CURECAST
CLINICAL PHOTO MANAGEMENT

Daily, Weekly and Yearly Checklist for Storing Clinical Photos

For clinics that use a clinical photo app

Daily

- [ ] Ask the patient for permission before taking the photo, and tell them how it will be used.
- [ ] Capture all clinical images through the app, not the phone's camera roll.
- [ ] Confirm each image is linked to the correct patient record before moving on.
- [ ] Check that each photo is tagged with what the patient agreed to: care, teaching or marketing.

Weekly

- [ ] Review the app's audit log for any access, downloads or shares that look unusual.
- [ ] Confirm no clinical images remain in staff phone camera rolls, text threads or personal cloud accounts.
- [ ] Check that clinical images are shared only through the app or another secure method, not by personal email, text message or chat apps.
- [ ] Check that new staff accounts have only the access their role needs.

Monthly

- [ ] Test that you can retrieve a specific patient's images from backup.
- [ ] Disable or remove access for staff who have changed roles or left the practice.
- [ ] Check that any patient who withdrew consent has been updated and tagged in the system.

Quarterly

- [ ] Audit a sample of patient records to confirm images have consent records that match signed forms.
- [ ] Review your app vendor's written agreement and confirm it is current and signed. It should say how they protect and use patient data.
- [ ] Confirm the vendor's security practices cover encryption, access controls, access logs and secure sending of data.
- [ ] Verify that automatic cloud backup on clinic devices is disabled or routed exclusively through the app.
- [ ] Make sure every staff member knows what to do if a device with access to clinical photos is lost or stolen: tell the clinic lead straight away, ask an administrator to sign the device out and remove its access (if you cannot do this, turn off that staff member's access instead), and write down what happened.

Annually

- [ ] Check all systems that store or send clinical images for security risks, and write down what you find and fix.
- [ ] Complete a full backup restoration test and document the result.
- [ ] Review and update your patient privacy notice if your clinical photography steps have changed.
- [ ] Confirm all staff with image access have completed privacy and security training in the past 12 months.
- [ ] Run a retention review: securely destroy images past your local retention period and log what was destroyed, the method, the date and the responsible person.
- [ ] Update your policies and procedures documentation to reflect any changes in software, devices or staff.

Important: *This checklist is a practical review aid. It is not legal advice, a certification or a guarantee that your clinic follows the law. Privacy rules differ by country and region, so check the rules where your clinic works and ask a qualified adviser when you need to.*

Source: CureCast
https://dr.curecasthealth.com/blog/checklist-storing-clinical-photos/

You are free to share this checklist. If you post it online, please add a link back to the source above.