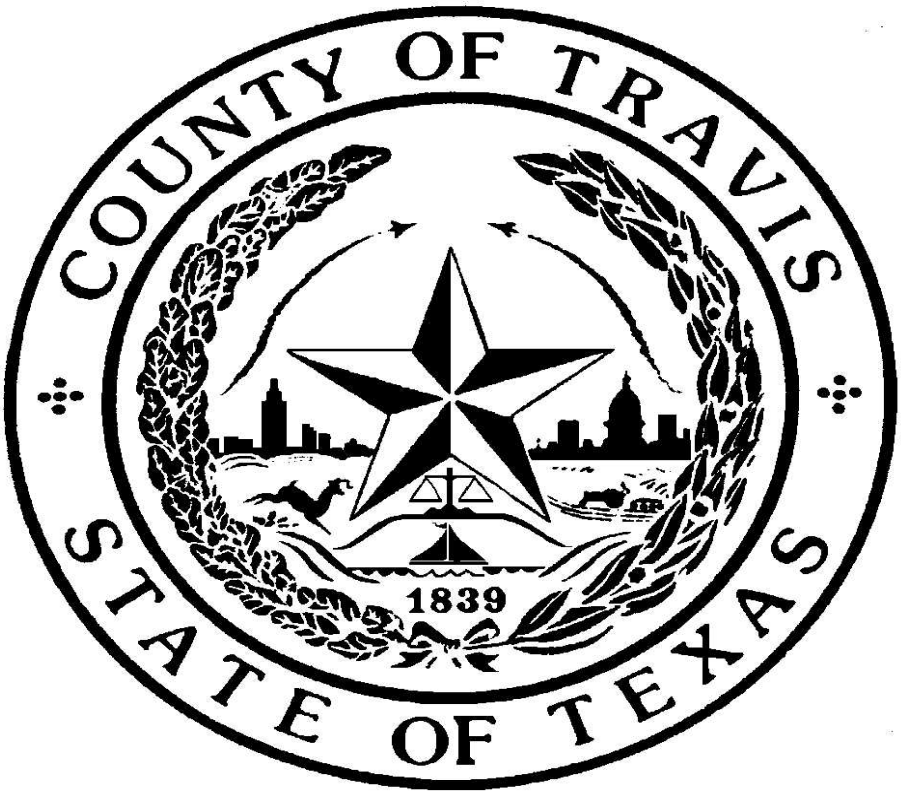


Travis County Health Insurance Portability and Accountability Act (HIPAA), Protected Health Information (PHI) Handbook

Policies

PRIVACY

About this Handbook:

This Policy Handbook contains the Privacy Policies and Procedures of Travis County ("County"). Its purpose is to ensure the privacy of Protected Health Information (PHI), and compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Texas Medical Records Privacy Act, and other applicable laws, regulations, and rules regarding confidential medical information. This handbook contains the policies and procedures you need to make decisions about handling PHI. The policies apply to all County workforce members (see "Definitions" on page 4 for workforce), who provide services for a County HIPAA covered component and who come into contact with PHI.

Information Sharing Within the County:

Travis County is a HIPAA "hybrid entity." That means that some of its divisions and programs handle PHI while others do not. The Commissioners Court, in consultation with affected department heads, has formally designated the programs within the County that are "covered components" under HIPAA. What does this mean to Travis County workforce members? Workforce members in a covered component can only share PHI within his or her covered component, and only as needed to provide the services required. A workforce member may not share PHI with anyone outside of his or her covered component, not even when it is with another covered component unless it is for a legally authorized purpose, or in a legally authorized manner. Simply put, do not assume you can share information simply because it would be shared with another part of the County organization. Workforce members working with PHI always must refer to HIPAA rules before and when using or disclosing any PHI.

Travis County's Commitment to Privacy:

Travis County is committed to full compliance with all Federal and State regulations and to the protection of the health information it holds.

Beyond this commitment, Travis County Government values an individual's privacy regarding his or her medical information.

The Travis County HIPAA Compliance and Privacy Officer is responsible for maintaining this handbook and for working with Privacy Liaisons to ensure policies meet the County departments or program's business and operational needs while remaining compliant with Federal and State statutes. Should you ever have a question or a concern about handling PHI, the HIPAA Compliance and Privacy Officer is available to assist you.

Travis County HIPAA Compliance and Privacy Office (CAP)

HIPAA Compliance and Privacy Officer: (512) 854-6278

HIPAA CAP Hotline: (512) 854-1114

Email: privacy@traviscountytx.gov

Appendix

Forms:

1. **Notice of Privacy Practices:** ENGLISH - SPANISH
2. **Privacy Complaint Form:** ENGLISH
3. **Authorization for Release of PHI:** ENGLISH - SPANISH
4. **Request for Restrictions for Uses and Disclosure of PHI:** ENGLISH - SPANISH
5. **Request for Confidential Communications:** ENGLISH - SPANISH
6. **Request to Access Records:** ENGLISH - SPANISH
7. **Request for Amendments to PHI:** ENGLISH - SPANISH
8. **Request for Accounting of Disclosures of PHI:** ENGLISH - SPANISH

DEFINITIONS

Authorization: The Authorization Form (Form 3) maintained and updated by the HIPAA Compliance and Privacy Officer.

Business Associate: Any Individual or entity, other than a workforce member, that creates, receives, maintains, or transmits PHI on behalf of a covered component or provides certain services that involve the disclosure of PHI/PII.

Business Associate Agreement (BAA): Is a written arrangement that specifies each party's responsibilities when it comes to PHI. HIPAA requires Covered Entities to only work with Business Associates who assure complete protection of PHI. These assurances must be in writing in the form of a contract or other agreement between the Covered Entity and the Business Associate.

Breach: An incident involving the improper or unauthorized access, collection, use, disclosure, or retention and/or disposal of personal information (PHI). Such activity is deemed to be "improper" or "unauthorized" if it occurs in contravention of the Privacy Act.

Commissioners Court: In Travis County, as a group, the commissioners and county judge are the chief policy-making and administrative branch of county government. Among their many functions, the court sets the tax rate, determines fees for many county services, and determines how the collected revenues will be distributed among different county departments to provide services to the community.

Complaint: Is a statement by an individual about an act or practice of a relevant entity (the respondent for the complaint) in relation to the individual's personal information that is a breach of the relevant entity's obligation.

Complainant: The individual who makes the complaint.

Covered Component: A program, department or division that performs the functions of a health plan or a health care provider and that Travis County as a hybrid entity has designated as a covered component in the *Order of the Travis County Commissioners Court declaring Travis County a Hybrid Entity, Designating Covered Entity and Business Component Units, Designating Privacy Official and Identifying Security Official.*

De-Identification: Process used to ensure personal data cannot be linked to an individual. De-identification is achieved by removing certain data elements from a data set so that the information could no longer be used to identify a specific individual.

Designated Record Set: A group of records maintained by a covered component within Travis County that includes patient medical and billing records for providers; the enrollment, payment, claims adjudication, and cases or medical management record systems maintained by or for a health plan, or used in whole, or in part, by or for the covered component to make decisions about individuals.

Electronic Protected Health Information (ePHI): is protected health information that that is produced, saved, transferred, or received in an electronic form.

Encryption: The conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals

the data's original meaning. Applicable law may provide for a minimum standard for compliant encryption, such as Health Insurance Portability and Accountability Act (HIPAA) or National Institute of Standards and Technology (NIST) standards.

Governing Committee: A group composed of Travis County workforce members and department heads that meet to make decisions about and recommendations related to HIPAA and medical privacy within Travis County.

Health Insurance Portability and Accountability Act (HIPAA) Compliance and Privacy Officer: A person directly employed by Travis County, appointed by the Travis County Commissioners Court and authorized by any elected or appointed officials to develop, implement, and enforce (with respect to Commissioners Court covered components) Travis County's compliance with HIPAA and medical privacy laws.

HIPAA Privacy Rule: Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (ePHI).

Hybrid Entity: A single legal entity that is a covered entity under the HIPAA Privacy Rule and whose business activities include both covered and non-covered HIPAA functions, and that designates health care components in accordance with 45 C.F.R. § 164.105(a)(2)(iii) (C). A Hybrid Entity must designate as a health care component, any other components of the entity that provide services to the covered functions for the purpose of facilitating the sharing of PHI (as defined below) with such functions of the hybrid entity without business associate agreements or individual authorizations.

Incident: Anything that a staff member feels should be report or addressed by the HIPAA Compliance and Privacy Office. Anything reported to the HIPAA Compliance and Privacy Office is considered an incident until a full investigation can be conducted by the HIPAA Compliance and Privacy Office makes a determination if incident is a Policy Violation, Breach, etc.

Individual: A person who is the subject of PHI maintained by a covered component of Travis County. **A Personal Representative (defined below) is treated as the Individual for purposes of administering Travis County HIPAA policies and procedures.**

Institutional Review Board: A committee consisting of appropriate persons and designated by an entity, such as an academic institution, to protect the rights of human subjects involved in research studies.

Limited Data Set: A limited set of identifiable information defined in the HIPAA privacy regulations that may be released for research, public health, or health care operations purposes only when certain conditions are met.

Personally Identifiable Information (PII): any information used to identity an individual directly or indirectly.

Personal Representative: A person authorized and designated by an Individual or a court acting on an Individual's behalf, or who is legally authorized by a state or other applicable law to act on behalf of an Individual in making health care decisions**.**

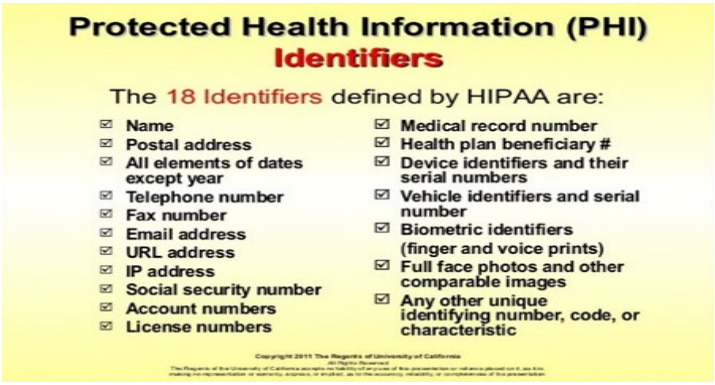
Power of Attorney: A written, witnessed, and notarized document in which one person appoints another person to act on his or her behalf, and authorizes the appointed person to perform the acts or functions stated in the document on behalf of the first person.

Privacy Liaison: A person within each department, division, or program identified as the person accountable for ensuring that the department, division, or program complies with the appropriate federal and state medical privacy laws.

Professional Judgement: Judgement that is informed by professional knowledge of curriculum expectations, context, evidence of learning, methods of instruction and assessment, and the criteria and standards that indicate success in student learning. In professional practice, judgement involves a purposeful and systematic thinking process that evolves in terms of accuracy and insight with ongoing reflection and self-correction.

Program: A section within a department in Travis County that either reports to the Commissioners Court or another elected or appointed official.

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium (including electronic (ePHI), oral, or paper) by a Covered Component or its Business Associate. Individually identifiable health information relates to the past, present, or future physical or mental health condition of an individual; the care of the individual; or the past, present, or future payment for healthcare to an individual; and includes enough information to provide a reasonable basis to believe that the information could be used to identify the individual.



Reasonable Diligence: The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. It may also be described as the care and attention that is expected and exercised by a reasonable and prudent person under the circumstances.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an information system that does not result in a breach. Examples include: Computer system breaches; Unauthorized access to, or use of, systems, software, or data; Unauthorized changes to systems, software, or data; Loss or theft of equipment storing institutional data; Denial of service attack; Interference with the intended use of IT resources; Compromised user accounts.

Workforce Member: An employee, volunteer, trainee, or other person whose conduct, in the performance of work for Travis County, is under the direct control of Travis County, whether or not they are paid by Travis County.

Policy Index

Travis County covered components work with PHI (Personal Health Information) and PII (Personally Identifiable Information) in different ways, so there are some situations in which different HIPAA rules apply. **Policies containing these differences are noted in ITALICS** as: *****SPECIAL NOTE:*** below. Contact the HIPAA Compliance and Privacy Officer if you are unsure if your status is a health care provider or a health plan.

1. **Privacy Administration:**
   - 1.1 Management of Privacy Complaints
   - 1.2 Prohibition of Intimidating or Retaliatory Acts
   - 1.3 Reporting, Investigating, & Documenting Suspected Breaches of PHI/PII
   - 1.4 Mitigation from Harm Resulting from PHI/PII Breaches
   - 1.5 Breach Notification
   - 1.6 Education and Training
   - 1.7 Sanctions

2. **Uses and Disclosures of PHI/PII:**
   - 2.1 Minimum Necessary Standard
   - 2.2 Disclosure to Persons Involved in Individual's Care
   - 2.3 Verifying Identity and Authority of a person requesting PHI/PII
   - 2.4 Permitted Uses and Disclosures of PHI/PII
     *****SPECIAL NOTE: for Plans, rule difference for corrections***
     A) 2.4.1 Disclosing PHI/PII for Research
   - 2.5 Authorization for Release of PHI/PII
   - 2.6 De-identification of PHI/PII
   - 2.7 Business Associates
   - 2.8 Safeguarding PHI/PII: Use and Storage

3. **Individual's Access to PHI/PII:**
   - 3.1 Provision of Notice of Privacy Practices
     *****SPECIAL NOTE: Rule Differences: Plans, Providers, Corrections***
   - 3.2 Rights to Access PHI/PII
     *****SPECIAL NOTE: Differences for Corrections***
   - 3.3 Requests for Restrictions on Uses and Disclosures
   - 3.4 Request for Confidential Communications
     *****SPECIAL NOTE: Rule difference for health plans***
   - 3.5 Designated Record Sets
     *****SPECIAL NOTE: Differences for health plans and health providers***
   - 3.6 Requests to Amend Records
   - 3.7 Accounting of Disclosures

Privacy Administration

Policy # 1.1

Management of Complaints

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To establish a formal complaint process for individuals to promptly resolve concerns about the privacy and confidentiality of PHI.

Policy: Travis County investigates and resolves complaints about violations of an Individual's privacy rights and complaints about specific Travis County policies or procedures related to the privacy and the security of PHI. Travis County does not require an Individual to waive the right to complain to receive healthcare treatment or to access health plans. **Workforce members involved in any complaint processes must keep information related to the complaint and complainant as confidential as possible.**

Process:

1. Individuals wishing to make a complaint are instructed to contact the Travis County HIPAA Compliance and Privacy Office, or department Privacy Liaison.

2. Individuals may make a complaint via email, phone, or by filling out the Travis County HIPAA Complaint Form. Complaints received by phone or email are recorded by the HIPAA Compliance and Privacy Office or Privacy Liaison on a Travis County HIPAA Complaint Form.

3. Privacy Liaisons send copies of complaint received by them to the HIPAA Compliance and Privacy Office one business day after receipt. The HIPAA Compliance and Privacy Office logs the complaint.

4. The HIPAA Compliance and Privacy Office or Privacy Liaison communicates with the complainant in writing acknowledging receipt of the complaint and that it will be addressed within thirty (**30**) days, as appropriate. The HIPAA Compliance and Privacy Office will notify the complainant of any delays in meeting this timeline.

5. Complaints are resolved within thirty **(30)** days of the date received by the HIPAA Compliance and Privacy Office or Privacy Liaison unless extenuating circumstances require longer.

6. The HIPAA Compliance and Privacy Office retains documentation related to complaints for at least six **(6)** years from the date of receipt. This documentation includes the complaint, documentation of the resolution of the complaint, and all correspondence with the complainant and others relating to the complaint.

Complaints Submitted pertaining to Commissioners Court Programs

The HIPAA Compliance and Privacy Office directly handles privacy complaints involving departments that report to the Commissioners Court according to the following procedures:

1. The HIPAA Compliance and Privacy Office notifies the department head or division manager, responsible for supervising the person or covered component that is the subject of the complaint.

2. The HIPAA Compliance and Privacy Office investigates the complaint, interviews involved persons and reviews applicable operational procedures. Departments furnish information necessary for the investigation in a timely manner. The HIPAA Compliance and Privacy Office will document **ALL** Complaints as required by 45 CFR Section 164.530(d)(2).

3. The HIPAA Compliance and Privacy Office prepares a report which may be provided to Legal Counsel for review and advice. The HIPAA Compliance and Privacy Office will determine a resolution of the complaint, which may include suggested operational changes, or changes to policies and procedures.

4. When the findings of the investigation indicate that an employee has violated the privacy policies, the HIPAA Compliance and Privacy Office consults with Human Resource Management Division (HRMD) Employee Relations appropriate Corrective/Disciplinary Actions in accordance with the Corrective/Disciplinary Action Policy. The HIPAA Compliance and Privacy Office informs appropriate managers, **as necessary**, of the recommendation.

