Policy Title: Policy on Protected Health Information Under the Health Insurance Portability and Accountability Act (HIPAA)	**Policy Number: BU-PP 048**
Date Issued: April 24, 2023	**Responsible Executive: HIPAA Privacy Officer**
Date Last Revised: April 24, 2023	**Responsible Office: Office of General Counsel**

Policy on Protected Health Information Under the Health Insurance Portability and Accountability Act (BU-PP 048)

Policy Statement

Baylor Community members may use or disclose Protected Health Information (PHI) only when permitted under the Health Insurance Portability and Accountability Act, as amended (HIPAA) Privacy Rule. Permissible use and disclosure of PHI shall be determined by the procedures stated in this policy.

Reason for the Policy

This policy is to inform Baylor Community members of the lawful handling of PHI and to establish a system for operating units to execute the provisions herein.

Individuals/Entities Affected by this Policy

All Baylor Community members, as defined below.

Exclusions

NONE

Definitions

These definitions apply to terms as they are used in this policy.

Application	A computer program that processes information.
Baylor Community	Workforce members who encounter PHI as a part of their duties.

Device	Any electronic appliance that stores and processes electronic data including desktop computers, laptops, tablets, mobile phones, medical devices, copiers, printers and fax machines that contain hard drives, and anything else that can store and process electronic data.
Disclosure	The release, transfer, access to, or divulging in any manner of information outside the entity holding the information.
Electronic media	(1) Electronic storage material on which data is or may be recorded electronically, including but not limited to, hard drives, flash/thumb drives, SIM cards, CD or other optical storage disk, magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, 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 if the information being exchanged did not exist in electronic form immediately before the transmission.
Electronic protected health information (ePHI)	Protected Health Information as defined herein when in electronic form.
Health care	Care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health care component	A component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(D).
Health care operations	Certain administrative, financial, legal, and quality improvement activities of a Covered Entity that are necessary to run its business and to support the core functions of treatment and payment, listed 45 CFR 164.501.
Health care provider	A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
Health information	Any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

HIPAA Contact	An Individual designated by each Covered Component to have primary responsibility for overseeing compliance with this policy within their operating unit. Each Covered Component shall designate two or more individuals to act as a HIPAA Contact.
Hybrid entity	A single legal entity: (1) that is a covered entity (i.e., provides health care services and collects and stores PHI); (2) whose business activities include both covered and non-covered functions (i.e., collects and stores health information, some of which is subject to HIPAA regulations and some of which is covered by FERPA or other laws); and (3) that designates health care components in accordance with paragraph §164.105(a)(2)(iii)(D).
Individual	The person who is the subject of protected health information. Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Media	Media means any item that can store but not process data, including USB drives, CD-ROMs, DVDs, hard drives, back up disks.
Protected health information (PHI)	Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

	(ii) In records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice. 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.
Research	A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
System	One or more computer servers and their related applications.
Treatment	The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
Use	With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
Workforce	Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

Contacts

Subject	Contact	Telephone	Office email/web site
Policy Questions	Chief Privacy Officer / HIPAA Privacy Officer	254-710-3821	https://go.web.baylor.edu/hipaa
	Chief Information Security Officer / HIPAA Security Officer	254-710-4357	https://go.web.baylor.edu/hipaa
Institutional Review Board	Assistant Vice Provost for	254-710-1438	https://www.baylor.edu/research/resources/index.php?id=963981

4. Policy on Protected Health Information Under the Health Insurance Portability and Accountability Act (HIPAA) (BU-PP 048)

	Research Compliance

Responsibilities

HIPAA Privacy Officer	Responsible for development, implementation, and enforcement of HIPAA privacy policies.
HIPAA Security Officer	Responsible for development, implementation, and enforcement of HIPAA security policies.
Covered Components	Each Covered Component must designate two or more individuals (aka HIPAA Contacts or Designated Individuals) to be responsible for implementing procedures under this policy for their unit. Every member of each Covered Component's Workforce is responsible for understanding and complying with this policy and the Covered Component's procedures, including completing annual HIPAA training.

Principles

Baylor is committed to protecting the privacy and confidentiality of PHI in accordance with HIPAA and the Texas Medical Records Privacy Act (TMRPA).[1]

Baylor has self-designated as a HIPAA Hybrid Entity, meaning certain operating units of the University which routinely handle PHI are designated as Covered Components (https://go.web.baylor.edu/sites/g/files/ecbvkj716/files/2023-05/HIPAA%20Hybrid%20Entity%20Self-Designation.pdf). In addition, other operating units handling PHI may not be subject to HIPAA but nevertheless are required to treat such information as if it were subject to HIPAA pursuant to the TMRPA. This policy provides guidance to those operating units for complying with HIPAA regulations.

