

HIPAA Compliance Checklist

MedSpaBinder

Clinic

Privacy / security official

Review date

HIPAA covers providers who bill health plans electronically. Many cash-only med spas aren't covered: check first.

Requirement	Done (Y / N)	Date	Owner	Evidence / where kept
Does HIPAA apply?				
Checked whether we're a covered entity (e.g. bill insurance)				
Privacy Rule				
Privacy official named				
Notice of privacy practices given and posted				
Policies for use and disclosure of patient info				
Patient access requests answered within 30 days				
Privacy complaint process in place and logged				
Staff trained on privacy (with dates)				
Sanctions policy for staff who break the rules				
Security Rule				
Security official named				
Security risk analysis done and updated				
Risk management plan for what it found				
Unique logins; access removed when staff leave				
Devices encrypted or safeguarded; screens locked				
Backups and a plan for outages				
Business associate agreements with vendors				
Breaches and records				
Breach response plan, including notification				
Policies and records kept 6 years				
Reviewed by (initials)				

Reviewed by: _____ Date: _____ Next review: _____