5. When the findings of the investigation reveal that a workforce member other than an employee, such as a contractor or a volunteer, has violated the privacy policies, the HIPAA Compliance and Privacy Office will work with the County Executive that oversees the covered component to determine the most appropriate resolution in accordance with the Corrective/Disciplinary Action policy.

6. Departments inform the HIPAA Compliance and Privacy Office of Corrective/Disciplinary Action applied, **if any**, and the outcomes for documentation purposes as required by 45 C.F.R. §164.530(e)(1)(2).

7. The HIPAA Compliance and Privacy Office notifies the complainant, **in writing**, of the resolution of the complaint.

Complaints Submitted pertaining to Non- Commissioners Court Departments

1. When complaints are received by the HIPAA Compliance and Privacy Office, it will forward a copy of the complaint with a tracking number to the appropriate Privacy Liaison within one business day of the receipt of the complaint.

2. The Privacy Liaison, or other workforce member as designated by the Covered Component, initiates an investigation of the complaint in accordance with its department protocol. The Covered Component may consult with the HIPAA Compliance and Privacy Office during the investigation for technical assistance and specific requirements of HIPAA and other medical privacy laws.

3. The Department determines a resolution of the complaint. Departments are encouraged to include and

apply Corrective/Disciplinary Actions in accordance with the Corrective/Disciplinary Action policy in the resolution. The HIPAA Compliance and Privacy Office and the Human Resources Department are available to provide technical assistance and recommendations during this process.

4. The Department or the HIPAA Compliance and Privacy Office/the Privacy Liaison (at the Department's request), responds to the complainant within thirty **(30)** days of receipt of the complaint. This response will advise the Individual of the resolution of his or her complaint.

5. The Department provides the HIPAA Compliance and Privacy Office with **ALL NECESSARY DOCUMENTATION** related to the complaint. The documentation includes the complaint, documentation of the resolution of the complaint and relevant investigation information to enable the HIPAA Compliance and Privacy Office to document **ALL** Complaints as required by 45 CFR Section 164.530(d)(2).

6. The HIPAA Compliance and Privacy Office retains documentation related to the complaint for at least six **(6)** years from the date of receipt.

Privacy Administration

Policy # 1.2

Prohibition of Intimidating or Retaliatory Acts

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To define actions that are prohibited when an Individual exercises his or her rights created by the federal HIPAA Laws and PHI Regulations.

Policy: Workforce members shall not intimidate, threaten, coerce, discriminate, or take other retaliatory actions against an individual or any other person for exercising any rights or for participating in processes established under the HIPAA Laws as well as PHI Regulations or for opposing acts or practices made unlawful by HIPAA **and/or** PHI if the Individual or person has a **good faith** belief the practice opposed is unlawful. Substantiated reports of intimidating, discriminatory, or retaliatory behavior will result in the imposition of Corrective/Disciplinary Actions.

Process:

1. Workforce members who suspect that intimidating, threatening, discriminatory, coercing, or retaliatory acts have been or are being taken toward an individual or other persons who have, **in good faith**, exercised their rights under HIPAA, PHI, or have participated in processes established by HIPAA, PHI must report this to the HIPAA Compliance and Privacy Office or Privacy Liaison **immediately**. If the HIPAA Compliance and Privacy Office or Privacy Liaison is implicated in retaliation, the workforce member should report to their Department Head or other Elected or Appointed Official.

2. The HIPAA Compliance and Privacy Officer informs the Department Head or Governance Committee member, **and/or** Legal Counsel, **as applicable**, if he or she becomes aware that an Individual has filed a complaint with the United States Department of Health and Human Services, or the State Attorney General. Has testified, assisted, or participated in any investigation or opposed any act or practice the Individual believes to be unlawful.

Reports Made Pertaining to Commissioners Court Departments

1. The HIPAA Compliance and Privacy Officer first contacts the head of the involved department, executive manager, HRMD, or the Governance Committee member.

2. The HIPAA Compliance and Privacy Office consults with HRMD and reviews applicable County policies. If it is determined that HRMD is the more appropriate body to review the complaint, then the HIPAA Compliance and Privacy Office will provide assistance.

3. The HIPAA Compliance and Privacy Officer works with the HRMD, **as appropriate**, to conduct a full investigation into the allegations. Any impermissible disclosures of PHI are considered in the investigation.

4. If the allegation in the complaint is substantiated, the HIPAA Compliance and Privacy Officer will work with the HRMD, **as appropriate**, regarding Corrective/Disciplinary Actions.

Reports Made Pertaining to Non- Commissioners Court Departments

1. The HIPAA Compliance and Privacy Officer contacts the Department head, elected/appointed official or Governance Committee member, **as appropriate**, for non-Commissioner Court departments to report the alleged act of retaliation.

2. The Department head, elected/appointed official or Governance Committee member initiates an investigation into the report in accordance with department protocol. If it is discovered that intimidating, discriminatory, coercive, or retaliatory behavior did occur, **the department is responsible** for taking appropriate action against the responsible Travis County employee(s) in accordance with department Corrective/Disciplinary Policies. The HIPAA Compliance and Privacy Officer is available to consult with the Department regarding corrective actions.

Privacy Administration

Policy # 1.3

Reporting, Investigating, & Documenting Suspected Breaches of PHI

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To provide a process by which to conduct a thorough investigation of any reported acquisition, access, use or disclosure of PHI that is not authorized by HIPAA (a breach or a potential breach).

Policy: Suspected breaches are treated as a priority by workforce members and other involved parties. Workforce members who suspect a breach of PHI must report this information immediately. Travis County investigates any suspected breaches of PHI of which it becomes aware.

Breaches are treated as "discovered" on the first "Date of Discovery" any workforce member in the covered component becomes aware of the breach OR the first "Date of Discovery" a workforce member would have been aware of a breach by exercising reasonable diligence, whichever is earlier.

Process:

Reports of Suspected Breaches of PHI:

1. Workforce members who suspect a breach must ***immediately*** report this information to the appropriate management personnel, as described in the table below. Workforce members should provide as much information as possible about suspected breach including, but not limited to:

    a) **Date of Discovery**
    b) **Discovered by who**
    c) **How it was discovered**
    d) **Employee(s) Involved – Any contact information**
    e) **Devices used and any associated numbers attached to devices**
    f) **Description of Incident – Detailed as possible**
    g) **Has employee been questioned by the appropriate staff (Security/HIPAA Compliance and Privacy)**

POTENTIAL BREACH	REPORT TO
Suspected virus, spyware, and other intrusions	➢ **ITS Service Desk at Extension = Internally: 4-9175** **1. (Externally: 512-854-9175)** • ***For after-hours calls, follow the prompts to report the incident as "critical."*** ➢ **STARFlight: W*orkforce members report directly to command staff, who then liaise with ITS. After hours, command staff should be paged to notify of incidents.***
Violations, or suspected violations, of access to confidential information and/or PHI	**1. ITS Service Desk at Extension = Internally: 4-9175** • **(Externally: 512-854-9175)** • ***For after-hours calls, follow the prompts to report the incident as "critical."*** ***2. AND Department Privacy Liaison or HIPAA Compliance and Privacy Officer*** ➢ **STARFlight: W*orkforce members should notify STARFlight command staff of issues requiring immediate attention after hours.***
Loss or theft of computer equipment, mobile device, or tablets	➢ ***Immediate:* ITS Service Desk at Extension = Internally: 4-9175** • **(Externally: 512-854-9175)** • ***For after-hours calls, follow the prompts to report the incident as "critical."*** ➢ **STARFlight: W*orkforce members report directly to command staff, who may enact security counter- measures and liaise with ITS. After hours, command staff should be paged to notify of incidents.*** **1. Then:** • **Supervisor(s)** • **Department Privacy liaison for non- Commissioners Court Departments** • **HIPAA Compliance and Privacy Officer for Commissioners Court Departments**
An event or incident that the workforce member is unsure of where to report	➢ ***Non-Commissioners Court Departments:*** **1. Supervisor and Department Privacy Liaison** ➢ **Commissioners Court Department:** **1. Supervisor and HIPAA Compliance and Privacy Officer**

1. Reporting a suspected breach can be made by phone, or email (privacy@traviscountytx.gov). Please keep in mind the severity of data disclosures. **It always recommended to speak to someone directly**.

2. Managers, Privacy Liaisons, and IT personnel who receive reports of suspected breaches must ***immediately*** inform the HIPAA Compliance and Privacy Office **(512-854-1114)**. Appropriate department IT/Security personnel should also be notified of any suspected breaches by the HIPAA Compliance and Privacy Office and workforce members.

3. The HIPAA Compliance and Privacy Office is responsible for ensuring timely checking of voice and email messages and will confirm receipt of reports with the workforce member.

Investigation of Suspected Breaches of PHI

1. The HIPAA Compliance and Privacy Officer informs the County Executive or Department Head responsible for covered components in which a breach is reported of any investigations of suspected breaches of PHI unless circumstances suggest that this action would adversely impact the investigation. The HIPAA Compliance and Privacy Officer uses their discretion at any point during the investigation about whether-or-not the Commissioners Court or sub-committee of the Commissioners Court should receive information pertaining to the potential breach or investigative process. Court or sub-committee of the Commissioners Court should receive information pertaining to the potential breach or investigative process.

2. The HIPAA Compliance and Privacy Officer or Privacy Liaison investigates the potential breach. The HIPAA Compliance and Privacy Officer is responsible for investigations in non-Commissioners Court Departments. The HIPAA Compliance and Privacy Officer coordinates with the Security Officer and will, in conjunction with the Security Officer and workforce members within the affected covered components, gather all relevant information related to the suspected breach.

3. Workforce members requested to provide information pursuant to a breach investigation must fully cooperate with the person making such requests and provide information within the timelines requested by the HIPAA Compliance and Privacy Officer **and/or** Security Officer.

4. The HIPAA Compliance and Privacy Officer ensures that all investigations are completed as soon as possible; and no later than sixty **(60)** days after discovery of the suspected breach for Commissioners Court Departments unless circumstances absolutely do not permit this deadline to be met. The sixty **(60)** day timeline begins from the **earlier of the first day a suspected breach is discovered** or **the first day a workforce member would have been aware of the breach by exercising reasonable diligence**.

Documentation and Determination of Breaches

1. The Security Officer reports technical information and conclusions to the HIPAA Compliance and Privacy Officer as soon as enough technical information is available for the HIPAA Compliance and Privacy Officer to determine if a breach has actually occurred.

2. The Privacy Officer documents all facts collected in the investigation in an internal report. The Security Officer provides a signed attestation of technical information and conclusions to the HIPAA Compliance and Privacy Officer for inclusion in that report. Draft documents and findings are provided to Legal Counsel for review.

3. The HIPAA Compliance and Privacy Officer reviews relevant information and, in consultation with Legal Counsel, **as necessary**, determines whether-or-not a breach has occurred. A breach is presumed to have occurred in all cases where the risk of compromise to PHI is greater than low, as based on the following risk factors:
    a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification (e.g., social security numbers, financial data, clinical detail, diagnosis, treatment, medications).
    b) The unauthorized person who used the PHI or to whom the disclosure was made.
    c) Whether the PHI was actually acquired or viewed.
    d) The extent to which the risk to the PHI has been mitigated.

4. If the incident is determined to be a violation, **but not a breach**, the HIPAA Compliance and Privacy Officer will appropriately document the violation and recommend any Corrective/Disciplinary Actions to prevent similar occurrences in the future.

5. If the incident is determined to be a breach, the HIPAA Compliance and the Privacy Officer and the Security Officer follow procedures in the policy entitled Mitigation of Harm Resulting from Impermissible Use or Disclosure of PHI /PII. The HIPAA Compliance and Privacy Officer maintains a log of all breaches. The Log contains the following information with respect to each breach:
    a) A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of victims/records affected, if known.
    b) A description of the types of unsecured PHI that were involved in the breach (such as full name, social security number, date of birth, home address, account number, etc...).
    c) A description of the action taken in-regards-to notification of patients regarding the breach.
    d) Steps taken to mitigate the breach and prevent future occurrences.

6. The HIPAA Compliance and Privacy Officer informs all appropriate parties of his or her determination whether a breach has occurred or not. The HIPAA Compliance and Privacy Officer, in consultation with the Risk Manager, Legal counsel, Security Officer, and other appropriate parties, **as necessary**, will recommend Corrective/Disciplinary Actions to help prevent future recurrences.

7. The HIPAA Compliance and Privacy Officer reports any violations or breaches that involve business associates to the Purchasing Agent and to the Department.

Privacy Administration

Policy # 1.4

Mitigation of Harm Resulting from Impermissible Use or Disclosure of PHI

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To establish a process to appropriately mitigate any potential harm to individuals due to possible exposure and/or disclosure of PHI.

Policy: Travis County mitigates, **to the extent possible**, any harmful effects of a violation of these HIPAA Policies/PHI Regulations or the ITS Security Policies or State or Federal Laws concerning the unauthorized access, acquisition, use or disclosure of PHI by workforce members or business associates.

Process:

1. The policy entitled Reporting, Investigating, and Documenting Suspected PHI Breach outlines the policy and process for determining whether-or-not a breach of PHI has occurred.

2. If the HIPAA Compliance and Privacy Office has determined that a breach of PHI has occurred, the HIPAA Compliance and Privacy Officer, in consultation with Legal Counsel, evaluates whether any damage has occurred, the extent of any damage that has occurred, and what actions should be taken to mitigate any damage. This includes an evaluation of applicable State and Federal statutes and regulations. The recommendations related to the actions that should be taken to mitigate any damage will be based on at least the following factors:
    - knowledge of where the information has been disclosed; and
    - how the information might be used to cause harm to the patient or another individual; and
    - what steps can actually have a mitigating effect under the facts and circumstances of any specific situation

3. The HIPAA Compliance and Privacy Officer and/or the Security Officer will review policies applicable to the suspected breach and evaluate whether there are ways to improve policies where necessary.

4. The HIPAA Compliance and Privacy Officer reports to the County Executive, Department Head, Elected/Appointed Official or their designee responsible for programs in which a breach is reported, the nature and any consequences of actual breaches of PHI. The HIPAA Compliance and Privacy and/or Security Officer may recommend possible operational improvements to prevent recurrence of any breach. The HIPAA Compliance and Privacy Officer reports, **in aggregate**, small and low-risk breaches to the County Risk Manager on a periodic basis. The HIPAA Compliance and Privacy Officer reports breaches of over **500** records to the County Risk Manager.

5. The HIPAA Compliance and Privacy Officer uses their **professional judgement** to determine whether circumstances warrant informing the Commissioners Court, or the HIPAA Compliance and Privacy Officer's Court subcommittee of a breach or violation. The HIPAA Compliance and Privacy Officer always informs the Court of suspected breaches involving more than **500** records. To inform the Court, the HIPAA Compliance and Privacy Officer issues a memo with information pertaining to the breach or violation and any actions the Officer believes are necessary to mitigate the breach. The Court may direct that certain action be taken to mitigate the risk.

6. If any circumstance prevents the Commissioners Court from taking action before the end of the time in which the County must provide individuals with notice, or if an immediate action is required to mitigate risk, the County Executive to whom the HIPAA Compliance and Privacy Officer reports has the authority to act on behalf of the County to mitigate risks associated with the breach.

The HIPAA Compliance and Privacy Officer and/or the Security Officer review policies applicable to the suspected breach and evaluate whether there are ways to improve policies.

Privacy Administration

Policy # 1.5

Breach Notification

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To provide a process for ensuring timely and appropriate notice to individuals whose PHI has been compromised by a breach.

Policy: Travis County notifies individuals whose unsecured PHI has been compromised by an impermissible access, use, or disclosure, and will notify the media, law enforcement, the state attorney general, and the United States Department of Health and Human Services, **as appropriate**, in accordance with HIPAA, Federal and State law standards. **All notices are to be written in plain language**.

Process:

1. The HIPAA Compliance and Privacy Officer and the County Executive or Department Head responsible for the Covered Component in which a breach has occurred will determine the verbiage to be included in the notice. The verbiage must be comprehensible to the Individual whose PHI was breached.

2. The HIPAA Compliance and Privacy Officer and the County Executive or Department Head decide the most appropriate person to sign the notice.

3. The HIPAA Compliance and Privacy Officer sends notification to the individual(s) whose PHI has been breached as soon as sufficient investigative information has been obtained to allow the HIPAA Compliance and Privacy Officer to comply with the requirements of 45 C.F.R. § 164.404, entitled "***Notification to Individuals***." In accordance with the Texas Medical Privacy Records Act, the HIPAA Compliance and Privacy Officer endeavors to send notice "**as soon as possible**" and "**without unreasonable delay**," but in no event later than sixty ***(60) days*** after the discovery of the breach.

