TeleSAFE IT Security Policy Development

Storage and Release of Clinical Photography

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

Purpose:

Clinical photographs taken as a component of the teleSAFE sexual assault medical forensic exam contain patient private health information and should be considered part of the medical record and stored, retained, and released in compliance with state and federal Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) regulations. A separate HIPAA-compliant release of information form must be completed for the release of patient photographs.

Policy Considerations:

- Clinical photographs taken as a component of the sexual assault medical forensic exam and part of the medical record should be provided the same privacy, security, and confidentiality requirements as every other document within the record. Because the state, federal, tribal, and territory criminal statutes of limitations vary, facilities may maintain records according to the jurisdictional statutes of limitations, rather than standard Health Information Management record retention policies.
- There are various products and processes available to secure, retain, and release clinical images. It is imperative that organizations research any second-and third-party vendors associated with clinical photography, and complete a thorough policy and risk review to ensure privacy and security measures meet state and federal HIPAA/HITECH requirements. Facilities should also require a Business Associate Agreement (BAA) with all vendors.
- Digital photos stored on portable media such as memory cards, external USB drives, on local hard drive storage of computer workstations and laptops, as well as in a clinical software program such as an Electronic Medical Record (EMR) system must be encrypted. Encryption is addressable according to HIPAA regulations [45 CFR 164.312(a)(2)(iv) and (E)(2)(ii)]. "Addressable" does not mean optional – an organization can choose to implement an encryption solution meeting the intent of the regulation without being prescriptive about which solution is implemented.
- Interdepartmental collaboration is required in the development of policies that address secure storage, retention, and release of photographs (e.g. IT Security, Compliance, Legal, HIM, Administration, and representation from the clinicians taking and storing the images).

TeleSAFE IT Security Policy Development

Storage and Release of Clinical Photography

- Release of these images to any party must follow all applicable disclosure of personal health information policies and procedures.
  A separate HIPAA-compliant release of information form must be completed for the release of patient photographs.
- It is strongly recommended that if patient digital images are being shared electronically for peer review, second opinion, or released to multidisciplinary team members, a process is in place to ensure the security and privacy of the image during transfer.
- Clinical photographs released per policy to multidisciplinary team members, such as law enforcement agencies or prosecutors for investigation are no longer covered by the privacy and security regulations of HIPAA/HITECH. It is strongly recommended that healthcare facilities engage multidisciplinary partners in an agreement to maintain patient PHI in compliance with privacy and security measures consistent with HIPAA requirements.