

GOVERNANCE DOCS

HIPAA Security, Privacy and Breach Notification Rules

Gap Assessment Report

HIPAA Security, Privacy and Breach Notification Rules (45 CFR Parts 160 and 164)

Oakridge Family Clinics (sample)

Electronic protected health information across six clinics, the patient portal and the billing service.

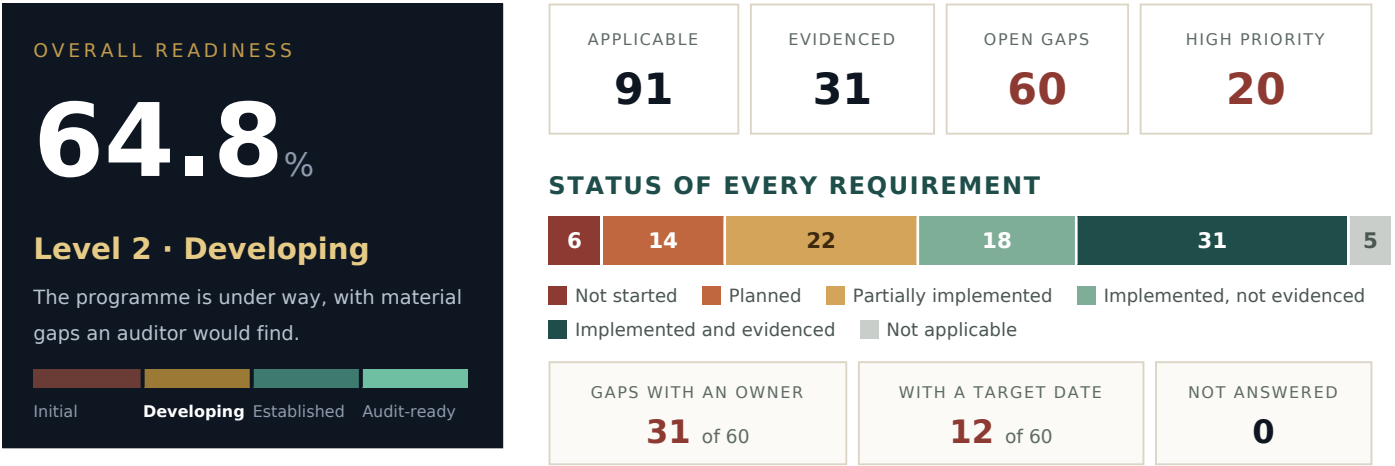
ASSESSED	25 September 2026
EDITION	45 CFR Parts 160 and 164
IN SCOPE	96 requirements, 91 applicable
PROFILE	Healthcare and life sciences · 50 to 249 people · HHS Office for Civil Rights
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Oakridge Family Clinics (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Oakridge Family Clinics (sample) stands against HIPAA



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 64.8% against HIPAA across 91 applicable controls. 31 of them are implemented and evidenced.
- Most open gaps: Administrative safeguards, with 11 at 76%. Strongest area: Privacy Rule - administrative requirements at 85%.
- 18 controls are operating but not evidenced. Collecting their records alone lifts the score to 69.8% (+5.0 points), the cheapest gain available.
- 20 gaps are high priority (not started or only planned); 6 of them are in Technical safeguards.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 6 high-priority gaps in Technical safeguards	HR Manager	HIPAA Access Control Policy
2	MEDIUM	Adopt and tailor the HIPAA Security Policies and Procedures, which closes 6 open gaps	To assign	HIPAA Security Policies and Procedures
3	LOW	Evidence the 18 controls that already operate (+5.0 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

At 64.8% readiness, the organization must resolve 20 high priority gaps, starting with core technical safeguards.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

The organization stands at a Developing readiness level of 64.8% under HIPAA requirements, with 60 open gaps remaining. Our primary exposure lies in Technical safeguards at 25%, where critical controls for user identification, authentication, and transmission security have not started. Furthermore, only 12 gaps currently have committed target dates. Leadership must approve clear operational ownership across departments, resource remediation for technical safeguard gaps, and mandate target completion dates across all 20 high priority items immediately.