4. The HIPAA Compliance and Privacy Officer reports the breach to the Secretary of the U.S. Department of Health and Human Services in the manner and time period described by the below sections labeled, **Notification Requirements for a breach of PHI for less than 500 individuals** OR **Notification Requirements for a breach of PHI for more than 500 individuals.** 45 CFR §§ 164.400-414.

Notification Requirements for a breach of PHI for less than 500 individuals:

1. The HIPAA Compliance and Privacy Officer submits the breach log, described in the Reporting & Investigating Breach Policy, to the Secretary of the U.S. Department of Health and Human Services within **sixty (60)** days after the end of each calendar year. The submission shall include all breaches discovered during the preceding calendar year.

Notification Requirements for a breach of the records of more than 500 individuals:

1. The HIPAA Compliance and Privacy Officer notifies the U.S. Department of Health and Human Services at the same time notice is made to affected individuals, and in no event later than **sixty (60)** days from the discovery of the breach, unless a law enforcement official requests a delay

2. The HIPAA Compliance and Privacy Officer notifies prominent media outlets that serve the geographic area of the State in which the affected individuals reside without unreasonable delay. Before making such notification, the HIPAA Compliance and Privacy Officer and Legal Counsel work with the County Executive or Department Head responsible for the Covered Component in which the breach occurred on the contents of, and method for notifying the media. All three parties collectively determine the geographic areas appropriate for media notification as well as the appropriate media outlets for notification.

Notification to Individuals:

1. The HIPAA Compliance and Privacy Officer develops a notification, **written in plain language**, that contains elements required by 45 C.F.R. § 164.404, to the extent they are possible to include. The notification is developed in consultation with the Covered Component and legal counsel, **as necessary**.

2. Urgent notice is provided to Individuals when the circumstances surrounding the breach indicate that the PHI may be misused. The HIPAA Compliance and Privacy Officer, in conjunction with the appropriate department parties **as necessary**, ensures that the notice is always provided in writing and will also provide notice by phone, or other means, as appropriate.

3. The HIPAA Compliance and Privacy Officer sends written notification by first-class mail to the Individual at the Individual's last known address. If First-Class mail is returned and/or the Individual has previously agreed to receive electronic notice (ePHI), and that agreement is still in place, then the HIPAA Compliance and Privacy Officer may send notice by electronic mail. For breaches that involve the PHI of deceased persons, the HIPAA Compliance and Privacy Officer sends written notification to the decedents' next of kin or personal representative. If insufficient or out of date contact information exists for a decedent's next of kin or personal representative, then substitute notice is not provided.

4. The HIPAA Compliance and Privacy Officer provides substitute notice when Covered Components have insufficient or out of date contact information. The form of substitute notice must be determined to be a reasonable method to reach the Individual. Notice is provided according to the following:

i. **Fewer than 10 Individuals**: substitute notice is provided by an alternate form of written notice, telephone, or some other method reasonably designed to reach the Individual.

ii. **Greater than 10 Individuals**: substitute notice is posted on the Travis County website and the Covered Component's home page for ninety **(90)** days or is provided as a conspicuous notice in major print or broadcast media serving geographic areas where the affected Individuals likely reside. Additionally, the County will include a toll-free phone number that is active for at least ninety **(90)** days so that an Individual may inquire as to whether-or-not their PHI was included in the breach.

Privacy Administration

Policy #1.6

Education and Training

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Policy: Workforce members who have access to PHI are trained on the requirements of HIPAA, State medical privacy laws, and Travis County Security Policies and these Privacy Policies in accordance with State and Federal laws. The HIPAA Compliance and Privacy Officer is responsible for developing, administering, and documenting training for Privacy Policies and the Security Officer is responsible for developing, administering, and documenting Security Policy training.

Purpose: To provide a method to appropriately train workforce members so that they may best safeguard PHI.

Process:

Training upon Initial Employment and Change in Employment Duties

1. Supervisors in Covered Components report new workforce members and workforce members who have either transferred departments or who have recently gained access to PHI due to a change in job responsibilities, to the HIPAA Compliance and Privacy Office as soon as possible.

2. HIPAA Compliance and Privacy Officer administers training to workforce members within thirty **(*30*) *days*** after their initial employment. Workforce members complete all assigned HIPAA required training components within thirty **(*30*) *days*** after receiving access to HIPAA training materials.

- Supervisors ensure that workforce members complete required training within the specified time frame.
- To facilitate this responsibility, Supervisors can view the status of his or her workforce members' training within Manager Self Service in SAP.

3. HIPAA Compliance and Privacy Officer runs reports and tracks compliance with training utilizing SAP. The HIPAA Compliance and Privacy Office keeps records of a workforce member's successful completion of Privacy training within SAP, or through other means as necessary.

Refresher Training and Training Following a Substantial Policy Revision

1. Workforce members receive mandatory annual HIPAA training. Refresher training is also assigned on a more frequent basis, if such training is deemed necessary by a County Executive or Department Head responsible for the covered component, or by the HIPAA Compliance and Privacy Officer.

2. HIPAA refresher training is conducted when a substantial policy revision takes place. When training is provided for these purposes, it must be completed within the timeframe set forth by HIPAA Compliance and Privacy Officer.

Failure to Meet Training Deadlines

1. The HIPAA Compliance and Privacy Officer consults with supervisors of workforce members who have failed to complete training on a timely basis.

2. Supervisors' direct workforce members to complete the training within **7** days unless there is an extenuating circumstance.

3. The HIPAA Compliance and Privacy Officer brings continued non-compliance of workforce members to the attention of workforce member's Department head, or the Department Head's Designated Governance Committee member, **as appropriate**.

4. The HIPAA Compliance and Privacy Officer continues to elevate issues of non-compliance up the workforce member's chain of command until the workforce member completes the required training. If training compliance is not achieved through this method, HIPAA Compliance and Privacy Officer assesses the risk of non-compliance and, **in consultation with the Security Officer**, ***may restrict*** the workforce member's access to electronic forms of PHI (ePHI) that reside on the Travis County network. County Executives or Department Heads will be notified of a pending termination of access before such action is taken.

5. The HIPAA Compliance and Privacy Officer consults with the Governance Board members or Elected or Appointed Officials **as appropriate** to discuss non-compliance and the potential termination of access to PHI.

Privacy Administration

Policy # 1.7

Corrective/Disciplinary Actions

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Policy: Travis County will appropriately discipline employees and workforce members in a manner appropriate for any violation of these Policies. Corrective/Disciplinary Action may include counseling, re-training, verbal or written warnings, reassignment to a job that does not have access to PHI, suspension of access to PHI, suspension of employment, and immediate termination of employment. These will be implemented in compliance with the policies appropriate for the involved department or office. Workforce members who knowingly and willfully violate State or Federal law for improper use or disclosure of a patient's information may be subject to criminal investigation and prosecution or civil monetary penalties. **Corrective/Disciplinary Action also applies to workforce members who fail to complete training**.

Purpose: To ensure that appropriate Corrective/Disciplinary Action is applied to workforce members who do not comply with the Policies for safeguarding PHI.

Process:

Commissioners Court Departments

1. Travis County, through its HIPAA Compliance and Privacy Officer or Human Resources Management Division (HRMD) fully investigates the circumstances around an alleged privacy or security violations after making a notification to the attention of the workforce member's Department head.

2. The HIPAA Compliance and Privacy Officer will review applicable policies and determine if Human Resources Management Department (HRMD) is the appropriate body to handle an alleged Policy Violation. If the Human Resources Management Department (HRMD) is found to be the more appropriate body to handle an **alleged policy violation**, then the HIPAA Compliance and Privacy Officer will provide assistance.

3. If it is determined by investigating parties, in consultation with the HIPAA Compliance and Privacy Officer, Security Officer, or Legal Counsel, that a violation or breach has occurred, the HIPAA Compliance and Privacy Officer and HR Employee Relations evaluate the investigative information to determine severity of the violation and to recommend the appropriate Corrective/Disciplinary Actions.

- The potential impact to Travis County of any violation or breach is considered in determining appropriate Corrective/Disciplinary Action against workforce members. Other factors considered are the Violation Type and The Cause or Motivation that caused the violation, as seen below:

****Anything reported is considered an INCIDENT until fully investigated by CAP to be otherwise:**

TYPE OF INCIDENT	ROOT CAUSE	POSSIBLE LEVEL OF IMPACT
COMMON ERRORS: (Errors in handling restricted or sensitive information or in maintaining security measure)	• Unintentional • Lack of Training • Inexperience • Poor Judgement (1ST Violation) • Poor Process (1ST Violation) • Human Error	***LOW:*** • # OF RECORDS: ➢ Between 1-50
POLICY VIOLATION	• Poor Judgement (2nd Violation) • Poor Process (2nd Violation) • Failure to Complete Training • Intentional, but not Malicious • Concern for Individual *****2nd Violation: Same employee performs the same error more than once after being addressed originally*****	***LOW:*** • # OF RECORDS: ➢ Between 1-50 ***MEDIUM:*** • # OF RECORDS: ➢ Between 51-200
POSSIBLE BREACH	• Malicious Intent • Curiosity (Snooping) • Financial Gain • Revenge • Protest • Gross Negligence • Human Error • Weak/Stolen Credentials • Application/OS Vulnerabilities • Social Engineering • Hacking • Insider Threats • 3rd Party Attacks • Data Disclosure • Physical Theft/Loss of Device • Vendor/Business Associate Compromises	***LOW:*** • # OF RECORDS ➢ Between 1-50 ***MEDIUM:*** • # OF RECORDS ➢ Between 51-200 ***HIGH:*** • # OF RECORDS: ➢ Between 201-500 ***EXTREME:*** • # OF RECORDS: ➢ 501+

4. An **intentional** violation of these privacy policies must be established by clear evidence (i.e., evidence that the disclosure was intentional and deliberate and that such workforce member knew that the action violated HIPAA, or the policies and procedures as set forth in this manual).

5. The Corrective/Disciplinary Actions for an **unintentional** failure to comply with these policies or procedures varies, **depending on the relevant facts and circumstances**. At a ***minimum***, the workforce member is **required** to meet with the HIPAA Compliance and Privacy Officer to review the violation and demonstrate, to the satisfaction of the HIPAA Compliance and Privacy Officer, that he or she understands the relevant policies and procedures.

6. All workforce members Corrective/Disciplinary Actions will be documented and retained for a period of at least **6** years from the date of its creation or the date when it was last in effect, **whichever is later**. An unproven or unsubstantiated allegation of a violation does not require documentation unless it is pursuant to another requirement under these policies such as a complaint.

Non-Commissioners Court Departments/Offices:

1. Travis County Covered Components appropriately and consistently discipline workforce members who are found to violate these HIPAA and/or PHI Policies or the Security Policies in accordance with this Corrective/Disciplinary Action policy.

2. Covered Components investigate the circumstances of the policy violation and determine whether-or-not improper uses or disclosures requiring further mitigation of harm have occurred (see the policy entitled, Mitigation from Harm Resulting from PHI Breaches). The HIPAA Compliance and Privacy Officer is available to assist, **as requested**.

3. Departments/Offices record all Corrective/Disciplinary Actions taken in the workforce member's employment records. The HIPAA Compliance and Privacy Officer is made aware of the Corrective/Disciplinary Action in general terms for purposes of documenting corrective action.

Corrective/Disciplinary Action against Workforce Members not directly employed by Travis County:

1. Commissioners Court Departments:

If a workforce member who is not directly employed by Travis County violates the County's HIPAA or Security policies and procedures, then the HIPAA Compliance and Privacy Officer, **in consultation with appropriate parties** such as the Purchasing Agent and/or County Attorney, considers the impact to the organization as well as the causes and motivations related to the violations. The HIPAA Compliance and Privacy Officer, **after consultation**, will then ***recommend*** to Department Heads over Covered Components appropriate Corrective/Disciplinary Actions which may include retraining, modification and/or termination of contracts or modification and/or termination of volunteer agreements. Covered Components inform the HIPAA Compliance and Privacy Officer of Corrective/Disciplinary Actions taken against workforce members not directly employed by Travis County. The HIPAA Compliance and Privacy Officer documents these actions.

2. Non-Commissioners Court Departments:

If a workforce member not directly employed by Travis County violates the County's HIPAA, PHI or Security policies and procedures, then the Elected or Appointed Official or their designee, in consultation with appropriate parties such as the Purchasing Agent or County Attorney, considers the impact to the organization, causes and motivations related to the violations. The HIPAA Compliance and Privacy Officer, **after consultation**, will then ***recommend*** Corrective/Disciplinary Actions which may include retraining, modification and/or termination of contracts, or modification and/or termination of volunteer agreements. The HIPAA Compliance and Privacy Officer is available for technical assistance. Covered Components inform the HIPAA Compliance and Privacy Officer of Corrective/Disciplinary Actions taken against workforce members not directly employed by Travis County. The HIPAA Compliance and Privacy Officer documents these actions.

Uses and Disclosures of Protected Health Information (PHI)

Policy # 2.1

Minimum Necessary Standard

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To develop procedures to limit the PHI requested, used, or disclosed to the amount reasonably necessary to achieve the purpose of the request, use or disclosure.

Policy: Workforce members are granted access to the minimum amount of PHI necessary to perform their job functions. When requesting, using, or disclosing PHI, as allowed under these HIPAA Policies, workforce members use or disclose only the minimum PHI necessary to accomplish the purpose of the use, request, or disclosure. A workforce member does not use, disclose, or request an entire medical record unless the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.

This policy **does not apply** to the following uses or disclosures:

- **disclosures to or requests by a provider for treatment;**
- **uses or disclosures made to the Individual who is the subject of the information;**
- **uses or disclosures pursuant to an authorization;**
- **disclosures made to the United States Department of Health and Human Services;**
- **uses or disclosures required by law; and**
- **uses or disclosures required for compliance with applicable requirements of the HIPAA Privacy Rules.**

Process:

<u>Responding to requests for PHI</u>

1. When responding to a request for PHI, Travis County workforce members discuss with the requestor, or obtain written descriptions from the requestor that explain, the purpose of the request and the type of PHI needed. This procedure applies to ***<u>every</u>*** request, including requests that originate in departments that have been designated a Travis County ***"Business Associate"*** under the County's Hybrid Designation.
    - Travis County *Business Associate* Components (Departments) are:
        - **County Attorney**
        - **County Auditor**
        - **Records Management & Communication Resources**
        - **Information Technology Services**

Using and Disclosing PHI

1. For any use or disclosure of PHI made on a routine and recurring basis, workforce members can rely on established and appropriately reviewed practices in determining the amount of information needed to perform the particular function and do not need to engage in a case-by-case review of whether the information used or disclosed conforms to the minimum necessary standard. Routine and recurring uses and disclosures shall include, **but are not limited to**, the following:
    - uses or disclosures of PHI for the purposes of conducting treatment, payment or health care operation functions or activities in relation to the Covered Component,
    - activities involving the coordination of benefits,
    - disclosure of enrollment/disenrollment status of an Individual under a Group Health Plan,
    - disclosures to an Individual or an Individual's family member or other person closely involved in the Individual's care.

    Workforce members may also rely on an internal department memo that establishes the minimum amount of PHI necessary to disclose to *Business Associate* departments. A copy of internal department memos is provided to the HIPAA Compliance and Privacy Officer.

2. For any use or disclosure of PHI that is not made on a routine and recurring basis, workforce members review the request, and determine the minimum PHI necessary to accomplish its purpose.

3. When Federal or State law requires a disclosure of PHI, the minimum necessary information considered to be what is required to comply with the law.

Minimum Necessary Access

1. The HIPAA Compliance and Privacy Officer will assess whether various classifications of personnel have appropriate access to PHI, and will recommend access restrictions, **where appropriate**.

2. The HIPAA Compliance and Privacy Officer works with covered components, including Privacy Liaisons, program managers and others, to identify workforce members that may access PHI by position, job class, or any other mechanism most appropriate to the covered components.

3. Appropriate workforce members provide job functions, and level of access requirements to the HIPAA Compliance and Privacy Officer. The HIPAA Compliance and Privacy Officer reviews, and communicates concerns related to levels of access back to the covered component. Access is re-reviewed and justified, modified, or terminated by the covered component, in consultation with the HIPAA Compliance and Privacy Officer.

4. The HIPAA Compliance and Privacy Officer provides HIPAA Training List, by position number, to the Security Officer to facilitate implementation of TC-ITS- 102, entitled, "Access Control Policy."

5. Covered Components inform the HIPAA Compliance and Privacy Officer of new positions or reorganized positions or job functions that require access to PHI prior to allowing such access. The HIPAA Compliance and Privacy Officer and covered components review the justification for PHI access in accordance with these procedures. Anyone having access to PHI must have completed the mandatory HIPAA Training before being granted access.