The Workforces of each Covered Component are required by HIPAA to secure and keep private all PHI they create, receive, maintain, or transmit. PHI includes written physical documents, electronically stored records, audio and video recordings, biometric identifiers and other forms of records containing health information. They also observe the rights of individuals regarding their PHI as mandated by HIPAA.

The HIPAA Privacy Officer and the HIPAA Security Officer have the authority to approve the new and/or ongoing collection, processing, and retention of PHI. Failure to comply with this university policy will result in revocation of a PHI approval. If a breach, including unauthorized access or inadvertent disclosures, of PHI was caused by a Workforce

[1] The TMRPA is sometimes referred to as HB300

member, that person may be subject to disciplinary action, up to and including termination of employment, and the possibility of civil and/or criminal liability.

In the event this policy conflicts with any other Baylor policy, this policy shall govern.

I. HIPAA Privacy and Security Rules

Under HIPAA, there are two rules covering PHI: the Privacy Rule and the Security Rule.

The Privacy Rule describes who can access, use, and disclose PHI, and for what purposes. The Privacy Rule also describes how Covered Components assist Individuals with exercising their rights under HIPAA to access and control the use of his or her PHI.

The Security Rule describes how to protect electronic PHI ("ePHI") when using, storing, or transmitting it to minimize the risk of improper access or disclosure.

A. HIPAA Covered Components

Baylor is a HIPAA Hybrid Entity, meaning some of its operations are subject to HIPAA and are designated as HIPAA Covered Components.

The following are designated as Covered Components:

Clinical Operations – Academic departments and student support services of the university engage in standard HIPAA transactions, including but not limited to: providing health care services, maintaining protected health information and transmitting PHI electronically for the purpose of insurance billing:

1. Intercollegiate Athletics—Sports Medicine, to the extent its health care providers conduct any standard HIPAA transactions electronically, directly or through a vendor;
2. Division of Student Life—Student Health Services (including massage therapy, medical, pharmacy, physical therapy, psychiatry and psychology services) to the extent that its health care providers conduct any standard HIPAA transactions electronically, directly or through a vendor.

Administrative Support Services – Professional staff departments of Baylor, to the extent any personnel use and disclose individually identifiable health information in providing administrative and support services to the designated entities above, and would constitute a business associate if the department was a separate legal entity:

1. General Counsel
2. Human Resource Services

3. Information Technology Services (ITS)
4. Intercollegiate Athletics
5. Internal Audit
6. Privacy Office
7. University Compliance and Risk Services

Certain other operations of Baylor would otherwise meet the statutory definition of a Covered Component, including the Speech and Hearing Clinic, Clinical Psychology, Piper Center, and Center for Developmental Disabilities, but these do not engage in billing insurance, and as a result, are not subject to the HIPAA Privacy and Security Rules. However, the TMRPA requires that such PHI be treated as if these operations were Covered Components.

B. Protected Health Information

PHI is any individually identifiable health information that can be linked to a particular person using one or more of eighteen (18) identifiers, from whatever source obtained, including information that was received, created, stored, used, or disclosed to Baylor, relating to: 1) an individual's past, present or future physical or mental health or condition; 2) providing health care to the individual; or 3) payment for past, present, or future health care provided to the individual. Those identifiers are:

1. name;
2. geographical identifier smaller than a state (except for the first 3 numbers of a zip code);
3. dates directly related to an individual (i.e. birthday, anniversary);
4. phone number;
5. fax number;
6. email address;
7. social security number;
8. medical record number;
9. health insurance beneficiary numbers;
10. account numbers;
11. certificate/license numbers (e.g., medical license, law license, CPA license);
12. vehicle identifiers (serial number and license plate number);
13. device identifiers and serial numbers;
14. internet URLs;
15. internet IP addresses;
16. biometric identifiers (including fingerprints, retina scans and voice prints);
17. full face photographic images;
18. any other unique identifier assigned for the purpose of coding data to an individual.

Health information that cannot be identified to an individual or that cannot be used to identify an individual is not PHI. However, care must be taken to verify that no identifier is associated with such information. For example, a list of diagnoses by themselves do not constitute PHI, but if the list includes birthdates or insurance policy numbers, it must be treated as PHI. Removing those identifiers is a process called "de-identification" and if done successfully, takes the data out of the PHI category and relieves the user from heightened treatment under HIPAA.

