

Willow Creek Family Clinic

HIPAA Security Policy and Operating Procedures

Document WCFC-SEC-001 | Version 1.0 | Effective October 6, 2026

1. Organization, ownership, and scope

Willow Creek Family Clinic is a fictional outpatient healthcare practice in Illinois. It provides primary care, preventive visits, and follow-up care. The clinic submits standard electronic healthcare claims and conducts electronic eligibility transactions. For this scenario, the clinic is a HIPAA covered entity and its policy addresses the HIPAA Security Rule, 45 CFR Part 164, Subpart C. The clinic operates only in the United States.

The clinic creates, receives, maintains, and transmits electronic protected health information (ePHI) through its electronic health record, patient portal, electronic prescribing workflow, laboratory interface, and claims clearinghouse. Patient records, appointment histories, clinical notes, and referral messages are within the policy scope. Paper records are handled under a companion privacy procedure; the electronic security controls here apply to ePHI.

The Clinic Administrator is the designated Security Official. The Privacy Officer reviews permitted uses, disclosures, and possible breach notices. Department supervisors approve job-based access. Technical staff operate accounts, backups, logging, and device controls. Each role is assigned to a position rather than an unnamed group. The governing partners approved this fictional policy on October 6, 2026; policy approval does not close the outstanding implementation issues described below.

This document contains policy descriptions and fictional operational facts only. It includes no patient names, birth dates, medical record numbers, diagnoses tied to people, account credentials, or actual clinical records. It is an evaluation fixture, not an operational policy adopted by a real clinic.

2. System inventory and risk analysis

The Security Official maintains an inventory covering the hosted electronic health record, patient portal, claims interface, laboratory messaging, staff laptops, front-desk workstations, network equipment, removable media, and encrypted backups. Each entry identifies its business owner, system location, data flows, access groups, and recovery dependency. Technical staff update entries before a new application enters service and within five business days after a material change.

The annual risk analysis considers potential threats to the confidentiality, integrity, and availability of ePHI. Reviewers record threat likelihood, operational impact, existing controls, residual risk, an action owner, and the target date for each corrective action. The Security Official reviews the risk register with the governing partners each quarter. A changed vendor connection or serious security event triggers an additional review rather than waiting for the calendar review.

The September 2026 assessment reviewed the electronic health record, portal, and office network. It did not include two older examination-room laptops or removable drives used for document transfers. The inventory lists those devices, but no threat assessment or corrective-action decision covers their use. Their risks remain open; the completed assessment for the other systems does not resolve this omission.

Before approving a corrective action as closed, the Security Official must attach the configuration record, test result, or other supporting evidence and record who verified it. An invoice or a statement that a product supports a safeguard is insufficient to establish that the clinic enabled and checked the safeguard. Relevant policy topic: 45 CFR 164.308(a)(1).

3. Workforce access and training

Supervisors request access through a documented ticket identifying the employee role, required patient-record functions, and requested start date. The Security Official approves the access group, and technical staff create a unique account. Front-desk staff receive scheduling functions; clinicians receive treatment functions appropriate to their assignments; billing staff receive claim-processing functions. Shared clinical accounts are prohibited. Access reviews occur quarterly, with unnecessary permissions removed and the decision retained.

Technical staff disable a departing employee account by the end of the final work shift and revoke portal, remote-access, and vendor-console sessions. The supervisor submits the departure ticket before the final shift whenever possible. A role change requires a new approval; inherited access is reviewed at the same time. Emergency access uses a named emergency account, a recorded reason, and review by the Security Official on the next business day.

Clinic policy requires security orientation before routine access to ePHI and a yearly refresher covering phishing, screen locking, incident reporting, and acceptable handling of patient records. New employees currently receive verbal instruction from their supervisor. The clinic has no attendance register, recorded completion acknowledgments, or retained training materials for the September intake group. A proposed electronic training register has not been implemented; no evidence establishes that every workforce member completed the required instruction.