Uses and Disclosures of PHI
Policy # 2.2

Disclosure to Persons Involved in Individual's Care

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To provide a policy for circumstances under which a disclosure may be made to a person involved in an individual's care.

Policy: Travis County Covered Components disclose PHI to an Individual's family member, or a person involved in the Individual's care or payment related to the Individual's care when:

- the Individual has an opportunity to authorize, agree or object to the disclosure of such information; or
- the Individual is incapacitated or is otherwise unable to authorize, agree or object and the Covered Component believes that disclosure is in the best interest of the Individual.

Covered Components follow all applicable laws, regulations, and these Policies in making such disclosures.

Process:

1. **Before disclosing PHI**
   Workforce members will comply with the policy entitled Minimum Necessary Standard. Any disclosure will be **limited** to that information which is directly relevant to the recipient's involvement with the Individual's health care or payment related to the Individual's health care.

2. **Requesting Authorizations**

   - Covered Components may seek an Individual's authorization to disclose his or her PHI to authorized or identified family members, friends, or any other person specified by the Individual upon enrollment in a County program. See the policy entitled Authorization for Release of PHI.

   - A family member includes a dependent and any other person who is at least a fourth degree relative of the Individual. By example: Fourth-degree relatives include an individual's **great-great-grandparents, great-great-grandchildren, and first cousins once-removed** (i.e., the children of the individual's first cousins). (b) Family medical history. Family medical history means information about the manifestation of disease or disorder in family members of the individual.

3. **Disclosures when no Authorization is provided**

- If the Individual is **present and capacitated** at the time of the proposed disclosure to the Individual's family member(s) or others involved in the Individual's care or payment for care, workforce members either:
    - obtain the Individual's oral or written agreement to the disclosure; or
    - provide the Individual with the opportunity to object to the disclosure. Workforce members may use **professional judgement** to make a reasonable inference, **from the circumstances**, that the Individual does not object to the disclosure.

- If the Individual is **incapacitated or otherwise unable to agree or object** to the proposed disclosure, workforce members exercise their **professional judgment** in deciding whether to disclose the Individual's PHI. The PHI disclosed is limited to the person's involvement in the Individual's care. In making this decision, workforce members consider:
    - whether disclosure would be in the best interests of the Individual, and
    - whether the Individual has previously expressed a preference on the subject.

4. **Disclosures to Personal Representatives**

Questions about disclosures to persons involved in an individual's care are directed to the HIPAA Compliance and Privacy Officer. Workforce members may also disclose PHI to a **personal representative** given the following:

- the workforce member obtains documentation that designates the person as a personal representative and,
- PHI is disclosed only to the extent allowed in the document designating the person as a personal representative of the Individual and,
- the disclosure **is limited** to information directly relevant to the health care provided to the Individual by the person to whom PHI is disclosed, or payment for health care for the Individual by the person to whom PHI is disclosed, or the information necessary to achieve the allowable purpose.

Note: A workforce member may **decline** to disclose PHI to a personal representative if:

- the workforce member believes that the Individual has been or may be subject to domestic violence, abuse, or neglect by such person; or treating such person as the personal representative could endanger the individual; and
- the workforce member, in the exercise of his or her professional judgment, decides that it is not in the best interest of the Individual to treat the person as the Individual's personal representative.
- You can find the list of acceptable Personal Representatives ***here.***

5. **Deceased Individuals**

- Workforce members may disclose PHI related to deceased Individuals to family members (upon verifying proof of relationship) and others who were involved in the care or payment for care (upon verification) of the Individual prior to death, unless it is inconsistent with any prior expressed preference of the Individual that is known to the Covered Component.

- Workforce members disclose PHI to a personal representative when the workforce member obtains documentation that shows the person has been designated as the Individual's personal representative. Workforce members may decline to disclose PHI to a personal representative for the reasons listed in **#3 above in this section.**

- You can find the list of acceptable Personal Representatives ***here***

6. **Disaster Relief Purposes**

- Workforce members disclose PHI to a public or private entity, authorized by law or by its charter to assist in disaster relief efforts, for the purpose of assisting in the notification of an Individual's family member, personal representative, or person responsible for the Individual's care of the Individual's location, general condition, or death.

Uses and Disclosures of PHI

Policy # 2.3

Verifying the Identity and Authority of a Person Requesting PHI

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To ensure that PHI is disclosed only to people authorized to receive PHI under HIPAA rules and Federal and State medical privacy records laws.

Policy: Travis County Covered Components verify the identity and authority of the person requesting the PHI if they are not already known to the Covered Component **prior to** using or disclosing PHI as allowable by HIPAA rules and Federal and State laws.

Process:

1. When a request for PHI is made, workforce members may demand any reasonable form of identification to verify the identity of a requestor it does not already know. Acceptable forms of identification will vary, depending upon how the request is made (i.e., in person or by phone), but may include such forms and methods as are included in the chart below.

Table 1: Verification Requirements

Person requesting PHI and manner of request:	**Requirements for verification:**
Request made in person	• A government-issued picture identification, such as a driver's license, passport, Travis County ID, or other government issued ID with a picture. • If the requestor is a public official or is authorized by law to request PHI, workforce members can also rely on: 1. an agency badge, with picture; or 2. a written statement of the legal authority under which the PHI is requested
Request made over the email	•The requestor must verify the following information about the Individual whose PHI is to be disclosed: 1. Name 2. Address 3. Phone Number 4. Birthdate 5. Another unique identifier, such as the last four digits of the Individual's social security number • The requestor must also give his or her name, address, and telephone number. • If the requestor is a provider, the provider should further provide the Covered Component with a copy of any authorizations or releases signed by the Individual with respect to the PHI requested. Where no release is necessary, workforce members should follow the requirements applicable to requests made in writing
Request made in person by a Personal Representative	• **The requestor must have and present:** 1. Knowledge of the Individual's o Address o Phone Number o Birthdate o Another unique identifier (last 4 of SSN; email address etc...) 2. a written Power of Attorney; **or** 3. a signed Authorization by the individual. •The Personal Representative must also present a government-issued picture identification.

Request made in person by a Parent of a minor.	• If the minor is accompanied by the parent, and the minor acknowledges that the adult is his or her parent, no further information is needed. • Otherwise, the parent must follow the requirements as described in requests made in person by a personal representative.
Request made in writing	• Workforce members will make reasonable efforts to verify that the requestor is who he or she claims to be. This may include contacting the requestor's employer or the Individual whose PHI is to be disclosed to discuss the request. • If the requestor is a public official, workforce members can rely on requests written on official government letterhead stationery.
Requests on behalf of a Public Official	• Workforce members may rely on a written statement evidencing that the person is acting on behalf of the public official

2. Workforce members examine and copy each of the documents provided and store them with the Individual's medical records. If any questions arise about the validity of a requestor's identity or authority, the HIPAA Compliance and Privacy Officer is consulted.

3. Once the requestor's identity and authority are verified, workforce members determine the amount of PHI necessary to fulfill the request for disclosure. Workforce members will comply with the policy entitled Minimum Necessary Standard.

4. The requested PHI is **delivered to the requesting party in a secure and confidential manner**, such that the information cannot be accessed by employees or other persons not authorized to access the PHI. If sending PHI via email, the email **must be encrypted**. You can find encrypting email instructions here. To delay sending an email by putting a time and date when you would like the email sent out, you can find that here.

The HIPAA Compliance and Privacy Officer or Privacy Liaison appropriately tracks the disclosure (when required; see the policy entitled Accounting of Disclosures) and delivery of the PHI.

Uses and Disclosures of PHI

Policy # 2.4

Permitted Uses and Disclosures of PHI

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To define the purposes for which PHI may be accessed, used, or disclosed**.**

Policy: Workforce members access, use and disclosure of PHI are only allowable by HIPAA, State laws, and these Policies. Workforce members obtain an Individual's Authorization before accessing, using, or disclosing PHI for any purpose other than those purposes specifically exempt from such requirement by HIPAA, Federal or State law.

Process:

1. Workforce members ascertain the purpose of the access, use, or disclosure.
    - **Important:** This procedure is **critical** to complying with HIPAA because there are different procedures and legal requirements for different purposes.
    - Consult with the HIPAA Compliance and Privacy Officer when in doubt about whether-or-not you may acquire, access, use, or disclose PHI in a certain way.

2. Workforce members consult the tables below and follow the policy applicable to the specific purpose for which the PHI will be acquired, accessed, used, or disclosed. Where a Covered Component has adopted supplemental policies to safeguard PHI, workforce members consult such policies too.

3. The PHI is disclosed in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information. Examples of this are Confirmation Faxes; Certified Mail Requiring a Signature; Encrypted Work Emails; Hard Drives; USBs; approved Travis County Equipment.

Table 1: Disclosures for Treatment, Payment, and Operations Purposes

Type of Use or Disclosure	Policy and Procedures
Treatment	**Policy:** Covered Components may not disclose PHI for treatment purposes without authorization from an Individual. Treatment is defined as the provision, coordination, or management of health care and related services by Covered Components or other healthcare providers, including consultation between Covered Components and other health care providers about a patient and referrals of patients. **Procedures:** 1. Disclosure is not subject to the "**Minimum Necessary Standard"** described in these policies. 2. Covered Components may use or disclose PHI to a business associate, if treatment falls within the scope of services that the business associate is to perform under the Business Associate Agreement it executed with the County. 3. Before disclosing the requested information to the health care provider, the Covered Component, through authorized workforce members, must verify the identity of the person making the request. See the Policy entitled "**Verifying the Identity and Authority of a Person Requesting PHI.**"
Payment	**Policy:** Covered Components may use or disclose PHI for payment purposes without authorization from an Individual. Payment activities include, but are not limited to: • obtaining premiums, • determining eligibility or coverage, • coordinating benefits, • adjudicating or subrogating health benefit claims, • risk adjusting amounts, • billing, • claims management, • collection activities, • obtaining payment under a contract for reinsurance, • related health care data processing, • medical necessity or coverage review, • utilization review—regardless of when it is performed, and • disclosure of certain information to consumer reporting agencies.

Type of Use or Disclosure	Policy and Procedures
Payment (cont...)	**Procedures:** 1. Any use of disclosure of PHI for payment activities is limited to that described in the Minimum Necessary Standard policy unless the information is required to be transmitted as an electronic transaction, pursuant to 45 CFR 1(60).102 and 45 CFR 164.502(b)(2)(vi). 2. Before disclosing the requested information to the health care provider, the Covered Component, through its authorized workforce members, must verify the identity of the person making the request. See the Policy entitled **"Verifying the Identity and Authority of a Person Requesting PHI."**
Health Care Operations: **(**SPECIAL NOTE)**	• "***Health care operations***" are 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. These activities, which are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501, include: o Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; o Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; o Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims; o Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; o Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and o Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale, or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. General Provisions at 45 CFR 164.506.

Policy: Covered Components may use and disclose PHI for health care operations without authorization from an Individual. Health care operation activities may include, **but are not limited to**:

- A hospital may use protected health information about an individual to provide health care to the individual and may consult with other health care providers about the individual's treatment.
- A health care provider may disclose protected health information about an individual as part of a claim for payment to a health plan.
- A health plan may use protected health information to provide customer service to its enrollees.

Procedures:

- Any use or disclosure of PHI for health care operation activities is limited to the Minimum Necessary Standard policy.
- Before disclosing the requested information to another covered entity, the Covered Component, through its authorized workforce members, must comply with the policy "Verifying the Identity and Authority of a Person Requesting PHI."
- Disclosures in Table 2 below require that the workforce member who discloses the PHI, appropriately documents the request and delivery of the PHI on the tracking log provided by the HIPAA Compliance and Privacy Officer OR in the software in which medical records are kept. Such tracking will be completed as described in the policy Accounting of Disclosures.
- The person who discloses the PHI, either an authorized workforce member or the HIPAA Compliance and Privacy Officer, appropriately documents the request and delivery of the PHI on the tracking log provided by the HIPAA Compliance and Privacy Officer. Such tracking log will be completed as described in the policy Accounting of Disclosures (called "Tracking" in this table).

*****SPECIAL NOTE:***

- **FOR PLANS:** If an individual had been enrolled in a health plan of Covered Entity A ad switches to a health plan provided by Covered Entity B, Covered Entity A can disclose PHI to Covered Entity B for Covered Entity B to coordinate the individual's care, without the individual's authorization...Although such disclosures are permitted, they are subject to the minimum necessary standard. 45 CFR 164.502(b). https://www.hhs.gov/hipaa/for-professionals/faq/3014/uses-and-disclosures-for-care-coordination-and-continuity-of-care/index.html

Table 2: Non-routine Permitted Disclosures

Type of Use or Disclosure	Policy and Procedures
Response to judicial and administrative requests, including subpoenas	**Policy**: Covered Components comply with all lawful and appropriate requests from regulatory and judicial authorities and may disclose PHI necessary to respond to: • a subpoena; • a discovery request or other lawful process that is not accompanied by an order of a court or administrative tribunal (subject to certain restrictions discussed below), or • a discovery request or other lawful process that is accompanied by or contained within an order of a court or administrative tribunal. • Any Legal Demands must be filled out entirely and signed by authorizing agent. An Individual's authorization is not required for such disclosures. **Procedures**: 1. All subpoenas issued by a court, grand jury, governmental or tribal inspector, or administrative body must be processed according to Covered Component protocol, HIPAA Compliance and Privacy Officer and Legal Counsel. 2. For discovery requests or other lawful processes, including investigative demands, that are **NOT** accompanied by a court order or an order of an administrative tribunal, the Covered Component alerts the HIPAA Compliance and HIPAA Compliance and Privacy Officer. 3. The HIPAA Compliance and Privacy Officer determines whether the disclosure is appropriate and should be made. Disclosure is only made if the HIPAA Compliance and Privacy Officer obtains evidence that provides satisfactory assurances that: • Reasonable efforts have been made to notify the Individual who is the subject of the request to allow for the Individual to object to the disclosure (the "**Notice Method**"), **OR** • Reasonable efforts have been made to obtain a "qualified protective order*" for the information (the "**QPO Method**"). **Notice Method** 1. The HIPAA Compliance and Privacy Officer must obtain a written Statement from the requestor that demonstrates that notice has been given (or a good faith effort to notify the Individual has been made) and that such notice contained enough detail about the litigation or proceeding for the Individual to be able to raise an objection to the disclosure.

Response to judicial and administrative requests, including subpoenas (cont...)	2. The HIPAA Compliance and Privacy Officer must also obtain a written Statement and documentation demonstrating that: • enough time was given to the Individual to object, and that this time has elapsed; • either no objections were filed, or any objections raised have been resolved by the entity deciding the case; and • the disclosures sought are consistent with the entity's resolution about any objections. **QPO Method** ****Qualified protective order (QPO) means a court order or order of an administrative tribunal or an agreement by the Individual and the requestor that prohibits them from using or disclosing the* **PHI** *for any purpose other than the purpose for which it was requested, and that requires the* **PHI** *to be returned or destroyed at the end of the proceeding.*** 1. The HIPAA Compliance and Privacy Officer must obtain a written Statement from the requestor that demonstrates that: • The parties to the judicial or administrative proceeding have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or • The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal. 2. The Covered Component may skip Procedure 3 if the Covered Component makes reasonable efforts to provide notice to the Individual sufficient to meet the requirements of Procedure 2(a) or 2(b).
Public health activities	**Policy**: Covered Components may disclose PHI to public health authorities, entities, and persons authorized by law to receive such information for public health activities. **Procedures**: 1. The Covered Component must verify the authority and identity of the person or entity seeking a disclosure per the appropriate policy for the purpose of: • preventing or controlling disease, injury, or disability; • conducting public health surveillance; • conducting public health investigations; • conducting public health interventions; • reporting child abuse or neglect, certain injuries, or birth or death; or • notifying a person exposed to a communicable disease or at risk of contracting or spreading them. 2. Once the identity and authority of the person requesting PHI is confirmed, the Covered Component alerts the HIPAA Compliance and Privacy Officer of the request.