Some health information is not subject to HIPAA, even if it clearly identifies the individual because of exceptions enumerated in the law:

1. Treatment and Education Records covered by FERPA;
2. Baylor Human Resources employee records;
3. Health information in records about a person deceased more than 50 years;
4. Data that identifies an individual in research performed by an entity that is not subject to HIPAA (however, consider treatment under TMRPA); and
5. De-identified data.

Although such health information is not covered by HIPAA or this policy, care must be taken to keep such information secure and confidential. A good rule for Workforce members to follow with regard to this information is to consider the manner in which that Workforce member would want such information on themselves to be handled.

C. De-Identified PHI

As noted above, PHI is health information plus two or more identifiers. If information originally exists as PHI but is de-identified, it is no longer PHI and its use and disclosure will not require any individual to authorize its use. De-identification is preferred for research data sets because such data is not subject to HIPAA rules.

De-identification simply means that all of the identifiers of the individual (and sometimes, of parent, guardian, or other relatives and household members of the individual) are removed from the data set.

The HIPAA Privacy and Security Officers are available to confirm the information has been adequately de-identified, or to assist with obtaining the data in another form.

D. Designated Record Set

A Designated Record Set includes an individual's medical records that are used, in whole or in part, by a Covered Component to make health care decisions about that Individual. A typical Designated Record Set includes:

1) assessment and care notes;
2) diagnoses;
3) diagnostic studies and tests;
4) treatments and therapies;
5) assessment of outcomes;
6) referral notes and letters;
7) disposition and discharge records; and
8) billing records.

The Designated Record Set comprises all records of whatever type, electronic, paper, or other forms such as video, audio, photographic and the like, wherever and however kept. The fact that a particular record is not located in the Covered Component's physical location does not exclude it from the Designated Record Set.

When an individual makes a HIPAA request for access to or copies of their records, the Designated Record Set is what shall be provided in response to that request.

E. Designation of Covered Component Workforce

Each Covered Component should designate and document its HIPAA Workforce, and the HIPAA Contacts are responsible for updating the designation as necessary. The designation should include each individual's name, title, and training completion. Records shall be provided to University Administrative Support Services, as requested.

F. Access to PHI

Each designated Workforce member should be granted access to PHI depending on the actual need for such information to complete the duties of their job. Each individual's access should be guided by the principle that, unless otherwise approved, the minimum necessary access should be provided, and nothing more without further authorization.

Care providers, for example, should have full and complete access to a patient/client record so that the provider can give the best care and treatment based on all the available information. Those involved in administrative tasks such as scheduling should have more limited access. In the event a person's role

changes, the Covered Component's HIPAA Contacts should review and revise access as needed.

In the event of termination of employment, extended leaves of absence, retirement or reassignment to another role, the Workforce member's PHI access shall be reviewed and restricted accordingly, including but not limited to, changing access to all relevant electronic systems and secured physical storage areas.

G. HIPAA Training

Each Workforce member, as well as any support unit employee who handles PHI as a part of their duties, shall complete annual HIPAA training, which will be assigned through Ignite. Students with clinical assignments as a part of their coursework will also be assigned HIPAA training. This training shall be completed prior to being granted access to any PHI for new employees, and for existing Workforce members, access shall be removed until the training is completed. The HIPAA Contacts for each Covered Component shall ensure and keep record of its Workforce members' training.

II. Securing PHI

Keeping PHI private and confidential from access or disclosure to unauthorized persons is the essence of HIPAA. Workforce members must protect PHI in whatever form—electronic, paper, verbal or other tangible formats—from being shared with individuals without a need to know such information for the execution of their duties. As such, the following guidelines should be followed:

A. Physical Forms of PHI

For physical forms of PHI:

1. Do not remove any physical media containing PHI (such as paper files, photos, videos, x-rays, or recordings) from a Covered Component location unless approved by one of the Covered Component's HIPAA Contacts.
2. If you have permission from the HIPPA Privacy Officer to remove PHI from its secure location, do not leave it where it can be seen or easily stolen, such as in a visible location in your car.
3. Store PHI in drawers, cabinets, closets, or rooms with physical access controls such as locks or card swipe; do not store PHI in public areas or hallways.
4. Do not leave PHI unsecured on workspaces when not working on it. Lock all PHI away at night, and when not working on it, in a locked cabinet or locked office.