Supervisors report policy violations to the Clinic Administrator, who records investigation outcomes and any disciplinary action under the personnel procedure. The access ticket, quarterly review, and departure record are retained in the security evidence library. Policy topics include workforce security, authorization, and security awareness under 45 CFR 164.308(a)(3)-(5).

4. Workstations, authentication, and audit records

Each managed workstation requires a named account and locks after five minutes without activity. Remote access and privileged administration require multi-factor authentication under clinic policy. Technical staff verify these settings at enrollment and after a security-related configuration change. Device compliance reports identify machines missing the approved configuration; a nonconforming device cannot reconnect to clinical systems until the issue is resolved or a documented temporary decision is approved.

Clinic policy requires encryption on managed laptops and approved transport protection for electronic health record, portal, and vendor connections. Configuration records identify the system, enabled settings, verification date, and owner. The clinic chooses these technical measures as part of its own risk-management process; this fictional procedure does not present every chosen technology as a universal statutory requirement. Requests for an alternate measure must explain the risk and the proposed safeguard before approval.

The electronic health record logs authentication events, patient-record access, exports, permission changes, and administrator actions. Technical staff check collection health daily. The Security Official reviews suspicious access alerts each business day and performs a monthly sample review of privileged actions and bulk exports. Each review records the time window, reviewer, investigated events, disposition, and follow-up ticket. Log access is restricted to authorized reviewers, and changes to collection settings are recorded.

Visitors sign in at reception and remain escorted in work areas. Examination-room screens face away from public waiting areas. Network equipment is kept in a locked cabinet with an access register. Technical staff inspect locking and screen placement during quarterly walkthroughs. Evidence includes enrollment reports, access-log reviews, and walkthrough records. Policy topics: 45 CFR 164.310 and 164.312.

5. Business associates and information exchanges

The Privacy Officer maintains a register of organizations that create, receive, maintain, or transmit ePHI on the clinic's behalf. Each entry identifies the service, exchanged information, approved connection, contract owner, and review date. The electronic health record host, claims clearinghouse, portal operator, and backup operator are listed. A business associate agreement and security review are required by clinic procedure before an approved service begins handling ePHI.

The contract review records safeguards, incident reporting arrangements, restrictions on use, subcontractor responsibilities, and the return or destruction arrangements at service termination. The Privacy Officer keeps the signed agreement and checks the register quarterly for expired or missing documents. Technical staff confirm the connection matches the approved data flow and document any material change before enabling it.

One laboratory-message relay is already in use. Its service contract is signed, but the business associate agreement remains an unsigned draft. The relay handles ePHI for the clinic and is listed as a business associate in the register. A future plan to obtain a signature does not supply an executed agreement. The Privacy Officer has not documented a corrective-action deadline, temporary restriction, or authorized resolution. This issue remains open.

At contract termination, the contract owner coordinates removal of accounts and interfaces and obtains written confirmation of the agreed data disposition. Where destruction is not feasible, the contract owner escalates the remaining obligations to the Privacy Officer for documented handling. The evidence library keeps the register, approved exchanges, signed agreements, access removal tickets, and termination confirmations. Policy topics: 45 CFR 164.308(b) and 164.314(a).

6. Security incidents and breach review

Workforce members report suspected inappropriate access, lost devices, malware, or exposed patient records immediately to the Security Official. The service desk records the report time, reporter role, affected system, observed facts, and urgent patient-care impact. Staff must avoid copying clinical content into a general support ticket. An incident identifier connects the ticket to a restricted evidence record.

The Security Official leads the incident response team and assigns containment, evidence preservation, and recovery tasks. Technical staff isolate an affected account or device when appropriate, preserve logs, and document every action. The Privacy Officer separately evaluates whether an impermissible use or disclosure occurred, the information involved, who received it, whether access actually occurred, and the effectiveness of mitigation. The record includes the decision and supporting facts.

