CURECAST

Checklist 1: US clinics using a clinical photo app

A. Before a device goes missing

- [ ] Choose one person to handle lost-device incidents and another person as backup.
- [ ] Keep a list of every phone, tablet and laptop used for patient photos. Record who uses each device.
- [ ] Make sure every device has a passcode, automatic screen lock and encryption (protection that makes stored information unreadable without the right access).
- [ ] Turn on Find My for iPhones or Find Hub for Android phones.
- [ ] Turn off personal cloud photo backup on devices used for patient photos.
- [ ] Print the first-hour instructions and put them in the staff room. Save a digital copy too.
- [ ] Check whether you have a signed Business Associate Agreement (BAA) with your clinical photo app provider. A BAA is a HIPAA-required agreement about how the provider protects patient information.
- [ ] Check whether your clinical photo app provides these five security features:
  - **End one device's session:** Sign out the missing device without affecting the staff member's other devices.
  - **Deactivate a staff account:** Stop a staff member's access when needed.
  - **Audit trail:** Record who viewed, downloaded or shared patient photos from lost device.
  - **Reauthentication:** Ask staff for their password or a code again after a period of inactivity. This stops someone from using a lost phone that is still signed in.
  - **Photo storage:** Save photos to the patient record instead of the phone's normal camera roll.
- [ ] Check whether an administrator can use these features directly or must contact the clinical photo app provider.

B. First hour: What to do when a device is lost

- [ ] Write down when your clinic found out the device was missing and who reported it.
- [ ] Use Find My or Find Hub to mark the device as lost and lock it remotely.
- [ ] Ask an administrator to end the missing device's active session in the clinical photo app.
- [ ] If the app cannot end one device's session, deactivate the staff account if that feature is available and appropriate. This may also stop access on the staff member's other devices.
- [ ] If the app has no admin panel or cannot block access, contact the clinical photo app provider immediately. Ask them to secure the account or device and confirm what they have done.
- [ ] If the device was stolen, report it to the police and save the report number.

- [ ] Decide whether to erase the device remotely using Find My or Find Hub. The command may not work until the phone connects to the internet. Erasing cannot be undone. Record when you sent the command.

C. Check which patient photos may have been exposed

- [ ] Ask an administrator to open the app's audit trail (a record of who viewed, downloaded or shared each photo) and filter it by that staff account and that device. Look at the time from before the device went missing until you ended its session. Save a copy as evidence, for example a download, a screenshot or a printout.
- [ ] Check which patient photos were viewed, downloaded or shared by the relevant account or device, where the app records this information.
- [ ] Look for unusual activity around the time the device went missing and afterward.
- [ ] Check whether the app saved patient photos to the phone's camera roll or other local folders.
- [ ] Ask whether the staff member also used the phone's normal camera, email or messaging apps for patient photos.
- [ ] List the patients whose photos may have been exposed.

Important: An audit trail may not show photos opened outside the clinical photo app, such as images already saved in the phone's gallery.

D. Decide whether the incident is a HIPAA breach

- [ ] Ask your IT support to confirm in writing whether the device had a passcode and encrypted storage. If you have no IT support, check your device records and account settings. Write down what you can confirm.
- [ ] If the patient information was encrypted according to HHS guidance (US Department of Health and Human Services rules), HIPAA breach notification may not be required. Still record what happened.
- [ ] Use what you found in section C. If the audit trail shows no access after the device went missing, you ended its session quickly, and you found no copies of patient photos on the phone, the chance of compromise may be low. In that case the incident may not be a reportable breach. Write down your reasons.
- [ ] If the audit trail shows access, or the phone may hold copies of patient photos, assess four things:
    1. What patient information was on the device?
    2. Who may have the device now?
    3. Did anyone access or view the information?
    4. What did your clinic do to reduce the risk?
- [ ] Write down your findings and whether the incident needs to be reported.

E. If the breach must be reported

- [ ] **Affected patients:** Tell them without unreasonable delay, and no later than 60 days after discovering the breach.
- [ ] **HHS, 500 or more affected people:** Report without unreasonable delay, and no later than 60 days after discovery.
- [ ] **HHS, fewer than 500 affected people:** Report within 60 days after the end of the calendar year in which the breach was discovered.
- [ ] **Local media:** If more than 500 residents of one state or jurisdiction are affected, tell prominent media outlets serving that area without unreasonable delay and within 60 days.
- [ ] Check your state's breach reporting laws. Some states have shorter deadlines.
- [ ] Tell affected patients what happened, what information was involved, what they can do, what your clinic is doing and how to contact you.

F. After the incident

- [ ] Save the audit trail, security records, incident report and details of every action taken.
- [ ] Keep the required HIPAA records for six years.
- [ ] Review what went wrong and make changes to prevent another incident.

Source: CureCast
https://dr.curecasthealth.com/

You are free to share or adapt this checklist for your own clinic rules. If you post it online, please add a link back to the source above. This checklist is general information about HIPAA and clinical photography. It is not legal advice, and state privacy and retention requirements vary. Check your own policies with your compliance lead or counsel.