Public health activities (cont...)	3. The HIPAA Compliance and Privacy Officer determines whether the disclosure is appropriate and should be made. The HIPAA Compliance and Privacy Officer may rely on the word of the public health authority to state what information is needed to carry out the lawful purpose and disclose that information.
Report abuse, neglect, or domestic violence	**Policy**: Covered Components may disclose PHI to a public health authority or other appropriate government authority authorized by law to receive reports of abuse, neglect, or domestic violence. An Individual's authorization is not required. **Procedures**: 1. If a workforce member reasonably believes that an Individual is the victim of abuse, neglect or domestic violence, the workforce member will tell a supervisor, or the Privacy Liaison or HIPAA Compliance and Privacy Officer about his or her suspicions. • "Abuse" means harm or threatened harm to an Individual's health, safety, or welfare. "Neglect" means a failure to provide (i) adequate food, clothing, shelter, medical care, and supervision; (ii) special care which is necessary because of the physical or mental condition of the child; or (iii) abandonment. 2. The workforce member authorized to make such report (based on department policy), a supervisor, the Privacy Liaison or the HIPAA Compliance and Privacy Officer reports the abuse, neglect or domestic violence to the public health authority or other appropriate government authority authorized by law to receive such reports, including a social service or protective service agency. The report may disclose PHI, but only: • To the extent that disclosure complies with and is limited to the relevant requirements of the law that requires reporting; • The Individual agrees to the disclosure; or • To the extent that the disclosure is expressly authorized by law and o Workforce members in the Covered Component believe disclosure is necessary to prevent serious harm to the Individual or others, or o The Individual cannot agree because of incapacity and a law enforcement or other public official authorized to receive the report represents that ▪ the PHI will **NOT** be used against the Individual ▪ an immediate enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the Individual is able to agree to disclosure.

Report abuse, neglect, or domestic violence (cont...)	3. The disclosure limitations set forth in Procedure 2 **do not apply** when the victim of the abuse or neglect is a child. Clinical notes, x-rays, photographs, and those portions of previous or current medical records relevant to the abuse or neglect may be disclosed without restriction to the public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect. 4. The Supervisor or HIPAA Compliance and Privacy Officer must promptly inform the Individual (or the Individual's personal representative if the Individual is incapacitated) of the disclosure, unless: • it is believed that informing the Individual would place the Individual at risk of serious harm. • it is reasonably believed that the personal representative to whom notification would be made is the person responsible for the domestic violence, abuse, or neglect.
Law Enforcement Purposes	**Policy:** Covered Components may disclose PHI to a **Law Enforcement Officer*** in certain circumstances, as set forth in the procedures below. * "***Law Enforcement Officer***" means an officer or employee of any agency or authority of the United States, State, Indian tribe, county, city, town or municipality, who is empowered by law to (i) investigate or conduct an official inquiry into a potential violation of law; or (ii) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. **Procedures:** 1. Covered Components, excluding Covered Components that operate correctional facilities, inform the HIPAA Compliance and Privacy Officer of oral or written requests from law enforcement officials. Correctional facilities process requests in accordance with processes described in Correctional Institutions and other law enforcement custodial situations. 2. The HIPAA Compliance and Privacy Officer determines whether the disclosure is appropriate and should be made. Disclosure is appropriate: • to assist the official in the identification or location of a suspect, fugitive, material witness, or missing person (Class I); • when the PHI concerns a patient who is or is suspected to be a victim of a crime (Class II); • if the workforce member believes the PHI requested constitutes evidence of criminal conduct that occurred on the premises of the Covered Component (Class III); and • to alert law enforcement of the death of the Individual (Class IV);

Law Enforcement Purposes (cont...)

- in emergency situations, to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime (Class V).

<u>Class I</u> - To assist the official in the identification or location of a suspect, fugitive, material witness, or missing person.

Authorized workforce members may disclose limited PHI in response to a law enforcement official's request for Class I information. The information to be disclosed include the Individual's:

- 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
- Description of distinguishing characteristics (such as height, weight, race, hair and eye color, scars, tattoos)

Authorized workforce members **do not** disclose any PHI related to DNA or DNA analysis, dental records or typing, samples or analysis of body fluids or tissue.

<u>Class II -</u> When the PHI concerns a patient who is or is suspected to be a victim of a crime.

Authorized workforce members disclose PHI about a suspected victim of a crime only when:

- The Individual agrees to the disclosure, or
- The Individual cannot agree because of incapacity and a law enforcement official represents that
  - the information will be used to establish whether a crime has been committed,
  - the information will not be used against the Individual.
  - immediate law enforcement activity depends on the disclosure and would be materially and negatively impacted by waiting until the Individual is able to agree to disclosure, and
  - the workforce members, in the exercise of their **professional judgement**, determine the disclosure is in the best interest of the Individual.

<u>Class III</u>- If the workforce member believes the PHI requested constitutes evidence of criminal conduct that occurred on the premises of the Covered Component.
Authorized workforce members disclose PHI to a law enforcement official if the workforce member believes, in good faith, that the PHI constitutes evidence of criminal conduct that occurred on the Covered Component's property.

<u>Class IV -</u> To alert law enforcement of the death of the Individual.

Authorized workforce members disclose PHI about an Individual who has died if they have a suspicion that the Individual's death may have resulted from criminal conduct.

Law Enforcement Purposes (cont...)	**Class V** - In emergency situations, to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime. 1. Authorized workforce members providing emergency health care in response to a medical emergency, other than an emergency predicated by suspected abuse or domestic violence, may disclose PHI to a law enforcement official if the disclosure appears necessary to alert law enforcement to: • The commission and nature of the crime. • The location of this crime or the victims of the crime. • The identity, description, and location of the person responsible for the crime **2.** PHI is also disclosed on the Covered Component's own initiative to: • Report certain types of wounds or other physical injuries not associated with abuse, neglect, or domestic violence, or ○ Court orders and court-ordered warrants; ○ Summons issued **court **grand jury **governmental or tribal inspector**; or • Administrative request, including an administrative subpoena or summons a civil or authorized investigative demand, or similar process authorized under the law, provided that: ○ The PHI sought is relevant and material to a legitimate law enforcement inquiry; ○ The request is specific and limited is scope; and ○ De-identified information could not reasonably be used
Correctional Institutions and other law enforcement custodial situations ***(**Special Note)***	**Policy:** Covered Components may disclose PHI to a correctional institution or a law enforcement official that has lawful custody of a person provided tha 1. the individual is currently in custody and is not on parole, probation, or supervised release, or otherwise not in lawful custody; and 2. the institution or law enforcement official represents to the Covered Component that the requested PHI is necessary for any of the following: • Providing health care to the individual • The health and safety of the individual or other inmates • The health and safety of the officers or employees or of others at the correctional institution • The health and safety of such individuals or other persons responsible for transporting or transferring inmates • Law enforcement on the premises of the correctional institution The administration and maintenance of the safety, security, and good order of the correctional institution

Correctional Institutions and other law enforcement custodial situations (cont...)

Procedures:

Covered Components that are correctional institutions

1. Workforce members make disclosures based on department policy and/or operating procedures. Questions regarding the appropriateness of particular disclosures may be directed to supervisors or the HIPAA Compliance and Privacy Officer.

Covered Components that are not correctional institutions

Requests of an urgent nature. An urgent request is a request that requires immediate processing. When an urgent request is made, Covered Components may disclose PHI without the Privacy Liaison or HIPAA Compliance and Privacy Officer's involvement, provided that the Covered Component:

1. Documents the law enforcement official's representation that disclosure of PHI is necessary for any of the purposes described in the policy Statement set forth above and must be made immediately.

2. Verifies the identity and authority of the officer in accordance with the policy "Verifying the Identity and Authority of a Person Requesting PHI."

3. Determines disclosure is appropriate under the circumstances. Disclosure is not appropriate if workforce members are:
   - Unable to verify the identity or authority of the requestor
   - Uncertain about the Individual's lawful custody status
   - Concerned that the scope of the information requested is overly broad or subject to stricter privacy regulations. In this instance, workforce members may choose to limit the amount of information disclosed.

4. Gives the requesting law enforcement official's contact information to the HIPAA Compliance and Privacy Officer.

Requests that are not of an urgent nature. Workforce members direct requests of a non-urgent nature to the Covered Component's HIPAA Compliance and Privacy Officer.

1. The HIPAA Compliance and Privacy Officer verifies the identity and authority of the law enforcement official in accordance with policy "Verifying the Identity and Authority of a Person Requesting PHI."

2. He or she then determines what PHI is appropriate to release pursuant to the request.

3. He or she then informs the workforce member of the decision and authorizes the release of the information or releases it directly to the law enforcement official or correctional institution.

*****SPECIAL NOTE:***

- **RULE DIFFERENCE FOR CORRECTIONS:** Correctional institutions and other law enforcement custodial situations -

(i) Permitted disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; or

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) Permitted uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed. 45 CFR § 164.512 (k)(5).

Federal Officials for National Security and Intelligence Purposes	**Policy:** Covered Components may disclose PHI to Federal Officials for the conduct of certain national security and intelligence activities, for the conduct of protective services by Federal officials to the president and persons as authorized by Federal law. Requests of this nature are prioritized by Covered Components and the HIPAA Compliance and Privacy Officer. **Procedures:** 1. The Covered Component follows appropriate policies and procedures for verifying the identity and authority of individuals requesting PHI. 2. Covered Components collect detailed information relating to the request, then forwards the request to the HIPAA Compliance and Privacy Officer for review. 3. The HIPAA Compliance and Privacy Officer ensures that the statutory authority for the request is provided, and, in consultation with legal counsel **as necessary**, approves the request for PHI. 4. Covered Components provide the requested PHI in the format requested by the Federal official.
Coroners or Medical Examiners, and Funeral Directors	**Policy:** Covered Components are permitted to disclose PHI to coroners, medical examiners, and funeral directors without an Individual's authorization. **Procedures:** 1. Authorized workforce members may disclose PHI to coroners, and medical examiners for purpose of • identifying a deceased person, • determining the cause of death and, • to carry out their other lawful duties. 2. Workforce members may disclose PHI to funeral directors to carry out their lawful duties, and, where necessary, may disclose PHI prior to, and in reasonable anticipation of, the Individual's death.
Employer Compliance with OSHA or Workers' Compensation requirements	**Policy**: Covered Components may disclose PHI as authorized by and to comply with laws relating to workers' compensation, occupational safety, or other similar programs that provide benefits for work-related injuries or illness without regard to fault.

Employer Compliance with OSHA or Workers' Compensation requirements (cont...)	**Procedures**: 1. The Covered Component follows appropriate policies and procedures for verifying the identity and authority of individuals requesting PHI requesting PHI, for health oversight activities. 2. Once the identity and authority of the Individual requesting PHI is confirmed, the Covered Component alerts the HIPAA Compliance and Privacy Officer. 3. The HIPAA Compliance and Privacy Officer determines whether the disclosure is appropriate and should be made. Disclosure is appropriate to workers' compensation insurers, State administrators, employers, and other persons or entities involved in workers' compensation systems, without the individual's authorization if: • Health care is being provided to an Individual at the request of the employer to evaluate: ○ workplace medical surveillance for compliance with occupational health and safety laws (OSHA requirements) or ○ whether the Individual has a work-related illness or injury • the PHI to be disclosed relates to findings about workplace-related medical surveillance or a work-related illness or injury; or • the requestor is an employer who needs PHI to comply with worker's compensation laws, or occupational health and safety laws. 4. When a disclosure is made, the Covered Component must provide the Individual whose PHI was disclosed with written notice of the disclosure. Notice must be given either: • at the time the PHI is disclosed to the employer OR • by posting a notice in a prominent place where the health care is provided.
Compliance with the Texas Public Information Act	**Policy:** Covered Components may disclose PHI to the Travis County Attorney's Office or departmental staff assigned to handle Public Information Act requests without Individual authorization to comply with the Texas Public Information Act. **Procedures:** 1. The Covered Component provides documents responsive to the Public Information Act request to the County Attorney or authorized department staff, such as in-house legal counsel or paralegals. Covered Components will not redact PHI from these documents unless directed to do so by the County Attorney or department counsel. 2. The County Attorney or authorized department staff processes the PHI. If the release of any PHI is compelled by the law, the County Attorney or department staff notifies the Covered Component. The Covered Component then logs the disclosure in accordance with the Accounting of Disclosures policy.

Health oversight activities

Policy: Covered Components may disclose PHI without Individual authorization for health oversight activities. Covered Components ensure that any disclosure of PHI for health oversight release is in compliance with the HIPAA Privacy Rules.

Procedures:

1. The Covered Component, through its authorized workforce members, will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting PHI, for health oversight activities.

2. Once the identity and authority of the Individual requesting PHI is confirmed, workforce members alert the HIPAA Compliance and Privacy Officer.

3. The HIPAA Compliance and Privacy Officer determines whether the disclosure is appropriate and should be made. Disclosure is appropriate to a health oversight agency for oversight activities authorized by law including audits, civil, administrative, and criminal investigations, inspections, licensure or disciplinary actions, certain civil, administrative and criminal proceedings, and activities necessary for appropriate oversight of the following:
    - the health care system;
    - government benefit programs for which health information is relevant to beneficiary eligibility;
    - entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
    - entities subject to civil rights laws for which health information is necessary for determining compliance.

4. Disclosure is not appropriate if an investigation or other activity relates to an Individual but does not arise out of and is not directly related to:
    - the receipt of health care; or
    - a claim for public benefits related to health; or
    - qualification for or receipt of public benefits; or
    - services when an individual's health is integral to the claim for public benefits or services.

Other Disclosures Required by law

Policy: Covered Components disclose PHI as required by law, to lawful authorities. PHI disclosed is to the extent required by such law.

Procedures:

1. Workforce members alert the HIPAA Compliance and Privacy Officer to requests for PHI that are represented as required by law or that the workforce member believes is required by law and is not addressed in these policies.
2. Workforce members provide any written documentation provided by requestors to the HIPAA Compliance and Privacy Officer.

Other Disclosures Required by law (cont...)	3. The HIPAA Compliance and Privacy Officer contacts requestors for documentation that satisfies the requirements of the policy entitled "verifying the identity and authority of individuals requesting PHI." 4. The HIPAA Compliance and Privacy Officer or Privacy Liaison consult legal counsel, **as necessary**, to determine whether the disclosure should be made. 5. The HIPAA Compliance and Privacy Officer approves the disclosures. 6. The HIPAA Compliance and Privacy Officer obtains the relevant PHI, and reviews against the request prior to making a disclosure. The HIPAA Compliance and Privacy Officer directs authorized workforce members to note the disclosure in the Accounting of Disclosures log.
Research Purposes	Refer to policy entitled "Disclosing PHI for Research."
Cadaveric organ, eye, or tissue donation	**Policy**: Covered Components may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation. An Individual's authorization to the disclosure is not required. **Procedures**: 1. The Covered Component, through its authorized workforce members, follows appropriate policies and procedures for verifying the identity and authority of individuals requesting PHI. 2. Once the identity and authority of the Individual requesting PHI is confirmed, the Covered Component alerts the HIPAA Compliance and Privacy Officer. STARFlight workforce members alert the STARFlight privacy representative. 3. The HIPAA Compliance and Privacy Officer or STARFlight makes the determination as to whether the disclosure is appropriate and should be made.
Whistleblowers	**Policy:** Workforce members or business associates of Travis County may disclose PHI when workforce members have a good faith belief that a Covered Component has engaged in a conduct that is unlawful or that otherwise violates professional or clinical standards OR when a Covered Component provides conditions that could endanger a patient or patients, workers, or the public. Workforce members may disclose this PHI to: • A health oversight agency; or • A public health authority authorized by law to investigate or oversee the conduct the employee has good faith to believe is unlawful; or • An appropriate health care accreditation organization to report allegations of failure to meet professional standards or misconduct by a Covered Component; or

Whistleblowers (cont...)	• An attorney retained by or on behalf of the workforce member or a business associate to determine legal options for those parties with respect to this policy and 45 C.F.R. 164.502 (j)(1)(i). **Procedures:** 1. Workforce members make reasonable efforts to limit the disclosure to the minimum amount necessary. 2. Workforce members are not required to track these disclosures.
Workforce members who are victims of a crime	**Policy:** Workforce members who are victims of a criminal act may disclose PHI to a law enforcement official when: • The PHI disclosed is about the suspected perpetrator of the act; and • The PHI disclosed is limited to the following information: ○ 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 ○ Description of distinguishing characteristics (such as height, weight, race, hair and eye color, scars, tattoos) Authorized workforce members do not disclose any PHI related to DNA or DNA analysis, dental records or typing, samples or analysis of body fluids or tissue. **Procedures:** Workforce members may seek the assistance of the HIPAA Compliance and Privacy Officer when making such disclosures.

Special PHI Disclosure

1. The requested PHI will be reviewed before disclosure to the requesting party. If the PHI to be disclosed includes genetic information, HIV-related information, mental health information, or substance abuse treatment records, more specific procedures apply:

HIV/AIDS Information

1. Covered components **do not** disclose HIV/AIDS-related information unless required by law or pursuant to an Individual's authorization. Where PHI contains HIV/AIDS-related information, the HIPAA Compliance and Privacy Officer is alerted, and the HIPAA Compliance and Privacy Officer consults with the Legal Counsel.

Mental Health Information

1. Covered components **do not** disclose mental health information unless authorized by Chapter 611 of the Texas Health & Safety Code. Where PHI contains mental health information, the HIPAA Compliance and Privacy Officer is alerted, and the HIPAA Compliance and Privacy Officer consults with the Legal Counsel.

