TOOLKIT 17 · TELEMEDICINE · TOOL 3 OF 4

Telemedicine Platform — Data Protection Checklist

Twenty questions to ask before a platform carries a single consultation: encryption, storage, access, consent, breach, contract

Question	Yes	No
The platform		
End-to-end or transport encryption for video, audio and messages	☐	☐
Data at rest encrypted; storage location known (country) and compatible with the law	☐	☐
A written processor agreement with the provider covering confidentiality, sub-processors, deletion and breach notification	☐	☐
The provider does not use consultation data for its own purposes (advertising, training models)	☐	☐
Consumer messaging apps are not used for clinical consultations, images or records	☐	☐
Access		
Individual logins for every clinician; no shared accounts; two-factor authentication	☐	☐
Automatic logout; access removed the day a staff member leaves	☐	☐
Audit trail of who accessed which record, reviewed yearly	☐	☐
Recordings, if any, stored in the medical record system, not on the platform or a personal device	☐	☐
Patients		
Privacy notice explains what is collected, where stored, for how long, and rights (access, deletion)	☐	☐
Consent to the remote format and to any recording obtained and documented (Tool 1)	☐	☐
Patients told how to reach the service securely and what not to send by open email	☐	☐
Practice		
Clinicians consult from a private space; screens not visible to others; headphones	☐	☐
Personal devices, if used, are encrypted, passcoded and enrolled in the facility's device policy; no patient images in personal galleries	☐	☐
Consultation notes entered in the medical record within 24 hours	☐	☐
Breach process: reported to the data-protection lead within 24 h; to the authority within 72 h if required; patients informed if risk to them	☐	☐

Based on Regulation (EU) 2016/679 (GDPR), Articles 5, 28, 32–34, and the ASF Data Protection and IT & Data Security Policies.

ASF standards: Telemedicine Standard 5 — data protection (means of verification: completed checklist, processor agreement)