INTERNATIONAL ASSOCIATION OF Forensic Nurses

iTu Security
Healthcare Security & Privacy

TeleSAFE IT Security Policy Development

Sharing of TeleSAFE Exam Photography

The following are key concepts that should be included when developing policies for the sharing of teleSAFE exam photos. This should not be considered a comprehensive list and additional wording may be required to meet state, tribal, and jurisdictional requirements

Purpose:

Advancements in technology may also increase the risk of privacy and security breaches. Collaboration with the facility IT department and maintaining proper IT best practices and solutions can help to protect the privacy and security of the patient's health information.

Policy Considerations:

- Sharing photographs from the medical forensic exam (MFE) with SANE or other invested medical partners should be strictly limited to quality assurance/peer review or second opinion purposes.[1]
- Some commercial software programs include features that support the secure sharing of MFE photographs. If using such a commercial software program, confirm with the vendor or with IT that the product does share SANE photos securely.
    - ***Note:*** *Solutions that securely share sensitive photos generally allow a remote person to view the photos via a web browser without being able to copy or store the photos on their local computer*
- If sending the SANE photos via email, follow these important steps:
    - Ensure the sender has received training on any procedures and tools required for sending photos from the teleSAFE exam.
    - Double-check with the intended recipient that the destination email address is correct.
    - Ask the intended recipient if access to their email requires two-factor authentication (typically this means logging into email with a username, password, and entering a code received on the recipient's smartphone).
    - The preferred practice is to send the teleSAFE exam photos as an encrypted, zipped file attached to an encrypted email.
        - ***Note:*** *If the intended recipient does not use two-factor authentication to access email, the sender must send the photos as an encrypted, zipped file. Criminals able to gain unauthorized access to a person's email account would not be able to view the encrypted SANE photos attached to an email*

[1] Each program should have a peer review process that is defined and includes purpose of the review. Peer review should not be confused with an expert second opinion that includes consulted expert review of the medical report and photo-documentation and formal written review and conclusion that remains on the medical record. (See https://www.safeta.org/page/KIDSSectionA4)

  - Communicate the password for encrypted teleSAFE exam files to the intended recipient via phone call or text message; DO NOT send the password via email.
  - Encrypting the teleSAFE exam photos as an encrypted, zipped file may require copying the SANE photos from the digital camera's memory card to the hard drive of the computer from which the email is sent. In these cases, delete the files from the local hard drive after sending them. Use a software program specifically designed to delete files in a manner preventing them from being undeleted. ***Deleting files using Windows Explorer and then emptying the Recycle Bin does not remove the files in a manner preventing undeleting them.***
- If the intended recipient is an employee of the same organization as the person sending the teleSAFE exam photos, the recipient's computer must be equipped with software capable of deleting files in a manner preventing undeleting them.
- If sharing SANE photos via a cloud storage provider (examples include but are limited to Box, Dropbox, Google Drive, Microsoft Teams, Microsoft OneDrive, or Apple iCloud) these requirements must be met:
  - A Business Associate Agreement must be in place with the cloud vendor.
  - The cloud service must store files encrypted.
  - The cloud service must require a username and password to log in and should support the use of two-factor authentication.
  - Similar to sending SANE photos via email, upload SANE photos as an encrypted, zipped file, providing the password to decrypt the zipped file only over the phone or via text.
  - Have the recipient confirm the download and then delete the zipped files from the cloud storage system.