WHERE YOU STAND

The self-assessment places the organization at readiness level 2 of 4, named Developing, with an overall score of 64.8% across 91 applicable requirements. Out of 96 total requirements, the software identified 60 open gaps, including 20 high priority gaps. While 31 requirements are implemented and evidenced, another 18 are implemented without evidence, and 6 have not started. Only 31 gaps have an assigned owner and just 12 carry target completion dates.

WHAT IT MEANS FOR THE ORGANIZATION

The pattern shows uneven maturity across security and privacy disciplines. While Privacy Rule administrative requirements reached 85%, Technical safeguards scored lowest at 25% with 9 open gaps, and Privacy Rule individual rights reached 29.2% with 6 open gaps. These gaps directly matter to HHS Office for Civil Rights expectations in general terms. Leaving technical controls unstarted while many operational tasks lack assigned dates creates unmanaged operational friction during official regulatory scrutiny.

WHERE TO FOCUS FIRST

The immediate focus belongs on missing technical access and authentication controls, followed by individual privacy rights procedures. Beginning work on technical safeguards will address items currently marked as not started. Evidencing the 18 controls that already run will raise the score to 69.8%, while finishing partly implemented controls lifts it to 81.9%. Assigning accountable owners and target dates to all 60 open gaps will ensure sustained progress across both rules.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Establish Unique User Identification and Entity Authentication Controls 164.312(a)(2)(i) Unique user identification (required) · 164.312(d) Person or entity authentication (required)	Missing user identification and authentication controls leaves systems vulnerable to unauthorized access and compromises core technical safeguards. Addressing these closes high priority gaps that matter directly to supervisory scrutiny.	Draft user identification standards using the HIPAA Access Control Policy.	HIPAA Access Control Policy HIPAA Toolkit - Comprehensive 160+ Templates	30 DAYS
2 Implement Transmission Encryption and Network Integrity Safeguards 164.312(e)(2)(ii) Transmission encryption (addressable) · 164.312(e)(2)(i) Transmission integrity controls (addressable)	Unprotected transmissions expose electronic protected health information to interception and data corruption. Securing network pathways remediates critical deficiencies in technical safeguard requirements.	Review current transmission mechanisms against the HIPAA Compliant Encryption Policy.	HIPAA Compliant Encryption Policy HIPAA Toolkit - Comprehensive 160+ Templates	30 DAYS
3 Deploy Restriction Request and Confidential Communication Procedures 164.522(a) Right to request restrictions · 164.522(b) Confidential communications	Individual rights scored 29.2% with 6 open gaps, creating exposure to patient rights non-compliance. Establishing formal intake processes ensures patient restriction requests receive legally required handling.	Adopt the PHI Restriction Request Form for workforce use.	PHI Restriction Request Form HIPAA Toolkit - Comprehensive 160+ Templates	60 DAYS
4 Compile ePHI and Designated Record Sets Inventories SC.3 ePHI inventory · SC.4 Designated record sets	Scope and applicability scored 50% due to incomplete data maps across systems. Comprehensive inventories provide the baseline needed to protect health information across every repository.	Populate the ePHI System and Equipment Asset Inventory across primary departmental databases.	ePHI System and Equipment Asset Inventory HIPAA Toolkit - Comprehensive 160+ Templates	60 DAYS
5 Formalize Data Backup Plans and Breach Burden of Proof 164.308(a)(7)(ii)(A) Data backup plan (required) · 164.414 Burden of proof	Failing to document backup procedures and breach evaluation records prevents the organization from meeting regulatory burden of proof obligations. Formal records verify operational resilience during review.	Log recent recovery tests under the HIPAA Backup Data Recovery Policy.	HIPAA Backup Data Recovery Policy HIPAA Toolkit - Comprehensive 160+ Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Enforce unique user identification rules using the HIPAA Access Control Policy.
- Configure entity authentication mechanisms using the Password and Authentication Policy.
- Review transmission encryption standards alongside the Confidential Communication and PHI Transmission Security Policy.
- Assign accountable owners and target completion dates to all 20 high priority gaps.

