INTERNATIONAL ASSOCIATION OF Forensic Nurses

Security
Healthcare Security & Privacy

TeleSAFE IT security policy development

Technology Compliance, Privacy and Security

The following are key concepts that should be included when developing policies for teleSAFE technology privacy and security compliance. This should not be considered a comprehensive list and additional wording may be required to meet state, tribal, and jurisdictional requirements.

Purpose:

TeleSAFE is a two-way real-time patient care communication between the SAFE/SANE at the hub site and the clinician and patient at the remote or spoke site. The hub SAFE/SANE provides guidance and support to the clinician who has less or no experience in providing sexual assault care.

TeleSAFE technology must ensure compliance/privacy and security of the private health information that is transmitted.

The following items must be in place as part of the teleSAFE program:

- Conduct a periodic risk assessment on vendor hardware and software facilitating teleSAFE sessions. The risk assessment must include usability, and privacy and security controls. Document findings, create and track remediation of high-risk findings, per HIPAA risk analysis and risk management requirements.
- A Business Associate Agreement must be signed by vendors that are storing, processing, or transmitting Protected Health Information (PHI) on behalf of a Covered Entity.
- Ensure teleconferencing vendor provides training on the product to key facility departments (e.g. IT, Compliance, Clinical).
- Ensure the teleconferencing vendor provides 24-hour technical support.
- It is highly recommended that the computer hardware used to conduct teleSAFE exams is owned and managed by the hospital or clinic; personally-owned equipment must meet all hardware, software, and operational requirements listed on the Checklist for Clinicians using TeleSAFE Technology found in this Information Technology (IT) Tool.
- Require that the computer used for teleSAFE is username and password-protected to prevent unauthorized access.
- Ensure all computers run an operating system supported by Microsoft (for Windows) and Apple (for MAC OS).
- Ensure all computers run anti-malware software that scans for and protects from computer viruses.
- Apply anti-virus software updates regularly to patch security vulnerabilities.
- Designate computers to be used for teleSAFE and prohibit other usages.
-

TeleSAFE IT security policy development

Technology Compliance, Privacy and Security

- Do not use computers used for teleSAFE sessions to process or store medical-forensic exam photos.
- Do not use computers used for teleSAFE sessions to access personal or company email.

- Do not allow users running teleSAFE sessions to have system administrator rights on those computers.
- Ensure that wireless networks used by computers to connect to teleSAFE sessions at the hub and spoke sites are encrypted.
- Ensure that voice-activated assistants such as Alexa and Siri or Apple Watch are disabled or removed from areas where teleSAFE sessions are conducted.
- Ensure that the teleSAFE computer is in a room that prevents eavesdropping of conversations, has a locking door, and is positioned away from window view to prevent others from hearing or seeing any of the teleSAFE consultations.
- Ensure that Android and Apple authorized apps for personal cell phones, tablets, or other digital devices that interact with EMR are approved by the facility and maintain the highest standard of privacy and security for personal health information. No other use of personal cell phones, tablets, or digital devices is permitted.