5. If a clinic facility is visible from the exterior, make sure that patient confidentiality is obtained by closing window coverings or confirming that the patient is comfortable with the circumstances.
6. When disposing of physical PHI, use a shredder to destroy it; never place confidential documents of any kind in the trash.
7. When sharing physical PHI by fax, mail, or courier services, ensure that the addresses and numbers are correct and use tamper-resistant envelopes or boxes.

B. Verbal Forms of PHI

For verbal PHI:

1. Do not discuss patient information in waiting rooms, elevators, hallways or other open public areas; use a treatment room or office with a closed door for such conversations.
2. Make efforts to minimize the ability of other patients and visitors in the waiting room to overhear conversations with staff.
3. Telephones—both landlines and mobile phones—are reasonably secure, but as with in-person conversations, be careful to have conversations in private locations.

C. Electronic PHI

For Electronic PHI:

1. Any storage of ePHI must receive approval of the HIPAA Security Officer.
2. ITS will publish the technical process and configuration requirements for the storage of ePHI. The documents will be collectively referred to as the Baylor University ePHI technology and security standards.
3. Only use devices, applications, services, and storage media approved by ITS. Personal and non-encrypted devices may not be used to access or send PHI. If in doubt, ask ITS.
4. Common means of communication, including Baylor email and text messaging from a cell phone, are not secure to HIPAA standards. PHI may be sent by email or text message ***only*** if the recipient has given written prior consent/waiver or has made a specific written request to receive unsecured messages via these means.
5. As between co-workers, it is permissible to text de-identified messages such as “your 10:00 client is running late.”
6. Configure workstations in a way that keeps PHI from being seen by unauthorized persons.
7. Change passwords often, and never share your password with anyone.

III. Reporting HIPAA Disclosure Incidents

Immediately report to HIPAA Privacy Officer, HIPAA Security Officer, or a HIPAA Contact any lost documents or other physical forms of PHI, loss of any device containing or permitting access to PHI, any accidental release of PHI outside Baylor, or any unusual activity that may indicate a system compromise (i.e., a "hack").

IV. Permitted Disclosures of PHI

Permitted disclosures of PHI fall into two categories—routine and non-routine.

Routine disclosures are those that are made regularly and frequently. For example, using PHI for treatment and to obtain payment for that treatment is a routine disclosure. PHI is also routinely used to manage a health care clinic. Detailed information on HIPAA's rules for these routine uses is provided in this policy to facilitate the routine activities of the Covered Components.

Non-routine disclosures are rarely encountered. Covered Components are always encouraged (and in some circumstances required) to contact the HIPAA Privacy Officer for guidance and/or approval in these non-routine circumstances.

This policy will also note when disclosures (both routine and non-routine) may or must be made without a written and signed Authorization.

A. Minimum Necessary Rule

When using or disclosing PHI, both internally and externally, the PHI shared by the Covered Component must be limited to only that which is necessary to accomplish the intended purpose thereof. However, the following exceptions exist to this rule:

- Between health care providers for treatment purposes whose professional judgment shall determine what information is necessary;
- When authorized by the patient, in person or in writing;
- When required by law (e.g., pursuant to subpoena, to governmental agencies for audit or public health purposes, required reports of abuse, neglect or domestic violence).

B. Limited Data Sets

A limited data set is de-identified PHI that excludes all direct identifiers of the individual (or of the individual's relatives, guardians, employers, or household members as described above), excepting dates. Limited data sets are frequently used in research.

A Covered Component may use or disclose a Limited Data Set only for the purposes of research, public health, or health care operations, and only after entering into a Limited Data Use Agreement with the recipient.

C. Data Use Agreements

A data use agreement is required for all sharing of limited data sets outside of Baylor. If a data use agreement is received from an outside entity, or if one is needed before sharing, contact the Chief Privacy Officer for review and approval of any data use agreement before data is shared.

If a Covered Component believes that a Data Use Agreement has been breached, the Covered Component must report the suspected breach to the HIPAA Privacy Officer, who will work with the Covered Component to investigate and, if necessary, cure the breach, end the violation, or discontinue disclosure of the data.

D. Billing/Payment

In the event a Covered Component engages in billing a patient's health insurance or Medicare/Medicaid coverage for services provided, an authorization is not required to use PHI for such purposes. Payment purposes include all activities directed at obtaining reimbursement for health care services, such as:

- verifying insurance coverage;
- starting an insurance claim;
- sending the claim to the patient and/or the patient's insurer;
- interactions with the patient's insurer for the purpose of obtaining payment;
- processing payments;
- collections activities; and
- evaluating an Individual's eligibility for financial assistance.