DAYS 31 TO 60

- Roll out the PHI Restriction Request Form and confidential communications procedures.
- Complete the ePHI System and Equipment Asset Inventory across all systems.
- Document designated record sets within the HIPAA Designated Record Sets Inventory.
- Collate operational proof for the 18 requirements implemented without evidence.

DAYS 61 TO 90

- Validate the data backup plan against the HIPAA Backup Data Recovery Policy.
- Establish incident assessment documentation using the HIPAA Breach Notification Incident Log.
- Complete implementation across the 22 partially implemented requirements to reach 81.9% readiness.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and applicability	2 2 1	50%	2 2 0
Security Rule - general rules	1 2	58%	1 0 2
Administrative safeguards	2 6 3 11	76%	2 6 3
Physical safeguards	2 2 2 3	67%	2 2 2
Technical safeguards	4 2 2 1	25%	6 2 1
Organizational requirements and documentation	2 4 2	69%	2 0 4
Privacy Rule - uses and disclosures	5 2 3	70%	0 5 2
Privacy Rule - individual rights	2 2 1 1	29%	4 1 1
Privacy Rule - administrative requirements	3 7	85%	0 3 0
Breach notification	3 4	78%	1 1 3

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		64.8%
Evidence what already runs 18 requirements		69.8% +5.0
Finish what is partly in place 22 requirements		81.9% +12.1
Implement what is planned 14 requirements		93.4% +11.5
Start what has not begun 6 requirements		100.0% +6.6

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

HIPAA Security Policies and Procedures		6
HIPAA Access Control Policy		4
HIPAA Backup Data Recovery Policy		4
Master Document Register		4
Confidential Communication and PHI Transmission Security Policy		3
HIPAA Business Associate Agreement		3

All of these are in the HIPAA Toolkit (165 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 6

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
164.312(a)(2)(i)	Unique user identification (required)	Technical safeguards	Operations Manager 4 Feb 2027	HIPAA Access Control Policy · User Access Management Process
164.312(c)(2)	Mechanism to authenticate ePHI (addressable)	Technical safeguards	HR Manager 10 Dec 2026	HIPAA Security Policies and Procedures · HIPAA Backup Data Recovery Policy
164.312(d)	Person or entity authentication (required)	Technical safeguards	To assign	Password and Authentication Policy · Password Authentication Controls Reference
164.312(e)(2)(ii)	Transmission encryption (addressable)	Technical safeguards	To assign	Confidential Communication and PHI Transmission Security Policy · HIPAA Compliant Encryption Policy
164.522(a)	Right to request restrictions	Privacy Rule - individual rights	HR Manager	PHI Restriction Request Form · PHI Access Restriction and Use Limitation Policy +1 more
164.522(b)	Confidential communications	Privacy Rule - individual rights	IT Manager	Confidential Communication and PHI Transmission Security Policy

HIGH Planned · 14

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
SC.3	ePHI inventory	Scope and applicability	Risk Manager	ePHI System and Equipment Asset Inventory · Software and Hardware Asset Management Policy

SC.4	Designated record sets	Scope and applicability	To assign	HIPAA Designated Record Sets Inventory
164.306(b)	Flexibility of approach	Security Rule - general rules	To assign	HIPAA Security Risk Assessment · HIPAA Security Compliance Reference Guide
164.308(a)(4)(ii)(C)	Access establishment and modification (addressable)	Administrative safeguards	Compliance Lead	User Access Management Process · HIPAA ePHI System Access Request Form
164.308(a)(7)(ii)(A)	Data backup plan (required)	Administrative safeguards	HR Manager 7 Jan 2027	HIPAA Backup Data Recovery Policy
164.310(a)(2)(iii)	Access control and validation (addressable)	Physical safeguards	To assign	Guidelines for Working in Secure Areas HIPAA · HIPAA Privacy Security Office Walkthrough
164.310(d)(2)(iii)	Accountability for media (addressable)	Physical safeguards	Risk Manager 21 Jan 2027	Media Transit Log · HIPAA Media Transit Form +1 more
164.312(b)	Audit controls (required)	Technical safeguards	Compliance Lead	HIPAA Security Event Logging and Monitoring Policy · IT Systems Monitoring Procedure
164.312(e)(2)(i)	Transmission integrity controls (addressable)	Technical safeguards	To assign	Confidential Communication and PHI Transmission Security Policy · Network Security Policy HIPAA
164.314(b)	Group health plan requirements	Organizational requirements and documentation	Operations Manager	HIPAA Legal Responsibilities Policy · Legal Regulatory Requirements Procedure HIPAA
164.316(b)(2)(i)	Six year retention	Organizational requirements and documentation	IT Manager 10 Dec 2026	Records Retention and Protection Policy · Master Document Register

