



**OFFICE OF THE DIRECTOR OF POLICE  
THE UNIVERSITY OF TEXAS SYSTEM  
POLICY AND PROCEDURE MANUAL**



Subject			Policy Number
<b>COMPLIANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)</b>			<b>130</b>
Effective Date	Revision Date	Reevaluation Date	Number of Pages
January 7, 2013	January 30, 2019	Annually	7
Reference Standards		Rescinds or Amends Policy Number	
TPCA: CALEA: 54.1.1 IACLEA: 16.2.1			

**I. PURPOSE**

The purpose of this policy is to provide guidance to the University of Texas System Police (UTSP) in identifying and clarifying the requirements of The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related federal regulations.

**II. POLICY**

It is the policy of the University of Texas System Police to comply with the requirements of HIPAA.

**III. DEFINITIONS**

**Administrative Request**—means an administrative subpoena or investigative demand or other written request from a law enforcement official.

Because an administrative request may be made without judicial involvement, the Rule *requires* all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used. (45 CFR 164.512(f)(1)(ii)(C)).

**Covered entity**—is one of the following:

1. **Health Care Provider**, if it transmit any information in an electronic form in connection with a transaction for which the Department of Health and Human Services (HHS) has adopted a standard:
  - a. Doctors
  - b. Clinics
  - c. Psychologists
  - d. Dentists
  - e. Chiropractors
  - f. Nursing homes
  - g. Pharmacies

**2. A Health Plan**

- a. Health insurance companies
- b. HMOs
- c. Company health plans
- d. Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs

**3. A Health Care Clearinghouse**

- a. Includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa

**De-identified Health Information**—Under HIPAA's "safe harbor" standard, information is considered de-identified if all protected health information has been removed, and there is no reasonable basis to believe that the remaining information could be used to identify a person.

There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. De-identified information is not protected, and can be shared without limit.

**Disclosure**—Covered entities may only use or disclose PHI as permitted or required by the Privacy Rule. Disclosure is the release, transfer, provision of access to, or divulging in any other manner of information outside the entity. Examples of permitted uses and disclosures of PHI are:

- a. Required by law
- b. Public health activities
- c. About victims of abuse, neglect or domestic violence
- d. Health oversight activities
- e. Judicial and administrative proceedings
- f. Law enforcement purposes
- g. To avert a serious threat to health or safety

**Family Educational Rights and Privacy Act of 1974 (FERPA)** -- FERPA is a federal law that, along with federal regulations implementing the law, protects the privacy of student education records. FERPA generally requires a university to have written permission from a student attending the university before the university may release any information from the student's education record. *FERPA applies only to the disclosure of information obtained from an education record.*

FERPA does not apply to the disclosure of information from any other source. *However, once the information is reported to a university official and becomes a record, the information in the record becomes subject to FERPA.*

**The Health Insurance Portability and Accountability Act of 1996 (HIPAA)** -- The Health Insurance Portability and Accountability Act of 1996 is a law passed by Congress intended to establish transaction, security, privacy and other standards to address concerns about the electronic exchange of health information.

- 1. HIPAA does not apply to student medical records
- 2. HIPAA does not apply to student education records subject to FERPA

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. The Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI).

The Security Rule specifies a series of administrative, physical and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.

**Hybrid Entity**—For example, a university health clinic that is a HIPAA covered entity and has health information to which the Privacy Rule does *not* apply.

**In Electronic Form**—means using electronic media, electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media.

Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.

Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

**Minimum Necessary Standard**—A standard in HIPAA's privacy rule that requires covered entities to make reasonable efforts to limit protected health information (PHI) to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

**Privacy Rule**-- The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used.

*The Privacy Rule does not prevent covered entities from establishing internal policies that provide greater protections, or that offer consumers greater rights; moreover, the Rule does not preempt more stringent state laws.*

Effective September 1, 2012 **Texas House Bill 300** expanded the definition of a covered entity, mandated new patient privacy protocols for covered entities and implemented harsher penalties for privacy violations related to electronic health records. House Bill 300 significantly expanded patient privacy protections for Texas covered entities beyond those federal requirements as outlined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health (or "HITECH") Act.

**Protected Health Information (PHI)**—all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

PHI is information, including demographic data, that relates to:

1. The individual’s past, present or future physical or mental health or condition
2. The provision of health care to the individual
3. 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.

Individually identifiable health information includes many common identifiers:

1. Name
2. Address
3. Birth date
4. Social Security number
5. Electronic mail addresses
6. Vehicle identifiers including license plate numbers
7. Full face photographic images

The definition of protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) specifically excludes identifiable health information in "education records" subject to the Family Education Rights and Privacy Act (FERPA, 20 USC 1232g).

**Security Rule**—The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity.

#### **IV. DISCLOSURE OF INFORMATION TO LAW ENFORCEMENT**

The Rule permits covered entities to disclose protected health information (PHI) to law enforcement officials, without the individual’s written authorization, under specific circumstances.