E. Using PHI for Health Care Operations

An authorization is not required for a Covered Component's operations to use PHI in the normal course of business. Operations, in this context, means the administrative functions of providing health care. The operations include such functions as:

- accreditation
- case management
- certification
- compliance
- credentialing and licensing

- financial and operational planning and budgeting
- human resource management, including personnel performance evaluations and review
- internal investigations
- quality assurance and improvement
- training.

In the operational use of PHI, the minimum necessary rule applies.

F. Disclosures to Designated Persons

Individuals may choose to involve third parties, such as family, friends, caretakers, and legal guardians, in their care, and Covered Components should disclose PHI to such parties to the extent the individual has authorized. This authorization may be accomplished by a formal, written Authorization signed by the patient and specifying what information may be shared. This is the preferred method of obtaining authorization and should be considered a best practice.

Authorization may also be accomplished informally, such as:

- the patient verbally directing the health care provider to share PHI with specified persons;
- by the party being present with the patient, who does not object to that individual hearing the information.

In addition, if a health care provider, through use of professional judgement, reasonably concludes from the context that the patient does not object to such disclosure to a third person, and also concludes that such person is involved in the patient's care, the provider may discuss the patient's diagnosis, condition, test results, treatment options/plan, and other matters appropriate for the circumstances.

G. Sharing PHI with Other Providers and Health Plans

HIPAA permits the sharing of PHI between health care providers and health care plans about patients who are common to both, for the purpose of coordinating treatment or to obtain payment for services. A patient Authorization is not required but is considered a best practice.

H. Disclosure of PHI to Business Associates

A Business Associate under HIPAA is a person or entity that is:

- not a member of the Covered Component Workforce,
- provides a service, or performs a function, or assists in the performance of a function or activity on behalf of a Covered Component, and
- in performing its duties for the Covered Component, may access, use, create or disclose PHI.

Covered Components may engage, or Baylor may engage on behalf of the Covered Components, third parties to perform services. When the services involve the outside entity accessing, using, creating or disclosing PHI held by any Covered Component, those entities are likely to be Business Associates of the Covered Component. PHI may not be disclosed to such third party until a Business Associate Agreement (BAA) is fully executed.

The Office of the General Counsel will either provide a standard form of Business Associate Agreement or will review and approve a third-party BAA. If the Covered Component cannot determine whether a BAA is necessary, the HIPAA Privacy Officer should be consulted.

On certain occasions, a Covered Component or other department may provide services to another person or entity that makes it a Business Associate to that third party. If an arrangement requires a Covered Component or other department of the university to access, use, create or disclose PHI for a third party, contact the HIPAA Privacy Officer to determine whether it is acting as a Business Associate and to prepare a BAA for that purpose.

V. Uses and Disclosures Required, Permitted and Prohibited by Law

Disclosures under this section should be coordinated by the Covered Component's Designated Individuals. The HIPAA Privacy Officer should always be notified in the event of such disclosures.

A. Required by Law

If a use or disclosure of PHI is required by law, no Authorization prior to disclosure is required, and Baylor will comply with any such required disclosure. Such instances include:

- Abuse and neglect mandatory reporting;
- Immunization records provided to other schools (e.g., meningitis);
- Public health reporting requirements;
- Other reports required by regulatory agencies (e.g., Food and Drug Administration).

B. Permitted by Law

In addition to the mandatory reports referenced above, Covered Components may, if they wish, disclose PHI without any patient Authorization in reporting:

- In response to a lawful subpoena, summons, discovery request, warrant, or other legal process (coordinate with Office of General Counsel);
- To law enforcement agencies, when:
  - the individual is a victim of a crime,
  - for the purpose of identifying a suspect,
  - the information is reasonably believed to be evidence of a crime that occurred at a Covered Component's facility, or the information is evidence of threatened criminal conduct;
- To workers' compensation programs related to work related injuries or illness;
- In response to a Health and Human Services audit or compliance review.

C. Prohibited Uses

Covered Component Workforce members may not access, disclose or use PHI for personal reasons unrelated to providing health care. Examples include:

- Posting any information, photos, videos or anything else about a patient on social media;
- Discussing patients, their conditions, treatment or other information with family members and close friends who are not part of the patient's care team;
- Discussing illness and injury conditions of student athletes with persons not a part of the care team;
- Baylor will not sell any PHI for direct or indirect forms of payment, unless specifically approved by the HIPAA Privacy Officer.
- Baylor will not use PHI to market third-party products and services to patients, whether health care related or not (excluding care and treatment by a health care provider during an appointment)
- Baylor will not use PHI, including contact information, for fundraising purposes.