Genetic Information

1. Covered components **do not** disclose genetic information without the written authorization of the Individual or as allowed by law. Where PHI contains genetic information, the HIPAA Compliance and Privacy Officer is alerted, and the HIPAA Compliance and Privacy Officer may choose to consult with the Legal Counsel.

Substance Abuse Treatment Records

1. Covered components **do not** disclose substance abuse treatment records without the written authorization of the Individual. Where PHI contains substance abuse treatment records, authorization must be obtained from an Individual.

Uses and Disclosures of PHI

Policy # 2.4.1

Disclosing PHI for Research

Original Effective Date: 10/24/2016

Revised Date: 3/28/2022

Purpose: To establish a formal process to ensure the privacy and confidentiality of PHI when participating in research activities that involve the disclosure of PHI.

Policy: Travis County Covered Components will use de-identified information whenever possible. If de-identified information cannot be used, Travis County Covered Components generally obtain either (1) patient or client authorization, (2) a complete or partial waiver, or (3) a data use agreement. All research projects are evaluated on a case-by-case basis, and participation in research activities is allowed only when approved in accordance with the process set forth in this policy. Failure to submit research proposals in accordance with this process may result in the denial of research requests.

Process:

1. Covered Components wishing to participate in research involving PHI will provide the research proposal to the HIPAA Compliance and Privacy Officer and/or Legal Counsel as soon as possible for evaluation, and no later than **3** weeks prior to the expected release of the data. Proposals submitted to the HIPAA Compliance and Privacy Officer and/or Legal Counsel must be approved through any internal department processes first. The research proposal must:
    - Include the name and contact information of the researcher
    - Identify the purpose of the research
    - Identify the subjects or class of subjects whose PHI will be required as part of the research
    - Identify the data fields to be provided and/or analyzed in the course of research
    - Describe how the research is likely to benefit Travis County or its clients
    - Demonstrate a plan for maintaining the confidentiality of any PHI requested
    - Provide a date by which the data will be required by the researcher

2. If the researcher represents that the data to be disclosed by the Covered Component is not PHI, Covered Components must verify the accuracy of the researcher's statement. Covered Components will consult the policy entitled, "De-identification of PHI" to confirm that the requested data does not constitute a "specific identifier" as set forth in 45 C.F.R. 164.514 (e)(2). In the event that the Covered Component is unable to confirm that the data is not PHI, the Covered Component will provide the research proposal to the HIPAA Compliance and Privacy Officer and/or Legal Counsel. The HIPAA Compliance and Privacy Officer and/or Legal Counsel will determine whether the research involves PHI; **when requested**, the HIPAA Compliance and Privacy Officer will make this determination.

3. The HIPAA Compliance and Privacy Officer or Privacy Liaison will review the research proposal and, where necessary, contact the researcher to obtain further documentation. The documentation required to be submitted is listed in procedure 4 below.

4. The HIPAA Compliance and Privacy Officer or Liaison may approve the disclosure of PHI when the researcher presents any one of the following:

Documentation	Requirements
Valid Authorization	Disclosure may be approved when: Covered Components are able to obtain valid Authorizations from Individuals for participation in the study. Valid Authorizations are obtained in accordance with policy 2.4, Authorization for the Release of PHI.
Written proposal to review PHI in preparation for research	Disclosure may be approved when the researcher certifies in writing that: • The disclosure of PHI is necessary to prepare a research protocol or other similar preparatory purpose. • The PHI will not be used in any research prior to IRB approval. • The PHI will not be removed from the Covered Component. • De-identified data cannot be used for this purpose. PHI released for this purpose allows researchers to do such things as identify prospective research participants, review charts or records, and review data base queries. Recruitment of Individuals for a study is <u>not allowed</u> as part of these activities.

Written representations	Disclosure of *decedents' information* may be approved when the researcher: • Represents that the disclosure pertains solely to deceased individuals • Produces documentation of the death of such individuals; and • Represents that the PHI to be disclosed is necessary for the research.
Signed Data Use Agreement	Disclosure of a limited data set must be approved by the Travis County Commissioners Court. The Commissioner's Court is the signatory for any data use agreement executed with the researcher. The HIPAA Compliance and Privacy Officer works with legal counsel and the Covered Component to: • Ensure that the limited data set excludes the direct identifiers set forth in 45 C.F.R. 164.514 (e)(2). • Ensure that the data use agreement is appropriately executed prior to the data release.

5. Prior to making such disclosures:

   a. The HIPAA Compliance and Privacy Officer must have all documentation supporting the release of the data.
   b. The Security Officer must determine that the proposed method of transmitting the data is secure.

6. Unless the data is disclosed as part of a limited data set or pursuant to a valid Authorization, disclosures for most research purposes must be tracked in accordance with the policy entitled "Accounting of Disclosures."

Uses and Disclosures of PHI

Policy # 2.5

Authorization for Release of PHI

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To provide authorization requirements for uses and disclosures of PHI that are not permitted or required under HIPAA.

Policy: Travis County Covered Components will obtain authorizations for release of PHI from an Individual when a disclosure of PHI is not otherwise permitted or required under HIPAA. Covered Components receiving valid authorizations use or disclose PHI consistent with the authorization. Authorizations include required core elements under HIPAA and applicable Federal, State laws, rules, and regulations.

Process:

Distribution of Authorization Forms

1. The HIPAA Compliance and Privacy Officer will provide Travis County Covered Components with the Authorization to Release PHI Form that has been developed to comply with the requirements of the HIPAA Privacy Rule. Covered Components do not alter the Authorization Form in any way, except that Covered Components may place their seal on the Authorization Form.

2. Covered Components distribute the Authorization to Release PHI Form to Individuals who seek the release or disclosure of their PHI. Alternatively, the Covered Component directs the individual to obtain the Authorization Form from the Travis County website (HIPAA Policies and Procedures).
    - NOTE: An Individual's personal representative may request the Individual's PHI and is subject to the Verifying of identity and Authority of a person requesting PHI.

3. A Covered Component seeking to use or disclose PHI for any purpose other than those set forth in the policy entitled "Permitted Uses and Disclosures of Protected Health Information" requests that an individual completes an Authorization Form. An Individual's authorization is **always** required to use or disclose **psychotherapy notes** for purposes other than those set forth below:
    - For treatment;
    - For internal training programs in which mental health trainees learn to practice their skills in group, joint, family or Individual counseling;
    - For the Covered Component's own defense in a legal proceeding brought by the Individual;

- When the disclosure is required by the Secretary of Health and Human Services to investigate a Covered Component's compliance with HIPAA requirements;
- When the disclosure is required by law;
- When the disclosure is required for health oversight activities;
- When the disclosure is to a medical examiner or coroner who is carrying out his or her lawful duties; **or**
- When disclosure is necessary to:
    - prevent or lessen a serious threat to the health or safety of a person or the public, **or**
    - identify or apprehend an Individual who has escaped from lawful custody or has admitted to participating in a violent crime believed to have caused serious harm to the victim

Obtaining and Retaining Authorizations

1. Individuals seeking PHI, or who have been requested to disclose PHI using an Authorization, **must complete**, **sign and submit** an Authorization Form to the Covered Component that holds the subject PHI. An Authorization may not be combined with any other document unless one of the following exceptions applies:
    - Authorizations to use or disclose PHI for a research study may be combined with any other type of written permission for the same research study, including a consent to participate in such research;
    - Authorizations to use or disclose psychotherapy notes may be combined with other Authorizations related to psychotherapy notes; or
    - Authorizations to use or disclose PHI other than psychotherapy notes may be combined, but only if the Covered Component has not conditioned the provision of treatment or payment upon obtaining the Authorization.

2. The Covered Component will forward a copy of the Authorization Form to the HIPAA Compliance and Privacy Officer or Privacy Liaison.

3. The HIPAA Compliance and Privacy Officer or Privacy Liaison will verify that the Authorization Form is complete and valid prior to directing the Covered Component to disclose the requested PHI.

4. If the Authorization is incomplete or invalid, the requestor is notified of the Authorization's deficiencies and told that they must be corrected. In the event that an Individual provides an Authorization on a form that was not developed by the HIPAA Compliance and Privacy Officer, the HIPAA Compliance and Privacy Officer or Liaison may request that the Individual re-submit the Authorization using the Travis County Form (Authorization to Release PHI Form) or may review and confirm that the submitted Authorization contains all of the elements required by law.

5. When a valid Authorization is received, the HIPAA Compliance and Privacy Officer or Privacy Liaison directs the Covered Component to disclose only the PHI specified in the Authorization.

6. The Authorization Form is retained by the Covered Component who received it for **6** years from the date of execution. The Authorization will be filed in the Individual's medical record or health plan file.

7. Covered Components **may not require** an Authorization to treat an Individual **except** if:

   - The creation of the PHI is done specifically to disclose the PHI to a third party.
   - The covered component is a health plan, and the authorization is a condition of eligibility for enrollment if the purpose is to determine underwriting or risk rating. This exception does not apply to authorizations for a use or disclosure of psychotherapy notes.

Revocation of Authorization

1. The requestor may revoke an Authorization in writing at any time, however, disclosures made by Travis County in reliance on the Authorization before Travis County receives the revocation are not subject to the revocation.
2. ***The Authorization may ONLY be revoked in writing***. Questions regarding revocation should be directed to the HIPAA Compliance and Privacy Officer.
3. Upon receipt of a written revocation, the Covered Component will forward the revocation and the original Authorization Form to the HIPAA Compliance and Privacy Officer or Privacy Liaison.
4. The HIPAA Compliance and Privacy Officer or Liaison will write the effective date of the revocation on the original Authorization Form.
5. When Authorizations are revoked, Travis County Covered Components no longer use or disclose the Individual's PHI for any purpose other than those set forth in the policy entitled "Permitted Uses and Disclosures of Protected Health Information."
6. The person who discloses the PHI, either an authorized workforce member or the HIPAA Compliance and Privacy Officer or Privacy Liaison, appropriately documents the request and delivery of the PHI on the tracking log provided by the HIPAA Compliance and Privacy Officer. Such tracking log will be completed as described in the policy Accounting of Disclosures (called "Tracking" in this table).

   Each revocation will be filed in the individual's medical record or health plan file and retained for **6** years from its effective date.

Uses and Disclosures

Policy # 2.6

De-Identification of PHI

Original Effective Date: 10/24/2016

Revised Date: 3/28/2022

Purpose: To establish methods for properly de-identifying PHI such that it is no longer PHI under HIPAA.

Policy: Travis County de-identifies PHI when it is possible and appropriate prior to disclosing data. If, **at any time**, a workforce member suspects that data to be released or that has been released is not de-identified, then the workforce member is required to report this suspicion to the HIPAA Compliance and Privacy Officer immediately. **De-identification of PHI or PII ensures personal data cannot be linked to an individual. De-identification is achieved by removing certain data elements from a data set so that the information could no longer be used to identify a specific individual.**

Process: PHI may be de-identified in one of three ways: a) the safe harbor method, b) the expert determination method or c) De-Identifying Images.

A) **Safe Harbor Method:** Covered Components, in consultation with the HIPAA Compliance and Privacy Officer, will remove the following 18 specific identifiers:

i. Names (including initials or partial names)

ii. All geographic subdivisions smaller than a state (including street address, city, county, precinct, zip code, and their equivalent geocodes), except for the first three digits of a zip code.

- **Note: For the following 17 partial Zip Codes, even the first three digits are considered an "identifier" and must be instead changed to "000" in order for it to meet the De-Identification standard: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893.**

iii. All elements of dates, **except year**, directly related to an individual (for example, birth date, admission date, discharge date, Treatment dates, date of death).

- **Note:**
  - **Ages 89 and less may be used, but ages 90 and greater must be changed to "90 or older."**
  - **It is permissible to convert dates to time periods using years (for example, "years between diagnosis and death: 3").**

iv. Telephone numbers.

v. Fax numbers.

vi. E-mail addresses.

vii. Social Security numbers.

viii. Medical record numbers.

ix. Health plan beneficiary numbers.

x. Account numbers.

xi. Certificate/license numbers.

xii. Vehicle identifiers and serial numbers, including license plate numbers.

xiii. Device identifiers and serial numbers.

xiv. Web Universal Resource Locators (URLs).

xv. Internet protocol (IP) address numbers.

xvi. Biometric identifiers including finger and voice prints.

xvii. Full face photographic images or other identifying images (for more information on de-identifying images, see procedure 2(c)).

xviii. Any other unique identifying number, characteristic or code (for example, study ID numbers), except as permitted under procedure 3 below.

B) <u>Expert Determination Method:</u> Covered Components may request written approval from the HIPAA Compliance and Privacy Officer to utilize the expert determination method when:

1. A person ("expert") with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable can be utilized to de-identify the information**;** and
2. The expert applies generally accepted statistical and scientific principles to determine the risk is very low that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information; and
3. The expert documents the methods and results of the analysis that justify such determination.

C) <u>De-identifying Images</u>

1. Covered Components remove identifiable traits on images of individuals such that it is not possible for someone (including an individual in the image) to recognize the individuals.
    a. For example, Covered Components obscure identifying markings such as the face, tattoos, birth marks, scars, and fingerprints. If, after obscuring the individual's face, the individual's body is still unique enough to be recognizable, the image is not considered de-identified.

b. Covered Components remove all identifying writing from diagnostic images, including the data and time that the image was taken, or any other number assigned to the image for identification purposes.

c. Covered Components de-identify images such that the image cannot be easily restored to its identified state. Common methods such as layering shapes over the image in a computer "paint" program are not sufficient to de-identify the image.

2. In the event that a Covered Component wishes to re-identify the individuals whose PHI is to be disclosed, the Covered Component may assign a unique code to each individual. The code will not be a "specific identifier" as described in procedure 2(a) provided that:

   a. The code is not derived from or related to information about the Individual and is nototherwise capable of being translated so as to identify the individual.

   b. Covered Components do not use or disclose the code for any other purpose and do not disclose the mechanism for re-identification.

   c. Covered Components restrict access to the code to those workforce members who require it.

   d. Covered Components do not provide the code to the researcher receiving the de-identified data.

3. The Covered Component consults with the HIPAA Compliance and Privacy Officer to ensure that the information or image has been properly de-identified.

   - Note: Workforce members are strictly **prohibited** from disclosing identifiable data or a unique access code assigned to de-identified data without first consulting with the HIPAA Compliance and Privacy Officer.

Uses and Disclosures of PHI

Policy # 2.7

Business Associates

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To outline a policy and procedure for ensuring that Travis County has entered into appropriate business associate agreements and manages the business associate relationship appropriately.

Policy: Travis County executes business associate agreements that define the use and disposition or destruction of PHI that is shared with certain contractors so that they can provide services needed by one or more covered components.

Process:

About Business Associates

Travis County often requires the assistance of a third party to conduct the business of its covered components. When it is necessary for the third party to acquire, access, use or disclose PHI or the contractor ‘‘creates, receives, maintains, transports, destroys or transmits’’ PHI on behalf of a covered component to provide the services described in the contract, the third party is a “business associate” under HIPAA. Contractors that maintain or store PHI on behalf of a covered component are also business associates, even if they do not actually access or use the PHI. Examples of these contractors include third party document scanning companies, document storage companies and IT companies whose maintenance agreements require access that could include PHI.

HIPAA requires Travis County to enter into a contract, or “business associate agreement” (BAA) that defines how this PHI can be used by these contractors.

Solicitation Development or Contract Modification Requests

1. When a solicitation request is developed by a department or when a contract is modified in a way that results in a contractor’s need to “acquire, access, use or disclose, create, receive, maintain, transport, destroy or transmit” PHI on behalf of a covered component, project managers responsible for the request for a solicitation conduct a thorough review of information flows that could involve PHI related to the service. The HIPAA Compliance and Privacy Officer or Security Officer is available to assist these workforce members with this review.

2. When requesting the procurement from the Purchasing Agent, the Purchasing Agent’s designated Buyer, the project manager provides a copy of a completed “**Vendor BAA Assessment**” to the HIPAA Compliance and Privacy Officer for review by electronic mail with a copy to the designated Buyer. The HIPAA Compliance and Privacy Officer consults with any appropriate parties, including the Security Officer, to determine whether a Business Associate Agreement is required.

3. The Purchasing Agent includes appropriate information related to HIPAA and Travis County requirements in solicitations for services that result in new business associates.

    a. If the preferred respondent to the solicitation is either unwilling or unable to comply with applicable HIPAA requirements, the workforce members must either select another respondent or project managers and workforce members must modify the requested service arrangement so that no PHI is acquired, accessed, used, disclosed, created, received, maintained, transported, destroyed or transmitted by the preferred respondent on behalf of a covered component so that there are no applicable HIPAA requirements and a business associate agreement is no longer necessary.

