situations in which a law enforcement official provides a statement in writing that the delay is necessary because notification would impede a criminal investigation or cause damage to national security, and specifies the time for which a delay is required. In such instances, the University is required to delay the notification, notice, or posting for the time period specified by the

official. If a law enforcement official states orally that notification would impede a criminal investigation or cause damage to national security a temporary delay of notification notice is required. This delay would be no longer than 30 days from the date of the oral statement, and must include the identity of the official making the statement unless a written statement was received during that time for a specified delay time.

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, without unreasonable delay and in no case later than 30 days, 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.

Content of the Notice

The HIPAA breach notification will include, to the extent possible, the following elements:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, or other types of information were involved);

3. Any steps the individual should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what the University is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, which must include a toll free telephone number, an e-mail address, website, or postal address.

Burden of Proof

In the event of an inappropriate use or disclosure the University or their business associate, as applicable, shall maintain documentation sufficient to meet its burden of proof demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.

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 and may not exceed $50,000, for each violation.

Category B: Violations due to reasonable cause and not to willful neglect. The penalty could be $1,000, and may not exceed $50,000, for each violation.

Category C: Violations due to willful neglect and was eventually corrected. The penalty could be $10,000, and may not exceed $50,000, for each violation.

Category D: Violations due to willful neglect and not corrected. The penalty could be $50,000 for each violation, and may not exceed $1.5 million in a calendar year.

For all the categories above all such violations of an identical provision shall not exceed $1.5 million 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.