VI. When an Authorization is Required

A. In General

In general, if a use or disclosure of PHI is not for the purpose of treatment, payment, for administrative purposes described herein, or for reasons that are

required or permitted by law, then the patient must sign a written Authorization allowing you to use/disclose the patient's information. Recipients of a written Authorization must make sure that the authorization is valid:

- it is filled out with enough specificity to understand the information to be provided;
- the expiration date has not passed;
- the patient (or legally authorized representative in the case of non-emancipated minors, deceased persons, and others whose estates are being managed through a court proceeding) has signed the form;
- there is no written revocation of that Authorization.

Baylor's HIPAA Authorization Form is located here: (https://go.web.baylor.edu/hipaa)

If a Covered Component receives a form from an external party, such authorization may suffice, but the Chief Privacy Officer must review and approve the form prior to any disclosure.

Any signed Authorization used to disclose PHI must be maintained in the records of the Covered Component for six years from the date.

Disclosures pursuant to a written Authorization should comply with the information requested in the Authorization as described by the patient—the Minimum Necessary rule does not apply to patient requests.

The PHI of a deceased individual is subject to HIPAA and remains protected under HIPAA for 50 years following the date of death.

B. Research Authorizations and Waivers

A written Authorization of a patient must be obtained prior to use and disclosure of PHI for research purposes unless the Institutional Review Board (IRB) has approved a waiver or alteration of Authorization.

C. Students and Observers

Students who participate in patient care within a Covered Component as part of their clinical training are members of the Workforce, and no Authorization is required for the student to access and use PHI. Care should be taken amongst students not to discuss the PHI of patients with other students who are not involved in the care of that patient, with the understanding that a generalized, non-identified discussion of a patient between students serves a legitimate pedagogical purpose.

Observers, such as prospective students, prospective faculty, shadowing students, and others who have a purpose related to the educational mission of the Covered Component (such as donors and accreditors) are permitted to observe patients so long as the patient has been informed of the observer's purpose and have an opportunity to object thereto.

VII. Patient's Rights Under HIPAA

A. Right to Notice of Privacy Practices

HIPAA requires that patients be informed of the potential uses and disclosures of their PHI, and of their rights and the Covered Component's responsibilities under HIPAA.

Baylor's Notice of Privacy Practices (NPP) form is located here: (https://go.web.baylor.edu/hipaa)

The patient must receive a copy of NPP no later than the first date the Covered Component provides health services to the individual, unless the circumstances make it reasonably impracticable, such as when contact is electronic, telephonic or under emergency circumstances, and then the NPP must be provided as soon as reasonably practicable. A signed copy must be placed in the records of the patient, or a notation of the patient's refusal to sign the same.

B. Right to Access and Copy Own Health Record

Except in limited circumstances, patients have the right to access, inspect, amend or correct, and receive a copy of their PHI in the Covered Component's Designated Record Set.

Use of Authorization Form:
A written request is not legally required in order to provide copies of the Designated Record Set, in whole or in part, to the patient to obtain his/her own information. However, a written request on an approved Authorization form will ensure the request is what the individual wishes to have and is done so in a timely manner.

A Designated Record Set is a group of records maintained by or for a Covered Component that is: 1) the medical records and billing records about individuals maintained by or for a covered health care provider; 2) the enrollment, payment, claims processing, and case or medical management record systems maintained by or for a health plan; or 3) used, in whole or in part, by or for the covered entity to make decisions about individuals.

When complete medical records (i.e., the Designated Record Set plus records not defined in the Designated Record Set but kept on the patient) are requested, an Authorization is required. **NOTE:** Complete medical records do not include psychotherapy notes.

Time to respond:
Record requests should be fulfilled as soon as practicable, but generally, within 30 days from the date the request was received. If the Covered Component is not able to provide the requested records or respond to the request within 30 days, the Covered Component should provide the requestor written notification of the reasons for the delay and the expected date of fulfilling the request.

Format and Fee:
Records should be provided in the format requested by the patient, if reasonably practicable. A reasonable fee may be charged for copying and mailing records, but no fee may be charged for retrieving records. A fee may not be charged in the limited instance where records are required for submitting a claim under any provision of the Social Security Act (i.e., disability, Medicare, Medicaid) or any need-based state or federal program.

If the individual requests inspection rather than a copy, the Covered Component shall arrange for a mutually convenient time and place for the individual to inspect the Designated Record Set.