- A. To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.
- B. To respond to an administrative request
- C. To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person.
  1. The covered entity must limit disclosures of PHI to name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics.

2. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request (45 CFR 164.512(f)(2)).

D. This same limited information may be reported to law enforcement:

1. About a suspected perpetrator of a crime when the report is made by the victim who is a member of the covered entity's workforce (45 CFR 164.502(j)(2));
2. To identify or apprehend an individual who has admitted participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual's request for therapy, counseling, or treatment related to the propensity to commit this type of violent act (45 CFR 164.512(j)(1)(ii)(A), (j)(2)-(3)).

## V. **Child Abuse Victims or Adult Victims of Abuse, Neglect or Domestic Violence**

Child abuse or neglect may be reported to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required (45 CFR 164.512(b)(1)(ii)).

Adult abuse, neglect, or domestic violence may be reported to a law enforcement official authorized by law to receive such reports (45 CFR 164.512(c)):

- If the individual agrees;
- If the report is required by law; or
- If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations (see 45 CFR 164.512(c)(1)(iii)(B)).

If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

Furthermore, covered entities may disclose information if, in their professional judgment, they believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, unless the covered entity believes informing the individual would place the individual at risk of serious harm.

Notice to the individual of the report may be required (see 45 CFR 164.512(c)(2)).

## VI. **SUPPLEMENTARY DISCLOSURES TO LAW ENFORCEMENT**

- A. State laws commonly require health care providers to report incidents of gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws. (See Section VII Texas Health and Safety Code)
- B. A covered entity may disclose PHI in response to a law enforcement official's request for information about an individual who is or is suspected to be a victim of a crime, if:

1. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
  2. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
- C. A covered entity may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct (45 CFR 164.512(f)(4)).
1. Information about a decedent may also be shared with medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties (45 CFR 164.512(g)(1)).
  2. To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the covered entity's premises (45 CFR 164.512(f)(5)).
- D. When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity, specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime (45 CFR 164.512(f)(6)). This provision does not apply if the covered health care provider believes that the individual in need of the emergency medical care is the victim of abuse, neglect or domestic violence; see above Adult abuse, neglect, or domestic violence for when reports to law enforcement are allowed under 45 CFR 164.512(c).
- E. When consistent with applicable law and ethical standards:
1. To a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public (45 CFR 164.512(j)(1)(i)); or
  2. To identify or apprehend an individual who appears to have escaped from lawful custody (45 CFR 164.512(j)(1)(ii)(B)).
- F. For certain other specialized governmental law enforcement purposes, such as:  
To federal officials authorized to conduct intelligence, counter-intelligence, and other national security activities under the National Security Act (45 CFR 164.512(k)(2)) or to provide protective services to the President and others and conduct related investigations (45 CFR 164.512(k)(3));
- G. To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody of an inmate or others if they represent such PHI is needed to provide health care to the individual; for the health and safety of the individual, other inmates, officers or employees of or others at a correctional institution or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility (45 CFR 164.512(k)(5)).

**Except when required by law, the disclosures to law enforcement summarized above are subject to a minimum necessary determination by the covered entity (45 CFR 164.502(b), 164.514(d)).**

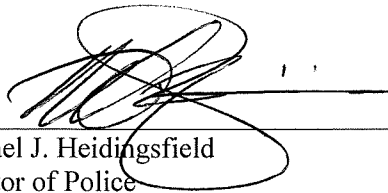
When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose (45 CFR 164.514(d)(3)(iii)(A)).

Moreover, if the law enforcement official making the request for information is not known to the covered entity, the covered entity must verify the identity and authority of such person prior to disclosing the information (45 CFR 164.514(h)).

## **VII. TEXAS HEALTH AND SAFETY CODE**

- A. All information about a patient obtained through the therapeutic relationship is confidential.
- B. The professional is prohibited from disclosing even the identity of a client to third parties unless specifically authorized by state law.
- C. Exception:
  - 1. Mental health care providers are specifically authorized to disclose patient information to medical or law enforcement personnel if the professional determines that:
    - a) There is a probability of imminent physical injury by the patient, to the patient or others, or
    - b) Determines there is a probability of immediate mental or emotional injury to the patient
  - 2. This information is not permitted to be disclosed to university officials who are neither medical nor law enforcement personnel.
- D. **Mandatory Reporting of Gunshot Wounds**

A physician who attends or treats, or who is requested to attend or treat, a bullet or gunshot wound, or the administrator, superintendent, or other person in charge of a hospital, sanitarium, or other institution in which a bullet or gunshot wound is attended or treated or in which the attention or treatment is requested, shall report the case at once to the law enforcement authority of the municipality or county in which the physician practices or in which the institution is located. (Texas HSC Ann. § 161.041)



---

Michael J. Heidingsfield  
Director of Police