Before an incident is closed, the Privacy Officer documents whether individual, HHS, or other notices are required under the applicable notification rules. For this fictional clinic, legal review must identify the applicable deadline and an accountable sender in the incident record; an internal escalation target is not treated as the legal notification deadline. Notification language and recipient lists require approval before release. If review concludes that notice is unnecessary, the reasons and supporting assessment must be retained.

The Security Official conducts a lessons-learned review within ten business days after operational recovery. The team assigns corrective actions, updates relevant procedures, and records verification of the actions. The incident evidence index includes the initial report, investigation timeline, containment approvals, notification decision, recovery test, and review record. Security incident procedures and breach notification are distinct topics: 45 CFR 164.308(a)(6) and Part 164, Subpart D.

7. Backup, emergency operation, and disposal

Technical staff run encrypted backups of the clinic-managed ePHI repository every night. They review job completion each morning, open a ticket for failed jobs, and retain the completion report. Backup access uses a separate administrative group. The inventory records the protected data, backup destination, approved retention setting, restore dependencies, and the staff authorized to begin recovery.

The emergency-mode procedure directs the Clinic Administrator to declare an outage, assign a clinical coordinator, and decide which appointments can safely continue. Staff use approved downtime forms kept in a secured cabinet. When the electronic health record is restored, authorized staff reconcile the downtime entries and document the reconciliation review. The outage record includes decisions, start and recovery times, and unresolved operational issues.

The vendor dashboard shows successful backup jobs, but the clinic has never carried out or documented a restore exercise. No record shows that an authorized employee recovered a sample data set, checked its readability, or tested the downtime reconciliation procedure. The proposed first exercise is not scheduled and has no assigned owner. Successful backup messages do not establish tested recovery capability; the testing and revision decisions remain undocumented.

Before a device leaves clinic control, technical staff record its asset identifier and verify approved sanitization or physical destruction. The Security Official checks the disposition record before authorizing pickup. The record states who performed and verified the work, when it occurred, and the disposition method. A general deletion command alone is not accepted as proof of sanitization under this clinic procedure. Records under an active legal hold are excluded from routine disposal pending documented release. Policy topics: 45 CFR 164.308(a)(7) and 164.310(d).

8. Review, evidence, and change control

The Clinic Administrator maintains the controlled policy copy and makes the current version available to workforce members responsible for its procedures. Each revision records the author role, approval date, change description, and superseded version. An annual review is scheduled for October, and an additional review follows material system changes, a serious incident, or a change in the services used to handle ePHI.

The Security Official performs a periodic technical and nontechnical evaluation and records the scope, methods, findings, owners, and closure decisions. Evaluations must consider the examination-room devices omitted from the September review. A plan to purchase a new service or an unsigned vendor proposal is recorded as a proposal; it does not count as an enabled control or completed corrective action.

The evidence library keeps policy versions and documentation of required security actions for six years after creation or the last date in effect, whichever is later. This security-documentation rule is separate from the clinic's medical-record retention schedule and does not set a blanket six-year retention period for patient records. The Records Coordinator applies the separate approved schedule and legal holds to clinical records.

At this revision, the governing partners have approved the policy wording, but four implementation issues remain open: the incomplete risk-analysis scope, missing workforce training records, the unsigned laboratory-relay agreement, and untested recovery procedures. Each needs an accountable owner, corrective-action date, and verification evidence. Acknowledgment of an open issue does not resolve it. Policy topics: 45 CFR 164.308(a)(8) and 164.316.

Reference materials checked October 6, 2026: HHS Summary of the HIPAA Security Rule; HHS Guidance on Risk Analysis; HHS Breach Notification Rule. The references guide the scenario topics. The clinic, decisions, intervals, approvals, vendors, and implementation facts are entirely fictional. This sample does not incorporate proposed rule changes as adopted requirements.