When Requests May be Denied:
A Covered Component may, under limited circumstances, deny access or copies of medical records of an individual. A decision to deny access or copies must be approved by the HIPAA Privacy Officer, who will also assist in drafting written notification to the individual of such denial. The limited occasions include:

- Requests for psychotherapy notes;
- Where a health care professional determines that the release of such records to the patient presents a danger to the patient or others;
- Where the record contains the names of others whose privacy or safety may be impacted;
- Where the patient participated in research and release of the requested information is restricted during the course of the research;
- Where the source of the requested information is someone other than a healthcare provider (i.e., parent/guardian/other third party providing information under promise of confidentiality).

Upon a determination that the request should be denied, the Covered Component and HIPAA Privacy Officer shall notify the individual in writing of the denial, including:

- A statement of the reason for denial.
- A statement of the individual's rights and instructions on:
    - How to request a review by an independent licensed health care professional (if applicable);
    - Filing a complaint with one of the Covered Component's HIPAA Contacts; and
    - Filing a complaint with the United States Secretary of Health and Human Services.

C. Right to Request Amendment or Correction

Individuals have the right to request in writing that records in a Designated Record Set be amended or corrected. The right to request is unrestricted; however, the right to amend or correct is not.

An individual who desires an amendment must provide a written statement identifying the record the individual considered inaccurate or incomplete and a statement of the information they wish to be added or substituted to the record.

One of the Covered Component's HIPAA Contacts shall review it. If the request is to correct demographic information or any information that originally came from the individual and which the individual says was recorded inaccurately, the HIPAA Contact, in his/her judgment, may make the correction. Examples include correcting spellings, ethnicity, date of birth and similar matters.

Any requests to amend information entered in the record by a treating health care provider (e.g., diagnosis; prognosis; history of condition; etc.) shall be forwarded to that provider and to Baylor's HIPAA Privacy Officer. The treating healthcare provider who made the entry will determine whether to allow the amendment. The request to amend may be denied if the original record is accurate.

The decision to grant or deny a request to amend should be made within 60 days of the request, by the Covered Component in consultation with the HIPAA Privacy Officer. The decision shall be communicated in writing to the requestor with the changes being made, or in the case of a denial, the reasons for such denial and instructions on how to appeal that denial. These communications should be placed in the individual's record.

If an amendment or correction is made, a notation shall be made in the records that indicates "amendment" at the location of the corrected record, together with the date of the change and the person making the change.

D. Right to an Accounting of Disclosures

Patients have the right under HIPAA to request an Accounting of disclosures of their health information.

An Accounting is a listing of all disclosures made without the individual's Authorization within the 6-year period prior to the date of the request, or for a shorter period if the individual may request. The Accounting would include the following types of disclosures:

- Public health reporting,
- Law enforcement and other government agencies, and
- Research.

But does not include disclosures:

- To carry out treatment, payment and health care operations;
- To the requesting individual;
- Incidental disclosures;
- Pursuant to an authorization;
- To persons involved in the individual's care or other notification purposes;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials;
- As part of a limited data set;
- That occurred prior to the compliance date for the covered entity.

The request must be made in writing specifying the period for which the Accounting is requested. A response to such request shall be made within 60 days, and should contain:

- The date of each disclosure;
- To whom the disclosure was made;
- A description of the PHI disclosed; and
- The reason for the disclosure.

If the disclosure is made for the purpose of research, the Accounting should also state:

- The name and description of the research protocol and selection criteria;
- The PHI disclosed; and
- The date of disclosure.

All responses to such requests should be coordinated with the HIPAA Privacy Officer if any Request for Accounting is received.

A fee may not be charged for the first Accounting in a 12-month period, but a reasonable fee may be charged thereafter for additional requests within that period.

E. Right to Request Restriction

Individuals have the right to request a restriction on uses and disclosure of their PHI. Typical requests include asking the Covered Component to not share any information, or a certain type of information, with a family member or friend of the Individual, which should be granted in most circumstances. The Covered Component should accommodate all reasonable requests but should not agree to a restriction if it is not feasible to comply with it.

All requests for restriction shall be forwarded to the Covered Component's HIPAA Contacts, who must consult the HIPAA Privacy Officer before denying. The Covered Component should inform the Individual in writing of its decision.

An Individual may make a request for a restriction either in writing or orally. If an oral request is made, the Covered Component should document the request in the Individual's record. There is no form required for requesting the restriction, but the writing needs to identify the information restricted and the persons or entities to whom disclosure would be barred. The Individual does not need to explain the reason for the request.

HIPAA recognizes that Individuals may wish to obtain specific health care services without informing their health care insurers. As such, an Individual may request that specific information not be sent to the Individual's health insurer, so long as the Individual has paid for the service in full.

