Privacy Office: 713-500-3391
https://inside.uth.edu/hipaa

UTHealth
The University of Texas
Health Science Center at Houston

HIPAA Overview and Information Safeguards

PRIVACY Refers to *WHAT* is protected — Health information about an individual and the determination of *WHO* is permitted to use, disclose, or access the information.

SECURITY Refers to *HOW* private information is safeguarded—Insuring privacy by controlling access to information and protecting it from inappropriate disclosure and accidental or intentional destruction or loss. Providers must, however, put in physical, administrative and technical safeguards to ensure that patient privacy is protected.

PROTECTED HEALTH INFORMATION (PHI) = Individually identifiable information relating to the past, present or future health condition of the individual *ALL* information whether maintained in electronic, paper or oral format that relates to

- the health or condition of an individual, or
- the provision of healthcare, or
- the payment of healthcare items or services, and
- was created by or received by a provider, health plan, employer, or healthcare clearinghouse.

FUNDAMENTAL RULES

- Patients' health information is to be used or disclosed only for work-related purposes;
- The uses and disclosures made by UTHealth employees must be no more than necessary to get the job done;
- It is everyone at UTHealth's responsibility to keep patients' information confidential and secure.

PATIENT PRIVACY RIGHTS.

- Patients have a right to understand how their health information will be used and disclosed by UTHealth.
- To that end, patients have a right to receive a notice of privacy practices—which will also be posted in UTHealth owned or operated clinics and at UTP clinics—that informs them about uses and disclosures of their health information;
- Patients have a right to ask questions about privacy, and have those questions clearly and promptly answered;
- Patients have a right to an accounting of who outside of the institution has seen their health information, and for what purpose;
- Patients have a right to see and obtain a copy of their records;
- Patients have a right to ask for an amendment—or inclusion of a statement of disagreement—for anything in the record that they believe is in error;
- Patients have a right to expect that their health information will be kept secure and only used for legitimate purposes;
- Patients have a right to agree or object to involving their friends and family in their care;
- Patients have a right to authorize or refuse additional uses of their information -- such as for fundraising, marketing or research;

- Patients have a right to request restrictions on the use or disclosure of information they consider especially sensitive, and to request confidential communication of especially sensitive information;
- Patients have a right to complain to UTHealth's Privacy Office—and to the Department of Health and Human Services' Office of Civil Rights—if they believe their rights have been violated.

SECURITY BASICS

- UTHealth's departments should be kept secure from intruders—with locks, alarm systems and other security devices and systems –the department is not open for business;
- Physical access to filing cabinets, computers and printers, photocopiers, fax machines and any other areas or equipment where patient information may be present should be controlled and monitored;
- All workers should wear UTHealth identification badges at all times;
- Patients and visitors should be appropriately escorted to ensure that they do not access restricted areas, and unidentified persons in restricted areas are (politely) challenged for identification;
- When a person no longer works at UTHealth, keys and identification badge should be returned, alarm codes are changed, and computer access should be removed within one day.

Confidentiality in oral exchanges

- Confidential conversations about patient information should not take place where they can easily be overheard by third parties;
- When possible, do not use names or other information that could identify patients;
- When it cannot be avoided, discussions about a patient's condition in public areas should be conducted quietly;
- In general, oral communications of patient information are limited to the minimum necessary to get the job done.

Confidentiality for telephone use

- Telephone conversations involving patient information should be conducted where they cannot be overheard, if at all possible;
- ALWAYS confirm the other person's identity when discussing confidential information with a patient, or about a patient to a third party;
- If the patient cannot be reached on the telephone, leave only names and callback numbers on answering machines, voicemail systems, or with the person that answers;

Paper information in general

- Paper that contains patient information should discarded in a secure container (for future shredding) or shredded immediately;
- Patient files are never left in plain view (e.g., if on a door rack, the identifying information must be obscured);
- If patient files must be left in an area where visitors are present, they are face down or otherwise concealed;
- Patient information should not be left in public areas, ever;
- Filing cabinets or rooms that contain patient information should be locked when unattended.

Non-routine uses and disclosures

- Non-routine uses and disclosures of patient information outside of UTHealth should be undertaken only by persons designated and trained for it,
- In general, anything out of the ordinary should be referred to the Privacy Officer.

Basic rules of electronic security

- Computer passwords should be kept secure, and changed regularly;
- Computer access tokens (such as key cards or USB keys), if used, should also be kept secure and encrypted;
- Computer screens should not be in plain view, where anyone other than staff can easily see them;
- Users should log in to computer systems or terminals only with their own userid, password or token;
- If there is no password protected screensaver on the computer, log off when a computer system or terminal is unattended, even if it is only for a short time;
- Portable computing devices (laptops, smartphones and tablets) should be kept secure by remaining in the department or by password protection; All portable devices should be encrypted.
- When a person no longer works at UTHSC-H, his/her computer userids and passwords should be immediately deleted, and any access tokens should be returned;
- Use of computer-based patient information should be limited to the minimum necessary to get the job done.
- PHI should be stored on the secure servers in Zone 100