164.526	Right to amendment	Privacy Rule - individual rights	Risk Manager 29 Oct 2026	Health Record Amendment Policy and Procedure · PHI Amendment Request Form +1 more
164.528	Accounting of disclosures	Privacy Rule - individual rights	Compliance Lead	HIPAA Accounting of Disclosures Policy · Accounting of Disclosures Request and Response Procedure +1 more
164.414	Burden of proof	Breach notification	Operations Manager 7 Jan 2027	HIPAA Breach Notification Incident Log · HIPAA Breach Risk Assessment Form +1 more

MEDIUM Partially implemented · 22

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
SC.1	Covered entity or business associate	Scope and applicability	Operations Manager	HIPAA Initial Compliance Assessment · HIPAA PreAssessment Checklist
SC.5	Security and privacy officials	Scope and applicability	Compliance Lead	HIPAA Designation of Privacy Official · HIPAA Security Officer Role Charter and Job Description +1 more
164.308(a)(1)(ii)(B)	Risk management (required)	Administrative safeguards	IT Manager	HIPAA Security Risk Assessment Policy · HIPAA Initial Compliance Assessment
164.308(a)(1)(ii)(D)	Information system activity review (required)	Administrative safeguards	Operations Manager	HIPAA Security Event Logging and Monitoring Policy · IT Systems Monitoring Procedure
164.308(a)(3)(ii)(C)	Termination procedures (addressable)	Administrative safeguards	IT Manager	HIPAA Employee Termination Checklist · HIPAA Workforce Exit Interview and Termination Checklist

164.308(a)(4)(ii)(A)	Isolating clearinghouse functions (required)	Administrative safeguards	Risk Manager 10 Dec 2026	HIPAA Access Control Policy · Segregation of Duties Guidelines for ePHI Systems
164.308(a)(7)(ii)(B)	Disaster recovery plan (required)	Administrative safeguards	HR Manager 21 Jan 2027	HIPAA Backup Data Recovery Policy · HIPAA Business Continuity Plan
164.308(a)(8)	Evaluation (required)	Administrative safeguards	HR Manager	HIPAA Security Assessment Tool · HIPAA Security Assessment Checklist Small Office
164.310(c)	Workstation security (required)	Physical safeguards	Risk Manager 21 Jan 2027	Physical Security Policy HIPAA · HIPAA Privacy Security Office Walkthrough
164.310(d)(2)(i)	Media disposal (required)	Physical safeguards	Operations Manager	HIPAA PHI Destruction and Media Disposal Policy · HIPAA Certificate of PHI Destruction +1 more
164.312(a)(2)(iii)	Automatic logoff (addressable)	Technical safeguards	HR Manager 12 Nov 2026	HIPAA Access Control Policy · HIPAA Acceptable Use Policy
164.312(a)(2)(iv)	Encryption and decryption at rest (addressable)	Technical safeguards	Compliance Lead	HIPAA Compliant Encryption Policy · HIPAA Cryptographic Controls Policy
164.502(b)	Minimum necessary	Privacy Rule - uses and disclosures	Compliance Lead	Minimum Necessary Use and Disclosure Policy · PHI Access Restriction and Use Limitation Policy
164.506	Treatment, payment and health care operations	Privacy Rule - uses and disclosures	To assign	HIPAA Security Policies and Procedures · Minimum Necessary Use and Disclosure Policy
164.512	Disclosures not requiring authorization	Privacy Rule - uses and disclosures	HR Manager	Routine PHI Disclosures and Requests Register · HIPAA Legal Responsibilities Policy

