CURECAST
CLINICAL PHOTO MANAGEMENT

Business Associate Agreement (BAA) Checklist for Patient Photos

- [ ] List every app and service that touches patient photos. Include camera apps, cloud backup, upload links and messaging tools.
- [ ] For each one, ask: does it store, receive or send photos for us?
- [ ] If yes, find the signed BAA. No BAA on file? Stop new uploads to that service today, then ask the vendor for one.
- [ ] Ask each vendor which subcontractors handle your photos and how quickly they would tell you about a breach. Write down the answers.
- [ ] Keep every signed BAA where your compliance lead can find it.
- [ ] Outside the US, get the local contract (the equivalent of a BAA) instead, such as a UK GDPR Article 28 processor contract.
- [ ] Review this list once a year and whenever you add a new app or service. You can do it as part of your HIPAA risk analysis, the clinic's review of where patient information could be at risk.
- [ ] Check each BAA against the 7 points above.

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/baa-for-photo-app/

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