

HIPAA Privacy Checklist

This checklist can help you implement the Travis County HIPAA policies and procedures, but is not comprehensive. Consult with your supervisor or the Privacy Officer (x49766) with any questions.

	Implemented?	Comments
NOTICE OF PRIVACY PRACTICES		
Travis County Policy Reference: #3.1		
Provide to client at first service encounter or upon enrollment for health plans Make a good faith efforts to obtain acknowledgment. Make note of refusal to acknowledge and place in record.		NOT required in corrections
Post in prominent location		NOT required in corrections.
TRAINING		
Travis County Policy Reference: #1.6		
Complete annual training: -HIPAA general -Travis County Policies and Procedures -Cybersecurity Awareness		
MINIMUM NECESSARY STANDARD		
Travis County Policy Reference: #2.1		
Limit use or disclosure to the minimum necessary to accomplish the purpose, subject to specified situations.		This applies to the use or disclosure of information
Define and limit workforce members' access to protected information.		Work with the Privacy Officer to develop your access lists.
Establish protocols for routine disclosures, and processes for handling others on an individual basis.		
Redact documents as necessary to meet minimum necessary requirements.		
ACCOUNTING OF DISCLOSURES		
Travis County Policy Reference: #3.7		
Establish a log of disclosures for each patient for disclosures for: <ul style="list-style-type: none"> • Response to judicial or administrative requests (i.e. subpoena). 		

<ul style="list-style-type: none"> • Public Health activities • PHI disclosed when reporting abuse, neglect, or domestic violence • Law enforcement purposes • Coroners or Medical Examiners, and Funeral Directors • Employer compliance w/OSHA or Worker’s Comp requirements • Health Oversight Activities • Research Purposes • Cadaveric organ, eye or tissue donation • Whistleblowers reporting to lawfully authorized authorities. 		
--	--	--

SAFEGUARDING PHI

Travis County Policy Reference: #2.7

<p>Provide justification for access, by position/job class to Privacy Officer -justification for access must consider policy #2.1, minimum necessary standard. Access level is appropriate to the person and task being performed.</p>		
--	--	--

<p>Inventory access points by positions and provide to Privacy Officer</p>		
--	--	--

<p>Inventory flash drives, cd’s, and other repositories for PHI and provide to Security Officer</p>		
---	--	--

<p>Inventory paper locations of PHI & verify security. Report any concerns about security of paper.</p>		
---	--	--

VERIFYING IDENTITY AND AUTHORITY

TC Policy Reference: #2.3

<p>Implement the requirements in this policy for verifying identity and authority</p>		
---	--	--

IMPLEMENT NEW TC Forms into workflows

TC Policy References: #2.5, #2.6, #3.2, #3.3, #3.4, #3.6, #3.7

<p>Determine how forms are processed before being sent to Privacy Officer or others, as required in related policies.</p>		
<p>ACCESS LOGS</p>		
<p>TC- ITS-302 (ITS security policies)</p>		
<p>Implement periodic audits of access logs at the application level for electronic medical records: -determine event triggers that require further inquiry -establish policies and procedures for monitoring and reporting event triggers</p>		