Checklist 2: US clinics not 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.
- [ ] Turn on Find My for iPhones or Find Hub for Android phones.
- [ ] Turn off personal cloud photo backup on devices used for patient photos.
- [ ] Decide where staff must save patient photos and how those photos will be added to the correct patient record.
- [ ] Print the first-hour instructions and put them in the staff room. Save a digital copy too.

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 the staff member which patient photos they took using the phone's normal camera.
- [ ] Ask whether they sent patient photos by text, messaging app or email.
- [ ] 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. Find out which patient photos may have been exposed

- [ ] From another device, check clinic email and messaging apps for patient photos sent from the missing phone.
- [ ] Ask the staff member to check their iCloud Photos or Google Photos account from another device. Photos stored there may remain available after the phone is erased.
- [ ] Ask whether patient photos were saved in Downloads, Files or an SD card.
- [ ] Because the device is missing, treat any unconfirmed local copies as potentially still present.
- [ ] List the patients whose photos may have been on the device. Use staff recollections, photo dates and available records.

D. Decide whether the incident is a HIPAA breach

- [ ] Ask IT support team to confirm in writing whether the device had a passcode and encrypted storage. If you have no IT support, check your available device records and write down what you can confirm.
- [ ] If the patient information was encrypted according to HHS guidance, HIPAA breach notification may not be required. Record why.
- [ ] Assess these four factors:
  1. What patient information was involved?
  2. Who may have the device or information now?
  3. Was the information actually accessed or viewed?
  4. What did your clinic do to reduce the risk?
- [ ] Write down your findings and whether the incident must 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 your incident report, security records 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.