

Android Patient Photo Security Checklist for Clinics

Use this checklist before allowing staff to take patient photos.

- ☐ Choose an approved clinical photo app and sign a BAA where HIPAA requires one.
- ☐ Write down the clinic's rules for taking and storing patient photos.
- ☐ Set a strong screen lock on every phone.
- ☐ Turn on available theft protection features.
- ☐ Check that Find Hub is configured.
- ☐ Turn off unapproved Google Photos backup.
- ☐ Avoid SD cards for storing patient photos.
- ☐ Hide sensitive notification content on the lock screen.
- ☐ Give each staff member their own app login.
- ☐ Confirm that photos are saved to the correct patient record.
- ☐ Add a step for ending app access when a staff member leaves.
- ☐ Train staff on what to do if a photo is saved to the wrong place or a phone is lost.
- ☐ Keep records of training and follow your clinic's security procedures (see 45 CFR § 164.308(a)(5)).

Source: CureCast

<https://dr.curecasthealth.com/blog/hipaa-compliant-photos-android-phone/>

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.