4. The Buyer, the project manager, or other responsible workforce members must attempt to include the right to review all practices, policies, and books of the business associate to ensure compliance in each business associate agreement.

5. If a workforce member becomes aware that an existing contractor might acquire, access, use, disclose create, receive, maintain, transport, destroy or transmit PHI on behalf of a covered component and is unsure of whether-or-not a Business Associate Agreement is in place, the workforce member reports this information to the HIPAA Compliance and Privacy Officer as soon as possible and the contractor is consulted to determine whether the contractor does provide any of these services on behalf of a covered component. If so, the Purchasing Agent and project manager and other involved workforce members negotiate a modification to the services contract with the contractor and the County and contractor must enter into a business associate agreement unless other or additional remedies can be implemented.

Contract Award/Modification

1. The County Attorney's office develops the business associate agreement for execution in conjunction with services contracts in which the contractor will acquire, access, use, disclose, create, receive, maintain, transport, destroy or transmit PHI on behalf of a covered component.

Business Associate Database

1. The Purchasing Agent, or the Purchasing Agent's designee, maintains a list of Business Associates with copies of their Business Associate Agreements on a SharePoint or SAP sites. The HIPAA Compliance and Privacy Officer and the Security Officer, and others who might require access, have access to this site.

Breaches Reported by Business Associates

1. Business Associates are contractually required to report breaches to Travis County. Workforce Members that receive reports of breaches in performance of business associate agreements by business associates should immediately contact the HIPAA Compliance and Privacy Officer or the Security Officer.

Uses and Disclosures of PHI
Policy # 2.8

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Safeguarding PHI: Use and Storage

Purpose: To provide a policy and standards for the safeguarding of PHI by workforce members.

Policy: Travis County**, to the extent possible**, implements measures to safeguard against the inappropriate disclosure of PHI.

Process:

Administrative Safeguards

1. The HIPAA Compliance and Privacy Officer will implement policies and procedures to prevent, detect, contain, and correct violations of the HIPAA Privacy Rule.

2. The HIPAA Compliance and Privacy Officer will periodically review these policies and procedures and will conduct evaluations of each Covered Component's compliance with these policies and procedures.

Physical Safeguards

Covered components ensure that reasonable physical safeguards are in place to ensure the privacy of PHI. For example, in County facilities where conversations involving PHI regularly occur, office spaces and cubicles should be located in areas that limit the ability of unauthorized persons to access PHI. Whenever possible, unauthorized persons are not allowed into areas where PHI is used or stored.

Physical Safeguards for Conversations

1. In County departments in which conservations, whether face-to-face, by telephone, or Remote Home Environments involve PHI, conversations are conducted:
    - In a private office; or
    - if no private office is available, in a non-public area where no other workforce members are present; or
    - if a public area cannot be avoided, only after unauthorized workforce members are asked to vacate the area and noise cancelling devices, fans, or other noise distorting equipment have been previously installed; or
    - using lowered voices to minimize the possibility that unauthorized persons may overhear a conversation; and
    - without excessive use of the Individual's name.

2. Workforce members should not leave a detailed message on an individual's answering machine or an individual's voice mail without an individual's consent. Only a generic message, **containing as little PHI as possible**, should be left.

Physical Safeguards for Printers, Copiers, and Fax Machines

1. In County departments or Remote Home Environments in which PHI is printed, copied, or faxed, the machines that perform these functions will be:
    - located in areas that are not easily accessible to unauthorized persons;
    - placed behind locked doors; and
    - if placement behind locked doors is not possible, have PIN controlled access capabilities.

2. Moreover, workforce members will:
    - promptly remove documents containing PHI from the printer, copier or fax machine;
    - mark all pages of an outgoing fax containing PHI as **"CONFIDENTIAL"**;
    - attach a facsimile cover sheet to an outgoing fax that:
        - informs the recipient of the fax that the information in the fax is confidential,
        - identifies the proper recipient, and
        - directs any other person who receives the fax to notify the sender of the error;
    - program frequently used numbers into the fax machine;
    - periodically check numbers programmed into the fax machine for accuracy;
    - verify the accuracy of new fax numbers before faxing PHI;
    - review fax confirmation sheets to determine whether the intended destination matches the number on the confirmation; and
    - promptly inform the HIPAA Compliance and Privacy Officer of any misdirected faxes. Workforce members may contact any unintended recipient of a fax to instruct the recipient to destroy the misdirected fax.

Physical Safeguards for PHI Maintained in Hard Copy Format

1. In County departments in which PHI is maintained in hard copy form, workforce members will:
    - clean desks and working areas such that all PHI is properly secured;
    - place documents containing PHI in a
        - locked file,
        - locked drawer,
        - locked room, or
        - safe;
    - Shred documents containing PHI or place the documents in secured shred bins for Travis County contractors to shred.
    - **Keep documents containing PHI at the office** (i.e., will not transport hard copies of PHI offsite.) Should the workforce member need to transport documents offsite, paper copies of PHI are not to be left unattended in vehicles or in alternate worksites.

Technical Safeguards

1. Workforce members under the authority of the Commissioners Court abide by the policies and procedures set forth in the Travis County Security Policies, which can be accessed on Travis Central under the ITS Security link, or by contacting the Security Officer. Workforce members pay particular attention to policies related to the use of county computers and the transmission of sensitive data.

2. Workforce members under the authority of a non-Commissioners Court Elected or Appointed officials abide by the Information Security Policies and Procedures adopted by the particular Elected or Appointed Official, where that Elected or Appointed Official has not adopted the policies and procedures set forth by the Chief Information Officer.

3. When transmitting PHI (such as when responding to an individual's request for PHI by mailing a requested flash drive), workforce members use reasonable and appropriate safeguards based on the method of transmission to ensure that unauthorized individuals will not be able to access such PHI. If an Individual emails a Workforce Member about an issue involving PHI, such Workforce Member should ask whether to **encrypt** the reply email and describe the risks of not encrypting an emailed communication.

In addition, workforce members acting on behalf of Travis County or any of its Covered Components take all reasonable precautions to safeguard PHI from all intentional and unintentional uses or disclosures in violation of the privacy rule, including storing electronic files (ePHI) securely. Workforce members ***DO NOT*** store files on local drives. Workforce Members will **NOT** use personal emails, texts, phones, software, hardware, computers, or any other device or mechanism ***NOT AUTHORIZED*** by Travis County to receive, send, transmit, store, or disclose PHI. Files containing PHI (ePHI) are stored on ***AUTHORIZED*** Servers and Travis County devices.

Individual's Access to PHI

Policy # 3.1

Provision of Notice of Privacy Practices

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To ensure that a Notice of Privacy Practices is provided to Individuals in accordance with HIPAA regulations.

Policy:
Travis County provides its Notice of Privacy Practices (**"Notice"**) consistent with the procedures described herein, and in accordance with HIPAA and State regulations.

Process:

1. The Travis County HIPAA Compliance and Privacy Officer maintains the Notice of Privacy Practices (**"Notice"**) for Travis County.

   Note: Individuals who reside in correctional institutions *DO NOT* have a right to a Notice of Privacy Practices.

2. The HIPAA Compliance and Privacy Officer also ensures that the Notice is posted on the County website and ensures substantial revisions are posted by their effective date.

3. In the event that the HIPAA Compliance and Privacy Officer makes a material change to the Notice, the HIPAA Compliance and Privacy Officer sends the revised Notice to the Covered Components, along with guidance on how to implement the changes contained in the Notice.

4. The Notice will be provided to enrollees, named insureds, and patients, and receipt of notice will be documented as follows:

Type of Covered Component	Health Plan	Health Provider
Providing the Notice	Notice must be provided to new enrollees (not the enrollee's dependents) and the named insureds: 1. at the time of enrollment or re-enrollment. 2. to the named insured of a policy under which coverage is provided or to the named insured and one	Notice must be provided to patients (clients): 1. at the first service encounter; **and/or** 2. as soon as possible after emergency treatment. The Notice of Privacy Practices must also be posted in a prominent location in the office for patients to see.

Providing the Notice (cont...)	or more dependents, when requested. 3. Notice must also be posted on any page of the group health plan's website that provides information about the group health plan's benefits.	N/A
Receipt of Notice	No Procedure Required.	1. Workforce members ask patients to sign a copy of the Travis County Notice. (which has a signature block) and file the Notice in the patient's file. 2. Patients are given an additional copy of the Notice. 3. Patients may refuse to sign the Notice. Workforce members note the refusal on the Notice and place it in the patient's medical record.
Revised Notice	The revised Notice, or information about the material change and how to obtain the revised notice, will be provided to individuals then covered by the health plan within **30** days of the material revision to the notice. The Revised Notice must also be posted on any page of the group health plan's website that provides information about the group health plan's benefits.	The revised Notice will be provided to patients upon request and will be posted in a prominent location in the office.

*****SPECIAL NOTE:***

General Rule. The Privacy Rule provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information about the individual, as well as his or her rights and the covered entity's obligations with respect to that information. Most covered entities must develop and provide individuals with this notice of their privacy practices. **The Privacy Rule does not require the following covered entities to develop a notice:**

***Health care clearinghouses:** If the only protected health information they create or receive is as a business associate of another covered entity. See 45 CFR 164.500(b)(1).

A correctional institution: A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; or

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

> **(i)** ***Permitted uses.*** A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.
>
> **(ii)** ***No application after release.*** For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody. See 45 C.F.R. §164.512(k)(5)(i).

A group health plan: That provides benefits only through one or more contracts of insurance with health insurance issuers or HMOs, and that does not create or receive protected health information other than summary health information or enrollment or disenrollment information. See 45 CFR 164.520(a).

Individual's Access to PHI

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Policy # 3.2

Rights to Access PHI

Purpose: To establish written policies and procedures regarding the rights of Individuals to access, inspect and/or obtain copies of their PHI in a timely manner.

Policy: Travis County Covered Components process Individual requests for access to PHI maintained in a designated record set in accordance with the procedures outlined below.

Process:

Request Submission

1. Workforce Members of the Covered Component directs Individuals to make requests for accessing, inspection of, or copies of PHI to the HIPAA Compliance and Privacy Officer via submission of a Request to Access PHI Form or an email to privacy@traviscountytx.gov.

2. Upon receipt of a request, the Covered Component or Compliance and Privacy Office informs the Individual of such receipt and logs the request in order to track it and issue a timely response.

3. Workforce member at the Covered Component or the Compliance and Privacy Office accesses the Individual's PHI and securely transmits it to the requestor. In the event that the Individual's PHI is not maintained in a designated record set by Travis County, the Covered Component makes the Privacy Office aware of this fact, and the Privacy Office closes the request upon issuing a response to the requesting Individual.
    a) When Travis County has knowledge of where the PHI is maintained, the HIPAA Compliance and Privacy Office response will include information about where the Individual may direct his or her request.

Determining Access in Whole, or in Part

1. The HIPAA Compliance and Privacy Officer, in consultation with the departmental Privacy Liaison and the Legal Counsel, **as needed**, review the request for PHI, **as necessary**. Requests are granted to the extent that they are not otherwise prohibited/unauthorized. The allowed reasons for denying access to an Individual include, but are not limited to, those set forth in the table below.

Table 1: Bases for denials.

Basis	Description or criteria
PHI is specifically excepted from rights of access under HIPAA	• Psychotherapy Notes • Information compiled to use, or anticipated to be used in a civil, criminal, or administrative action or proceeding.

Access to PHI is likely to endanger the life or physical safety of the Individual or another person; or access would jeopardize the health, safety, security, or rehabilitation of an Individual inmate or another person.
 	
Special Note:
Please see website link below to Inmates Rights on who can access their PHI.
Confidentiality and Release of Protected Health Information (texas.gov)
	The covered component is:
	• All or part of a correctional institution **or**
	• A Business Associate covered entity acting on behalf of a correctional institution **and either**
	  ○ the health, safety, security, custody, or rehabilitation of the Individual or of other inmates would be jeopardized, **or**
	  ○ The safety of any officer, employee, or other person at a correctional facility, or responsible for transporting an inmate would be jeopardized

PHI was created or obtained in the course of research and such research is still in progress	• The PHI was created or obtained by a covered health care provider conducting research • The Individual agreed to the denial of access during the research phase, and • The health care provider has informed the Individual that the right of access will be reinstated upon completion of the research
PHI was confidentially obtained	• The PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be likely to reveal the source of the information

Notification of the Response

1. The HIPAA Compliance and Privacy Officer sends a written notification to the requesting Individual, **in plain language**. The notice must include the following information:

    a. Whether or not access is granted to the whole designated record set, or only part of it.

    b. The format in which Travis County will provide access as discussed in Procedure 7 of this policy,

    c. Whether any fees apply to the requested access as discussed in Procedure 8 of this policy, and

    d. If access is denied:
        i. the basis of the denial
        ii. a statement that the denial is reviewable and instructions on how an Individual can request a review, if applicable
        iii. a description of how the Individual may complain to Travis County about our privacy policies or to the Secretary of the U.S. Department of Health and Human Services

    e. The HIPAA Compliance and Privacy Officer's name, phone number, and email

Providing Access

1. Covered Components provide the Individual, or the person designated by the Individual, with access to the requested PHI within **30** days of the request.

    a. If the Covered Component **cannot** fulfill the request for access within **30** days, the Covered Component may ask the HIPAA Compliance and Privacy Officer for an extension with sufficient reason to extend.
    b. The HIPAA Compliance and Privacy Officer may approve **one (30)** day extension.
    c. Upon the granting of an extension, the HIPAA Compliance and Privacy Officer (or Department, if deemed more appropriate) sends the Individual a written statement containing the reasons for the delay and the date by which Travis County expects to respond to the request.

        - **NOTE**: Before providing PHI to the person designated by the Individual, workforce members must verify the identity of the person requesting PHI (see the procedure entitled: "Verifying the Identity and Authority of a Person Requesting PHI") and use reasonable safeguards to protect the information that is being used or disclosed, such as ensuring that the third-party recipient's contact information is correctly entered prior to transmission.

2. The HIPAA Compliance and Privacy Officer, or Covered Component as mutually agreed upon, provides access to the PHI in the format requested by the Individual, if that format is readily available. If the

requested format is not readily available, Travis County provides the PHI in a readable hard copy, or in another form agreed to by Travis County and the Individual.

a. When providing PHI to an Individual, **in any form**, Workforce Members ensure that reasonable safeguards are in place to protect the PHI. For example, before sending an email to an Individual, Workforce Members will inform the Individual that all emails containing PHI will be **sent encrypted**. Workforce Members will send a 2nd email with instructions on how to decrypt.
b. Workforce Members **do not** provide copies of records on external media storage devices **provided by the individual** such as USB ("flash" or "thumb") drives or CD's. Plugging such devices into County equipment risk introduction of viruses and other malicious software onto the County's computer network. In such cases, the County may offer an alternative, such as the provision of that type of media or other means.

- **NOTE:** A summary or explanation of the requested PHI will be provided in lieu of access only when the Individual agrees to the summary or explanation and pays any related fees in advance.

Fees Imposed for Providing Access

1. The HIPAA Compliance and Privacy Officer determines if there are any cost-based fees associated with the access. Unless the actual costs associated with labor, copying, supplies, postage, retrieval from storage, or preparation of summary information represents a high cost to the County, Travis County tries to provide copies of PHI at no cost. Otherwise, the County charges a flat, cost- based fee not to exceed ***$10.00***.

Review of Denial of Access

1. When Travis County denies an Individual's request for access on the ground that a licensed The Health Care Professional ("Reviewing Official") in a Travis County covered component has determined, in the exercise of his or her professional judgement, that:

    a. Granting access to the PHI to the Individual or to a personal representative of the Individual is likely to endanger the life or physical safety of the Individual or another person.
    b. The PHI references another person (other than a health care provider) and the access requested will likely cause substantial harm to that other person.
    c. The Individual may request a review of denial by submitting a written request to the HIPAA Compliance and Privacy Officer or Privacy Liaison.

2. The HIPAA Compliance and Privacy Officer or Privacy Liaison will forward the request for review to a qualified licensed The Health Care Professional ("Reviewing Official") within the Covered Component. A qualified licensed The Health Care Professional ("Reviewing Official") is one that:

    a. Did not participate in the original denial of access.
    b. Is a workforce member of the Covered Component.

3. The Health Care Professional ("Reviewing Official") will determine, **within 10 business days**, whether to deny access based on the criteria set forth in Procedure 11 above. The Health Care Professional ("Reviewing Official") will report his or her decision to the HIPAA Compliance and Privacy Officer.

4. The HIPAA Compliance and Privacy Officer will inform the Individual of the Health Care Professional ("Reviewing Official")'s determination.

    a. If the Health Care Professional ("Reviewing Official") determines that the Individual should be granted access, then the Covered Component is notified and will provide access as described in Procedures 7 and 8.

