11.1.5 Patient Health Records

Chapter 11 - Patient Privacy	Original Effective Date: April 2003
Section: 11.1 General Oversight Policies	Date Last Reviewed: February 2016
Responsible Entity: Chief Compliance Officer for Regulatory Affairs & Compliance	Date Last Revised: February 2016

I. Purpose

To establish the handling and management of patient health records in compliance with legal and professional standards followed by UT Health San Antonio.

II. Scope

This policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other individual (collectively, Workforce Member, including employees and non-employees) who has direct or indirect access to patient protected health information (PHI) created, held or maintained by any UT Health San Antonio controlled affiliate, including, not limited to its clinics, hospitals, and research operations.

III. Policy

UT Health San Antonio (UTHSA) maintains patient health records in accordance with legal and professional standards to ensure the integrity and availability of health information to provide timely and appropriate care and health care planning for the patient.

A. Documentation Requirements

Only authorized individuals may document the patient's legal health record, including faculty and residents of any discipline. All entries into the health record should be recorded in ink and are considered permanent. Authors should be clearly identifiable with credentials including a signature. Entries must be legible and timed and dated. The author should correct errors on paper documents by drawing a single line through the incorrect entry, writing "error", initialing, and dating it, with the reason for the change, and errors in an electronic record should be completed with an addendum note if the record cannot be changed. Errors should never be obliterated. Documentation should be completed at the time services are rendered. Entries regarding patient care should never be made in advance of the actual provision of care. Amendments or

corrections requested by the patient are made according to HOP policy 11.3.2 Patient Right to Amend Patient Health Information.

Health records must contain adequate information to provide care to the patient, to provide communication between care providers within and external to the UTHSA, and to substantiate insurance claims. The health record is considered a legal document. The record should contain any laboratory, radiology, and other diagnostic reports that are used as part of the diagnostic and treatment process. Photographs, videotapes, or other images of the patient taken as part of the patient's treatment may be filed with the record. If they are not filed with the record, the health care provider must document in the record that the images were taken and their location. See HOP policy 11.1.4 Patient Photography, Videotaping, and Other Imaging.

Copies of reports of care provided at other facilities sent to UTHSA from other facilities to assist with care are considered part of the designated record set. The patient should be asked to specifically authorize disclosures of any such records. Any such records that are not needed by UTHSA practitioners to provide care and to substantiate care provided should be destroyed in the manner described in this policy. Re-disclosures of health information should be made in accordance with state and federal law.

B. Ownership and Patient Access

All parts of the health record belong to UTHSA; UTHSA must safeguard confidentiality and security of the record and the information contained in it. The information belongs to the patient, who is entitled to access according to HOP policy 11.3.6 Access to Protected Health Information. Original health records should not be removed from UTHSA except as directed by court order.

C. Case Management Files (Shadow Records)

Case management files or shadow records are comprised of medical or health information that is a duplicate of information contained in the legal health record. This is a temporary file and must be retained only for the duration necessary to assist the health care professional in tracking and providing care to the patient. This record must be destroyed within parameters established by UTHSA. A shadow record should not contain original documents not included in the legal record, except as provided in HOP policy 11.2.2 Use and Disclosure of Psychotherapy Notes. In addition, there should be no disclosure of information from this record.

D. Security and Storage

UTHSA must reasonably safeguard all protected health information from any intentional or unintentional use or disclosure. UTHSA must reasonably safeguard protected health information to limit incidental uses or disclosures made in the course of providing an otherwise permitted or required use or disclosure.

All paper health records, as defined above, must be maintained in secured areas. The files, cabinets, or storage areas must be locked after hours or when staff is not present.

Areas in which patient information is stored must not be left unattended. Patient information should not be readily accessible to the general public, or to other individuals who do not have a need to view such information, such as laying out on desks or counters, on fax machines, copy machine, etc.

Electronic health information must be maintained according to Health Science Center security guidelines. Computer screens potentially displaying patient information must not be accessible to anyone not authorized to view such information. Staff must follow UTHSA policies regarding use of computer passwords and logging off. Health information shall not be maintained on laptops and portable devices unless for short periods of time and on an approved encrypted, UTHSA-owned device. Health information should never be downloaded on personal devices. For additional security policies, see Chapter 5.8 of the HOP, Information Security.

Verbal exchange of patient information between care providers and those involved with the patient's care, payment, or other health care operations, must occur to ensure appropriate and timely care to the patient. Individuals who exchange verbal information must ensure that they are in areas where they cannot be overheard by others who are not involved in the patient's care and do not have a right to hear the information. Staff must be particularly diligent in ensuring confidentiality when exchanging patient information in treatment areas, over the telephone, and in areas accessible to common areas such as hallways, elevators, and cafeterias.

E. Retention

Records are retained according to the UTHSA records retention policy located at https://library.uthscsa.edu/services/records-management/.

F. Destruction

All health information must be destroyed in a confidential and secure manner. Approved methods of destruction may include shredding or use of an approved outside vendor that specializes in the destruction of confidential information. Confidential information must not be discarded in regular trash bins, recycling bins, or other publicly accessible locations. Electronic data must be disposed of according to UTHSA security policies.

The department or clinic, or outside vendor if used, responsible for the destruction of confidential information must document, in accordance with HOP policy 2.2.1 Records Management. The documentation should include the date of destruction, method of destruction, what records were destroyed, a statement that records were destroyed in the normal course of business, and a signature and date of the person supervising the destruction.

IV. Definitions

Confidential Information – Includes legal medical record components and designated record set components. Also, includes any directory type information or any document that contains patient-related and personal information.

Designated Record Set – The designated record set is created to respond to patients' requests concerning the information used in making decisions about them. The designated record set is comprised of subsets of health information and may be maintained in various locations or files. Includes medical/dental and billing records maintained for or by UTHSA, and any health information used, in whole or part, by UTHSA to make decisions about the patient. Includes any photographs, videotapes, or other images that identify the patient. Includes records from other providers.

Legal Health Record – The legal health (medical) record substantiates the care provided to the patient. Includes the actual paper or electronic health record maintained by UTHSA. Includes any photographs, videotapes, or other images that identify the patient. Does not include billing records. The term "health record" includes, by definition, all records generated for medical, dental, psychological patient care, exclusive of psychotherapy notes as defined in HOP policy 11.2.2 Use and Disclosure of Psychotherapy Notes.

Protected Health Information – Individually identifiable health information, including demographic data, that is maintained in any medium that relates to:

1. The individual's past, present or future physical or mental health or condition,
2. The genetic information of the individual,
3. The provision of health care to the individual, and/or
4. 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.

Record – Any information that includes protected health information and is maintained collected, used, or disseminated by UTHSA.

V. Related References

There are no related documents associated with this Policy.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
04/2003	Policy Origination		
03/2013	Policy Review		
02/2016	Policy Review		