Certain uses and disclosures may not be restricted:

- Information necessary for providing emergency treatment;
- Circumstances for which an Authorization or opportunity to agree or object is not required (e.g., public health requirements, national security);
- Abuse, neglect or domestic violence reporting requirements;
- Disclosures required by the Secretary of the Department of Health and Human Services to investigate or determine compliance with HIPAA.

The Covered Component may terminate a requested restriction if:

- the Individual requests the termination in writing;

- the Individual verbally requests termination and such request is documented.

F. Right to Request Confidential and Alternate Modes of Communication

Individuals have the right to request alternate communication modes with (e.g., written, electronic or oral) or at an alternative location (e.g., work, school or home). Requests should be submitted by the Individual in writing. The Individual is not required to provide a reason for the request.

When considering alternate communication requests, it is important to understand that text messaging and email are not secure under HIPAA standards. However, an individual may request non-secure communications if they have done so in writing prior to such communication. A form to be used for consent to non-secure communications can be found at https://go.web.baylor.edu/hipaa.

If a Workforce member receives a non-secure email or text from a patient without a signed consent to non-secure communication, the Workforce member should respond by sending a new email message (DO NOT REPLY to email or texts received to avoid re-publishing any identifiable health information in the initial message) with a link to the consent form:

Thank you for contacting me. Baylor _____ Clinic has a policy of not communicating with patients via regular email or text because they are not considered secure, and communications may be intercepted. If your preference is to communicate through text or email, please sign and return the consent form found at the following link.

Any request from an Individual to receive communications by an alternative means should be accommodated if reasonably possible. Before denying any such request, consult with the HIPAA Privacy Officer. Individuals making a request should be informed in writing of the decision to approve or deny alternative communication.

G. Right to Complain

Individuals have a right to make complaints if they believe their information privacy or security rights have been violated. The Covered Component may not retaliate against any patient who makes such a complaint. Complaints should be directed through ReportIt at https://www.baylor.edu/reportit/. Alternatively, an anonymous report may be submitted through EthicsPoint at https://bayloruniversity.ethicspoint.com/.

The HIPAA Privacy Officer shall be responsible for investigating and responding to such complaints.

VIII. Unauthorized Disclosures and Inadvertent Releases of PHI

Any Workforce Member who learns of or suspects an unauthorized disclosure or inadvertent release of PHI may have occurred must immediately notify their supervisor (and/or the Covered Component's HIPAA Contacts if not the supervisor) and the HIPAA Privacy Officer. Failure to make a report may lead to discipline, up to and including termination of employment.

No Baylor employee may intimidate, harass, threaten, coerce, discriminate against, or take other retaliatory action against any individual for his/her exercise of any right established by, or for participation in any process provided for, these policies or the law, including:

- Filing a complaint with the Covered Component;
- Filing a complaint with governmental authorities;
- Assisting or participating in an investigation or compliance review;
- Testifying in a proceeding or hearing by governmental authorities under HIPAA;
- Opposing, based on a good faith belief that an act or practice is unlawful under HIPAA.

The HIPAA Privacy Officer and HIPAA Security Officer are responsible for receiving and responding to all reports of data breaches involving PHI in violation of this policy or of HIPAA. This responsibility includes:

- Keeping record of all reported potential breaches;
- Investigating each report to determine whether a breach occurred;
- Documenting the conclusion;
- Taking all required steps to report and remedy the breach to the appropriate parties and governmental entities per Baylor's data breach response plan and applicable law regarding breach notifications.

If a breach, including unauthorized access or inadvertent disclosures, of PHI was caused by a Workforce member, that person may be subject to disciplinary action, up to and including termination of employment, and the possibility of civil and/or criminal liability.

IX. Documentation and Retention

The HIPAA Privacy Officer must keep a copy of all current HIPAA policies and procedures, and a copy of any superseded versions of the same which were effective during the preceding six (6) years.

In addition, the HIPAA Privacy Officer shall maintain a copy of all incident reports, investigative reports, regulatory responses, remedial responses, notice letters, access and Accounting requests, as well as information access authorizations and HIPAA training completion records for employees. These records shall be kept for six (6) years.

X. Exceptions

The HIPAA Privacy Officer and HIPAA Security Officer will jointly review any requested exceptions to the requirements set forth in this policy. Exceptions will be granted if a thorough review of the situation demonstrates appropriate compensating controls have been implemented, and the risk posed by the exception is reasonable and acceptable.