164.514(f)	Fundraising	Privacy Rule - uses and disclosures	To assign	HIPAA Notice of Privacy Practices · Minimum Necessary Use and Disclosure Policy
164.514(h)	Verification of identity and authority	Privacy Rule - uses and disclosures	To assign	Patient Right of Access Policy and Procedure · HIPAA Security Policies and Procedures
164.524	Right of access	Privacy Rule - individual rights	Compliance Lead 29 Oct 2026	Patient Right of Access Policy and Procedure · Patient Request for Access to PHI Form
164.530(e)	Sanctions	Privacy Rule - administrative requirements	To assign	HIPAA Workforce Disciplinary and Sanctions Policy
164.530(f)	Mitigation	Privacy Rule - administrative requirements	To assign	HIPAA Incident Response Procedure · HIPAA Security Incident Response and Breach Assessment Report
164.530(i)	Privacy policies and procedures	Privacy Rule - administrative requirements	Operations Manager	HIPAA Security Policies and Procedures · Master Document Register
164.410	Business associate notification	Breach notification	HR Manager	HIPAA Business Associate Agreement · HIPAA Incident Response Procedure

LOW Implemented, not evidenced · 18

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
164.306(a)	General security standards	Security Rule - general rules	To assign	HIPAA Security Policy Manual · HIPAA Security Policies and Procedures
164.306(d)	Addressable implementation specifications	Security Rule - general rules	To assign	HIPAA Security Risk Assessment Policy · HIPAA Security Rule Compliance Matrix
164.308(a)(5)(ii)(B)	Protection from malicious software (addressable)	Administrative safeguards	To assign	HIPAA Anti Malware Policy · HIPAA Anti Virus Security Guidelines

164.308(a)(7)(ii)(D)	Testing and revision procedures (addressable)	Administrative safeguards	To assign	HIPAA BCP Testing and Exercise Plan · HIPAA Business Continuity Test Report
164.308(a)(7)(ii)(E)	Applications and data criticality analysis (addressable)	Administrative safeguards	To assign	HIPAA Business Impact Analysis Process · HIPAA Capacity Plan
164.310(d)(2)(ii)	Media re-use (required)	Physical safeguards	To assign	Media Disposal Sanitization Procedure · Secure Information Deletion Policy
164.310(d)(2)(iv)	Data backup and storage (addressable)	Physical safeguards	To assign	HIPAA Backup Data Recovery Policy · Physical Media Transfer Procedure
164.312(a)(2)(ii)	Emergency access procedure (required)	Technical safeguards	To assign	HIPAA Access Control Policy · HIPAA Contingency Plan
164.314(a)(2)(ii)	Other arrangements	Organizational requirements and documentation	To assign	HIPAA ASP Engagement Policy · Third Party Network Connection Agreement
164.314(a)(2)(iii)	Subcontractor agreements	Organizational requirements and documentation	To assign	HIPAA Business Associate Agreement · Supplier Information Security Agreement
164.316(b)(2)(ii)	Availability of documentation	Organizational requirements and documentation	To assign	Master Document Register · HIPAA Security Policy Manual
164.316(b)(2)(iii)	Updating documentation	Organizational requirements and documentation	To assign	Master Document Register · HIPAA Security Policies and Procedures
164.502(e)	Disclosures to business associates	Privacy Rule - uses and disclosures	To assign	HIPAA Business Associate Agreement · Business Associate Agreement
164.514(a)	De-identification	Privacy Rule - uses and disclosures	To assign	HIPAA Data Masking Policy · Data Access and Classification Policy

164.520	Notice of privacy practices	Privacy Rule - individual rights	To assign	HIPAA Notice of Privacy Practices · NPP Distribution and Acknowledgement Policy +1 more
164.404(a)	Discovery of a breach	Breach notification	To assign	HIPAA Incident Response Procedure · HIPAA Breach Notification Incident Log
164.404(b)	Sixty day notification to individuals	Breach notification	To assign	HIPAA Privacy Breach Notification Policies and Procedures
164.408	Notification to the Secretary	Breach notification	To assign	HIPAA Breach Notification Incident Log

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com