CURECAST

Checklist 2: UAE 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.
- [ ] 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.
- [ ] Decide where staff must save patient photos and how those photos will be added to the correct patient record. Choose a place inside the UAE.
- [ ] 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 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. These services may store photos outside the UAE. Secure any patient photos found and arrange safe removal after preserving any evidence needed for the investigation.
- [ ] 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 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.
- [ ] You have no audit trail, so you cannot show that nobody opened the photos.
- [ ] 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 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 your incident report, security records and details of every action 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.