CURECAST

Checklist 1: UAE 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.
- [ ] Find out which health authority oversees your clinic, such as the Department of Health (DoH) in Abu Dhabi or the Dubai Health Authority (DHA) in Dubai.
- [ ] Save your health authority's contact details and reporting deadlines in your incident form.
- [ ] 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. UAE health data rules restrict storing or processing health information outside the country unless an exception or approval applies.
- [ ] Ask your clinical photo app provider where patient photos are stored, and get the answer in writing. The photos should be on servers inside the UAE, and so should any backup copies.
- [ ] 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.
- [ ] 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.
- [ ] **In Abu Dhabi:** Also record when your clinic first confirmed the incident, because this may affect the reporting deadline.
- [ ] 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 block access from the missing device, review account activity and confirm what action they have taken.
- [ ] 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 from the lost device.
- [ ] 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.
- [ ] If they used the phone's normal camera, ask the staff member to check their iCloud Photos or Google Photos account from another device. These services may store photos outside the UAE.
- [ ] 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 how serious the incident is

- [ ] 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.
- [ ] Use what you found in section C. Do not decide against reporting only because the audit trail shows no access. Ask your health authority first.
- [ ] Decide whether the incident is likely to put patients at high risk. Ask:
    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?

- [ ] Then follow the section for your emirate in section E.

E. Report to your health authority

If your clinic is in Abu Dhabi

- [ ] Contact the Abu Dhabi Health SOC, the DoH's health security team. Reporting deadlines may depend on how serious the incident is.
- [ ] Ask the DoH how to classify the lost-device incident. Report it as early as you can.
- [ ] If the incident involves your clinical photo app provider or its service, also inform the DoH promptly, as required by the applicable rules.
- [ ] If patient information was breached, submit the required Data Breach Form to the DoH within 72 hours after confirming the incident, under the DoH guidelines.
- [ ] Provide any additional information the DoH requires within 30 working days after the first report.
- [ ] Tell affected patients if the breach is likely to put them at high risk, following the applicable rules.

If your clinic is in Dubai

- [ ] Report the breach to the Dubai Health Authority (DHA) as required by its rules.
- [ ] If the incident involves NABIDH, Dubai's shared electronic health record system, check the requirement to notify NABIDH within 48 hours.
- [ ] Check whether a public notice is required within 30 days of discovering the breach.
- [ ] If your clinic is in Dubai Healthcare City, check whether additional health data rules apply.

If your clinic is in another emirate

- [ ] Contact your emirate's health regulator and confirm the incident reporting rules and deadlines.

F. After the incident

- [ ] Save the audit trail, security records, incident report and details of every action taken. Write down which security features were available and when each action was taken.
- [ ] Write down when your clinic discovered the loss, which patients may have been affected, who was notified and the reasons for your decisions, such as whether to tell patients.
- [ ] If you are in Abu Dhabi, keep the evidence for the required period. The DoH sample policy refers to at least one year.
- [ ] 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 UAE health data rules and clinical photography. It is not legal advice, and requirements vary by emirate and health authority. Check your own policies with your compliance lead or counsel.