HIPAA_Data_Recovery_SOP

- HIPAA_Data_Recovery_Form
- HIPAA_Data_Recovery_SOP

HIPAA_Data_Recovery_Form

HIPAA Data Recovery Request & Chain of Custody Form

Instructions: Complete all sections. Store completed forms for 6 years per HIPAA retention.

Section 1: Request Details
- Request ID: _____
- Request Date/Time: _____
- Requestor Name/Title/Department: _____
- Contact Info (email/phone): _____
- Business Justification (clinical/operational impact): _____
  _____

Section 2: Data/System Identification
- System/Application Name: _____
- Environment (Prod/Test/Dev): _____
- Data Type(s) (ePHI, PII, other): _____
- Data Owner: _____
- Location (server/VM/endpoint/cloud service): _____
- Asset Tag / Hostname: _____

Section 3: Recovery Parameters
- Incident/Change Reference #: _____
- Desired Restore Point (timestamp/snapshot): _____
- RTO Target (hours): _____
- RPO Target (minutes/hours): _____
- Scope (entire system / database / folder / files): _____
- Dependencies (DB, services, keys, networking): _____

Section 4: Authorization
- Security/Privacy Officer Approval (name/sign/date): _____
- System Owner Approval (name/sign/date): _____

Section 5: Recovery Execution (to be completed by IT)
- Assigned Engineer: _____
- Start Date/Time: _____
- Source Media (backup set ID, snapshot ID): _____
- Hash/Integrity Verification (method/result): _____
- Steps Performed (summary):
  _____
  _____
  _____

- End Date/Time: _____
- Outcome (success/partial/failed): _____
- Data Validation Results (owner sign-off): _____

Section 6: Post-Recovery Actions
- Incident Record Updated (yes/no): _____
- Gaps/Issues Identified: _____
  _____
- Corrective Actions/Follow-ups: _____
  _____
- Runbooks Updated (yes/no/date): _____

Chain of Custody (if physical media used)
- Media ID: _____
- Description: _____
- Custodian Transfer Log (name, date/time, from/to, signature):

Date/Time	From	To	Signature	Notes

HIPAA_Data_Recovery_SOP

HIPAA Data Recovery SOP (Printable Checklist)

Purpose: Ensure compliant, timely restoration of ePHI systems (HIPAA 45 CFR §164.308(a)(7)).

Section A: Triage & Authorization
[ ] Validate incident/change request and business impact.
[ ] Confirm data classification and owner; obtain approvals.

Section B: Identify Scope & Restore Point
[ ] Confirm system, dataset, dependencies, and desired timestamp.
[ ] Select backup/snapshot meeting RPO; verify media availability.

Section C: Prepare Environment
[ ] Isolate affected systems if incident-related (malware/ransomware).
[ ] Gather credentials/keys; ensure network and target capacity.

Section D: Execute Recovery
[ ] Follow runbook for system/db/file restore.
[ ] Track actions, timestamps, backup IDs.

Section E: Integrity Validation
[ ] Verify file/system integrity (hashes, DB consistency, app checks).
[ ] Obtain owner validation/sign-off.

Section F: Return to Service
[ ] Reconnect to production networks; monitor performance and logs.
[ ] Validate access controls and audit logging.

Section G: Documentation & Lessons Learned
[ ] Complete Data Recovery Form and attach artifacts (hashes, logs).
[ ] Update runbooks; record corrective actions and test plans.

Sign-Off
- Performed By (print/sign/date): _____
- Owner Validation (print/sign/date): _____
- Security/Privacy Review (print/sign/date): _____

Records: Retain forms, logs, approvals for 6 years.