5. Documentation
    a. The HIPAA Compliance and Privacy Office will appropriately document the resolution of the request and, where applicable, the delivery of the PHI.

Individual's Access to Protected Health Information (PHI)

Policy # 3.3

Requests for Restrictions on Uses and Disclosures

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To provide a process that allows Individuals to request restrictions on certain uses and disclosures of their PHI.

Policy: Travis County Covered Components review and consider Individual requests to restrict the permissible uses and disclosures of PHI. While Covered Components are generally not required to agree to the requested restrictions, they are required to permit the request. Covered Components inform all requesting Individuals of the status of their request (i.e., whether-or-not the County agrees to the request).

Process:

1. **Request Submission**. Covered Components provide, "Request for Restriction of Disclosure of PHI", to any Individual who wishes to restrict the use and disclosure of PHI for treatment, payment and health care operations **OR** to restrict the disclosure of PHI to family members and others involved in the Individual's care. The HIPAA Compliance and Privacy Office may assist the individual in completing the form.

2. **Considering Request**. The HIPAA Compliance and Privacy Officer, **as applicable**, and in consultation with appropriate workforce members, **as necessary**, decides whether to agree or disagree to the requested restriction.

3. The HIPAA Compliance and Privacy Officer must agree to the restriction if the request is to restrict health information to a ***health plan*** and:
    a) Disclosure of such health information is not required by law and is for the purpose of treatment, payment, or health care operations.
    b) The service or health care item that would be subject to the restriction has been paid in full by someone other than the health plan.

4. For most other requests, the HIPAA Compliance and Privacy Officer should consult with staff in the Covered Component, or in business associate covered components (such as the Auditor's Office), to determine the feasibility of the requested restriction. In deciding, strong consideration should be given to the need to treat or process payment for the treatment of an Individual.

Request Resolution

1. **Non-agreement**. If the HIPAA Compliance and Privacy Officer **DOES NOT AGREE** to the restriction, they will complete the applicable portion of the Request Form and provide a copy of the signed response to the Individual.

2. **Agreement.** If the Privacy Liaison or Officer **DOES AGREE** to the restriction, the affected Covered Component is promptly notified of the restriction. The requesting Individual is provided a copy of the completed Request for Restriction form, and the Covered Component adheres to the restriction, unless one of the exceptions in Procedure 6 applies.

3. **Exceptions to Restriction on Use and Disclosure**.
    a) The Covered Component is not required to honor a restriction when disclosure is to a treatment provider who is caring for a requesting Individual in need of emergency treatment and disclosure of the Individual's PHI is necessary;
        - In this case, the treatment provider must be asked not to further disclose the information.
    b) To the requesting Individual, for example, to provide the Individual with access or an accounting of disclosures; or
    c) Required by law.

Terminating a Restriction

1. A Covered Component may terminate its agreement to a restriction if:
    a) The Individual agrees to or requests the termination in writing; the Individual orally agrees or requests the termination, and the oral agreement or request is documented; or
    b) The Covered Component determines termination is necessary and the Individual has been informed of the termination. Terminations of this nature are documented in writing and are only effective with respect to PHI created or received after the Individual is informed of the termination.
        - **NOTE:** Covered Components cannot terminate restrictions identified in Procedure 2.

2. **Document Retention**. Documents related to restrictions on uses and disclosures of PHI are kept in the Individuals' records for a period of at least **6** years from the date of its creation or the date when it last was in effect, whichever is later.

Individual's Access to (PHI)

Policy # 3.4

Requests for Confidential Communications

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To ensure the right of an Individual to receive communications regarding their PHI in a means and location that the Individual feels is safe from unauthorized use or disclosure.

Policy: Travis County accommodates reasonable requests from Individuals to communicate PHI by an alternate means or to alternate locations.

Process:

General:

1. Individuals who wish to request confidential communications may do so orally or in writing by completing **"Requests for Confidential Communications"**. When an oral request is made, such request is documented and placed in the Individual's record. When a written request is made, Covered Component workforce members may provide the Individual with assistance in completing the form.

2. All reasonable requests are accommodated, and workforce members acting on behalf of the Covered Component **do not** require an explanation from the Individual as to the basis for the request.

*****Special Note:***

Health plans must accommodate an Individual's request for confidential communications if the Individual **clearly states** that the disclosure of all or part of his or her information could place the Individual in danger. The Covered Component may request or require a statement to that effect.

Individual's Access to (PHI)

Original Effective Date: 6/21/2016

Policy # 3.5

Revised Date: 3/28/2022

Designated Record Sets

Purpose: To describe the types of documents that comprise a Designated Record Set.

Policy: Travis County Covered Components maintain Designated Record Sets that include the medical records and billing information used to make decisions about Individuals.

Process:

1. Covered Components perform different roles within Travis County. For this reason, Covered Components must develop their own procedures regarding the creation of a Designated Record Set. These procedures address the amount of time that the information contained in a Designated Record Set will be retained (a "**retention period**").

2. For purposes of clarity, a Designated Record Set must include any item, collection, or grouping of information that contains PHI and is maintained, collected, used, or shared by a Covered Component or on behalf of a Covered Component if
   a) All or a portion of any record used to make decisions about an Individual.
   b) *****Special Note:***
      - ***For Health Providers****:* the record is a medical or billing record
      - ***For Health Plans****:* the record concerns enrollment, payment, claims, and case or medical management.

3. A Designated Record Set will **NOT** include:
   a) Psychotherapy notes
   b) Data collected and maintained for research
   c) Peer review data
   d) Performance improvement data
   e) Appointment and Scheduling information
   f) Employment information and records
   g) Educational records
   h) Metadata
   i) Risk Management Work
   j) Incident Reports
   k) Audit Information

4. The procedure developed by each Covered Component will be made a part of the Covered Component or Department policy, **as appropriate and necessary**.

5. Covered Components will provide the County HIPAA Compliance and Privacy Officer with a copy of the procedure, and any revisions made to it.

Individual's Access to (PHI)

Policy # 3.6

Requests to Amend Records

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To ensure the right of an Individual to request that PHI in his or her medical record be amended.

Policy: Travis County allows Individuals to request amendments to their PHI in a Designated Record Set and responds to these requests within the timelines required by HIPAA. When Travis County receives notice that another Covered Entity has agreed to amend an Individual's record, Travis County Covered Components append the amendment to the Individual's designated record set or provide a link to the amendment within an electronic record set (ePHI).

Process:

Receiving Requests for Amendments from Individuals:

1. Covered Components or the HIPAA Compliance and Privacy Officer provide **"**Request for Amendments to Protected Health Information**"**, to any individual who wishes to make such a request. The HIPAA Compliance and Privacy Officer or Privacy Liaison, **as applicable**, may assist the individual in completing the form.

2. The individual is instructed to submit the completed form to either the HIPAA Compliance and Privacy Officer or Privacy Liaison. If the form is submitted to the Privacy Liaison, the HIPAA Compliance and Privacy Officer must be provided a copy of the form for tracking purposes.

Reviewing the Amendment

1. The request will be referred to the Privacy Liaison or the HIPAA Compliance and Privacy Officer, depending on the status of the Covered Component that received the request (i.e., Commissioner Court or Non-Commissioners Court departments). The Privacy Liaison or HIPAA Compliance and Privacy Officer, **as applicable**, will work with appropriate Covered Component workforce members, and/or the Legal Counsel, to determine whether-or-not to accept an amendment **in whole or in part**.

2. The requested amendment will be evaluated by the appropriate workforce members against the denial criteria set forth below. If any of the denial criteria are met, the amendment may be denied. **If none of the denial criteria are met, the amendment must be accepted.**

Denial Criteria

- The PHI subject to the request is accurate and complete.
- The PHI subject to the request was not created by the Covered Component, and the creator of the PHI is still available.
- The PHI subject to the request is not part of a designated record set
- The PHI subject to the request is contained in psychotherapy notes.
- The PHI subject to the request would not be available for inspection under Policy entitled "Rights to Access to PHI" because it was compiled in anticipation of, or for use in a civil, criminal, or administrative action or proceeding.

Timeline:

1. Regardless of which Covered Component receives the request, ***the HIPAA Compliance and Privacy Officer is the Workforce Member responsible for enforcing deadlines.*** The time period to respond to a request for amendment is sixty **(60)** days after receipt of such request unless there is a specific reason why such timeframe cannot be met:

    a. If the timeframe cannot be met: The HIPAA Compliance and Privacy Officer may approve one thirty **(30) day** extension upon receiving a reasonable explanation as to why.
    b. The requesting Individual must be informed in writing of the extension, as well as the reason for the extension and the date by which the Covered Component will respond.

Accepting or Denying the Request for Amendment

1. ***ACCEPTING***. If the amendment is accepted, the Privacy Liaison or HIPAA Compliance and Privacy Officer, **as applicable**:

    a. Makes the appropriate amendment, either by appending the amendment to the applicable written record or providing a link to the location of the amendment for electronic records (ePHI); or arranges to have the necessary party make the amendment and;
    b. Informs the requesting Individual of the determination in writing; and
    c. Obtains the Individual's agreement to notify such other persons as would need notice of the amendment; and
    d. Makes reasonable efforts to inform and provide the amendment to persons identified by the Individual as needing the amendment; and
    e. Makes reasonable efforts to inform and provide the amendment to persons, including Business Associates, that the Covered Component knows have the affected PHI and that may have relied, or could foreseeably rely, on such information to the detriment of the Individual.

2. ***DENYING***. If the amendment is denied, the Privacy Liaison or HIPAA Compliance and Privacy Officer, **as applicable**, provides the Individual with a written denial in plain language that contains:

    a. The basis for the denial

    b. Information on the Individual's right to submit a written statement disagreeing with the denial; and

    c. A description of how the Individual may submit such written **statement of disagreement** with the denial.

    d. A statement that the Individual may ask that the request for amendment be included with the PHI in future disclosures.

    e. A description of how the Individual may complain to the Covered Component, the HIPAA Compliance and Privacy Officer, or to the Secretary of Health and Human Services, as outlined in the Notice of Privacy Practices.

    f. The name and contact information, including phone number for the HIPAA Compliance and Privacy Officer must also be provided.

        - The Covered Component:

            - Includes the Individual's request for amendment with future disclosures of the PHI to which the request relates.
            - Includes Statements of Disagreement, **if any**, with future disclosures of the PHI to which the statement relates.
            - If the statement is long, the Covered Component may provide an accurate summary of the statement with the disclosure.

3. ***Note on Future Disclosures***. When processing a HIPAA standard transaction (under 45 C.F.R. Part 162), the information may be sent separately if it cannot be transmitted with the standard transaction.

Statements of Disagreement (for amendments that were denied):

Individuals who wish to make a statement of disagreement may do so in writing and may submit that statement to the HIPAA Compliance and Privacy Officer.

1. The HIPAA Compliance and Privacy Officer:

    a. Consults with the Covered Component Workforce Members and/or the Legal Counsel's Office to determine whether-or-not a statement of rebuttal should be prepared.

        - If a rebuttal is prepared, a copy of the rebuttal is given to the Individual.

    b. Append or otherwise link the following to the designated record or PHI that is the subject of the disputed amendment:

        - the Individual's request for an amendment; and/or

- the denial of the request; and/or
- the Individual's statement of disagreement; and/or
- the Covered Component's rebuttal, **if any**.

2. **Document Retention**: The Travis County HIPAA Compliance and Privacy Officer maintains copies of all requests for amendment, and any forms related to this process for six **(6)** years.

Individual's Access to (PHI)

Policy # 3.7

Accounting of Disclosures

Original Effective Date: 6/21/2016

Revised Date: 3/28/2022

Purpose: To establish policies and procedures that govern how Individual requests for disclosures will be handled.

Policy: Travis County Covered Components provide Individuals with a list of instances in which the Individual's PHI was disclosed during the **6** years prior to the date of the request unless the County must temporarily suspend the Individual's right because of a valid law enforcement or health oversight agency activity. Covered Components provide the first list, or "**accounting"**, of disclosures requested in a **twelve-month period at no charge**.

Process:

1. Workforce members provide "**Request for Accounting of Disclosures"**, to Individuals who wish to make a request for an accounting of disclosures of their PHI. The Individual is instructed to complete and submit the Form to the HIPAA Compliance and Privacy Officer.

2. The HIPAA Compliance and Privacy Officer receives and logs this form. When the accounting is requested from a Covered Component that is a non-Commissioners Court department, the HIPAA Compliance and Privacy Officer contacts the Privacy Liaison to obtain the appropriate tracking logs.

3. The HIPAA Compliance and Privacy Officer forwards the request to the Covered Component(s) that maintains the Individual's Designated Record Set. Where the requested accounting covers disclosures of PHI made by a Business Associate, the HIPAA Compliance and Privacy Officer confers with that Business Associate to obtain the information needed to provide an accounting of such disclosures.

4. The Covered Component compiles a list of all instances in which the requesting Individual's PHI was disclosed during the six **(6)** years prior to the date of the request (the "Accounting"). The contents of the Accounting contain:
    a. Disclosures for the six **(6)** years before the request **OR** for any shorter time period requested by the Individual; and

b. Date of the disclosure; and
c. Name of the entity or person who received the PHI and the address, if known; and
d. A brief description of the PHI disclosed; and
e. A brief statement of the reason for the disclosure, or a copy of a written request for the disclosure (for example, a letter from a public health official); and
f. Any one of the following:
    - a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure;
    - a copy of the Individual's written authorization; or
    - a copy of the written request for disclosure made by a government entity.

5. For certain disclosures that occur on a regular basis, the Covered Component may provide a summary Accounting. A summary Accounting is permissible if, during the six **(6)** years prior to the request, the Covered Component has made multiple disclosures of PHI:
    a. To the same recipient pursuant to a single authorization signed by the Individual;
    b. To the Department of Health & Human Services so that the Department could investigate or determine the Covered Component's compliance with HIPAA; or
    c. To the same person or entity for a single national priority purpose.
        - the dates of the *first and last* disclosure
        - the frequency or number of disclosures during the accounting period.

6. In these circumstances, the Covered Component may limit the Accounting related to a series of disclosures to the following information:
    a. the core elements, as set forth in Procedure 4, for the first disclosure in the Accounting period; and
    b. the frequency or number of the disclosures made during the accounting period; and
    c. the date of the most recent disclosure in the series during the accounting period.

7. The Accounting may, but is **NOT** required, to contain disclosures that were made:
    a. to carry out treatment, payment, or health care operations
    b. to the Individual or to persons involved in the Individual's care where the requestor verbally agreed to the disclosure; or
    c. incidental to another permissible or required use or disclosure of PHI (as long as reasonable safeguards were observed and the minimum necessary standard was applied to the underlying communication); or
    d. pursuant to a valid authorization; or
    e. for notification purposes, such as identifying or locating a family member, or

informing a family member or personal representative of the Individual's general condition or death; or

f. for national security or intelligence purposes; or
g. to correctional facilities or law enforcement officials; or
h. as part of a Limited Data Set.

8. The Accounting is provided to the HIPAA Compliance and Privacy Officer, who must forward such list to the requesting Individual no later than sixty **(60)** days after receipt of the Individual's request and, **when applicable**, payment of the cost-based fee described in Procedure 8. If the HIPAA Compliance and Privacy Officer is unable to fulfill the request within this timeframe, the HIPAA Compliance and Privacy Officer may extend the time to provide the Accounting by thirty **(30)** days. He or she informs the requesting Individual in writing of the reason for the delay in response and the expected date by which the Covered Component will respond.

    a. **NOTE:** A health oversight agency or law enforcement official may request (orally or in writing) that a Covered Component temporarily suspend an Individual's right to receive an accounting of disclosures related to an activity of the health oversight agency or law enforcement official. When an oral request is made, the Covered Component:
        - Documents the statement, including the identity of the agency or official making the statement;
        - Temporarily suspends the individual's right to an accounting of disclosures subject to the statement; and
        - Limits the temporary suspension to no longer than thirty **(30)** days from the date of the oral statement unless a written statement from the agency or official is submitted during that time.

    b. When a written request is made, the Covered Component forwards such request to the HIPAA Compliance and Privacy Officer who suspends an Individual's right to receive an accounting of these disclosures for the time specified in the written request.

9. **Charges for Accounting of Disclosures.** Although the first Accounting within a twelve **(12)** month period is free of charge, Travis County charges a reasonable, cost-based fee for all additional requests for Accounting from the same Individual within a twelve **(12)** month period. When an Individual requests more than one Accounting in a twelve **(12)** month period, the Individual is notified of the charge for the additional Accounting and is given the opportunity to modify or withdraw his or her request in advance of its processing.

10. **Documentation.** The HIPAA Compliance and Privacy Officer documents and retains a

copy of the written accounting of disclosures made to the Individual for a period of at least six **(6)** years from the date of its creation. A copy of the Accounting is also filed in the Individual's record.