A Mini Risk Tool

from your friends at PERSON CENTERED TECH

This tool is for informational purposes only. In order to meet HIPAA compliance requirements, this tool must be paired with the Step 4: Risk Analysis service.

Tech Stack □

Outside

- ○ There are unmet functionality needs in either/both client-serving and internal operations.
- ○ Not all third-party services that handle client info (PHI) are a practice provided and controlled asset (e.g. personal services).
- ○ HIPAA Business Associate Agreements are not executed (or available) between all third-party service providers that handle PHI and *the practice.*
- ○ Systems containing or handling PHI are not configured to prevent information being "leaked" or "forgotten."
- ○ Documentation needs being met are reliant on behavior rather than automated by systems.

Inside

- ○ All functionality needs are effectively met (client-serving & internal operations)
- ○ All third-party services that handle client info (PHI) are a practice asset
  HIPAA Business Associate
- ○ Agreements are executed between all third-party service providers that handle PHI and the practice
- ○ All the practice's systems are set up so they don't "leak" or "forget" information.
- ○ Services help maintain documentation automatically (e.g. HIPAA-secure email, phone, texting.)

Training □

Outside

- ○ All workforce have not been trained on *the practice's* P&Ps.
- ○ All workforce do not have a foundational knowledge of HIPAA, state laws, and ethics standards appropriate and necessary to their role within the practice.
- ○ Reminders and trainings to ensure the P&Ps are understood and being followed by everyone (including the leadership team) are not being made.
- ○ All workforce are not trained on the P&Ps at least once a year.
- ○ All workforce do not have the training and help they need to make sure they can properly use the equipment and services within the circle.
- ○ All workforce do not have the training they need to maintain the circle and also do their jobs without interruption.

Inside

- ○ At onboarding, all workforce receive training on the P&Ps and other registration processes (e.g. remote workspaces and BYOD.) Training on HIPAA and other laws, as necessary.
- ○ All workforce have a foundational knowledge of HIPAA, state laws, and ethics standards appropriate and necessary to their role within the practice
- ○ Reminders and trainings are continuously provided as needed to ensure the P&Ps are understood and being followed by everyone (including the leadership team.)
- ○ All workforce are formally trained on the P&Ps at least once/year.
- ○ All workforce have the training and help they need to make sure they can properly use the equipment and services within the circle
- ○ All workforce have the training they need to maintain the circle and also do their jobs without interruption.

Device Security ☐

Outside

○ All practice-owned data-handling devices have not been "hardened" with necessary technical measures (e.g. full device encryption, strong and unique encryption passcodes, anti-virus/anti-malware, firewalls, etc.,)

○ All workforce members' personally-owned devices that ever touch client info have not been "hardened" with necessary technical measures (e.g. full device encryption, strong and unique encryption passcodes, anti-virus/anti-malware, firewalls, etc.,)

○ All practice-owned and personally-owned devices that touch PHI do not qualify for Safe Harbor under HIPAA's Breach Notification Rule

○ Hardening of all practice-owned devices has not been documented

○ All workforce have not been trained on the behavioral security measures (e.g. never connecting to WiFi that doesn't meet trusted network criteria, etc.,) that must be followed for any devices that ever touch PHI and agreed to abide by them

○ All workforce member's personally-owned devices that touch PHI have not been registered and approved as meeting the BYOD policy requirements for technical security measures and accompanying behavioral security measures

○ When any device that has touched practice PHI is no longer going to be used for practice work, the device is not properly "retired" (e.g. data scrubbed/wiped, factory reset) and documented as such

Inside

○ All practice-owned data-handling devices have been "hardened" with necessary technical measures (e.g. full device encryption, strong and unique encryption passcodes, anti-virus/anti-malware, firewalls, etc.,)

○ All workforce members' personally-owned devices that ever touch client info have been "hardened" with necessary technical measures (e.g. full device encryption, strong and unique encryption passcodes, anti-virus/anti-malware, firewalls, etc.,)

○ All practice-owned and personally-owned devices that touch PHI qualify for Safe Harbor under HIPAA's Breach Notification Rule

○ Hardening of all practice-owned devices is documented

○ All workforce have been trained on the behavioral security measures (e.g. never connecting to WiFi that doesn't meet trusted network criteria, etc.,) that must be followed for any devices that ever touch PHI and agreed to abide by them

○ All workforce member's personally-owned devices that touch PHI have been registered and approved as meeting the BYOD policy requirements for technical security measures and accompanying behavioral security measures

○ When any device that has touched practice PHI is no longer going to be used for practice work, the device is properly "retired" (e.g. data scrubbed/wiped, factory reset) and documented as such

Risk Analysis &
Risk Mitigation Planning

□

Outside

- ○ The practice has not conducted and documented an “accurate and thorough assessment” of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information the practice creates, receives, maintains or transmits
- ○ Threat likelihood and potential threat realization impact have not been ranked from highest to lowest
- ○ The practice has not assessed and documented the security measures (technical, administrative, physical) used to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly
- ○ Risks have not been categorized as “addressable” and “required” for mitigation
- ○ “Reasonable and appropriate” safeguards and security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of e-PHI have not been identified
- ○ A risk mitigation plan for implementing necessary safeguards and security measures has not been created, followed, and documented
- ○ Risk analysis is not updated on an annual and as-needed basis

Inside

- ○ The practice has conducted and documented an “accurate and thorough assessment” of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information the practice creates, receives, maintains or transmits
- ○ Threat likelihood and potential threat realization impact have been ranked from highest to lowest
- ○ The practice has assessed and documented the security measures (technical, administrative, physical) used to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly
- ○ Risks have been categorized as “addressable” and “required” for mitigation
- ○ “Reasonable and appropriate” safeguards and security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of e-PHI have been identified
- ○ A risk mitigation plan for implementing necessary safeguards and security measures has been created, followed, and documented
- ○ Risk analysis is updated on an annual and as-needed basis

HIPAA Compliance Manual/ Security Policies & Procedures

□

Outside

- ○ The practice does not have a comprehensive set of formal, written security compliance policies and procedures which address each standard of the HIPAA Security Rule and specify how the practice and its workforce meet each standard
- ○ Administrative safeguard policies and procedures do not address: Security Management Process, Security Personnel, Information Access Management, Workforce Training and Management, and Evaluation standards and requirements.
- ○ Physical safeguard policies and procedures do not address: Facility Access and Control, and Workstation and Device Security standards and requirements.
- ○ Technical safeguard policies and procedures do not address: Access Control, Audit Controls, Integrity Controls, and Transmission Security standards and requirements.
- ○ Written Security P&Ps have not been implemented and followed in-practice

Inside

- ○ The practice has a comprehensive set of formal, written security compliance policies and procedures which address each standard of the HIPAA Security Rule and specify how the practice and its workforce meet each standard
- ○ Administrative safeguard policies and procedures address: Security Management Process, Security Personnel, Information Access Management, Workforce Training and Management, and Evaluation standards and requirements.
- ○ Physical safeguard policies and procedures address: Facility Access and Control, and Workstation and Device Security standards and requirements.
- ○ Technical safeguard policies and procedures address: Access Control, Audit Controls, Integrity Controls, and Transmission Security standards and requirements.
- ○ Security P&Ps have been implemented and are followed in-practice