

ODA3 INSTITUTE

CROSSWALK

GAISSF™–HIPAA Mapping

AI Security, Privacy and Evidence Crosswalk — 45 CFR Parts 160 and 164

GAISSF-CRO-035 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 6 October 2026

© 2026 ODA3 Pvt Ltd

Executive Summary

This crosswalk maps all 59 GAISSF™ v1.0 controls to selected operationally material provisions of the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules. The GAISSF Applicable-Control Baseline is all 52 controls in D1-D8 plus D9 where Physical AI or cyber-physical actuation is in scope. The package contains 163 forward mapping records and a reverse coverage register for 39 HIPAA provisions.

The mapping supports gap analysis and evidence-reuse analysis. It does not determine whether an organization is a covered entity or business associate, whether information is PHI or ePHI, whether a use or disclosure is permitted, whether a breach-notification duty has been triggered, or whether HIPAA compliance has been achieved. Mapping does not establish equivalence, evidence sufficiency, operating effectiveness, HHS endorsement, legal compliance, or automatic GAISSF conformance.

1. Source Baseline

- GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 v1.0; 59 controls / 9 domains; Applicable-Control Baseline = 52 D1-D8 + applicable D9.
- 45 CFR Parts 160 and 164 remain the binding HIPAA regulatory baseline. HHS states that the current Security Rule remains in effect while the 2024 Security Rule NPRM is pending. The 2024 reproductive-health Privacy Rule was largely vacated by a federal district court on 18 June 2025; remaining Notice of Privacy Practices modifications remain in effect with a 16 February 2026 compliance date.
- HHS Office for Civil Rights (OCR) guidance is informative and subordinate to the regulations and applicable court orders.
- The 2024 HIPAA Security Rule modernization remains a proposed rule and is excluded from the normative mapping; the current Security Rule remains in effect.

2. Methodology

Mappings compare control outcomes, scope, evidence, responsible actors, and operating effect. Relationship codes are SP (strong partial), P (partial), S (supporting), C (contextual), N (no material mapping), O (outside scope), and U (unable to determine). No mapping is legal equivalence, evidence sufficiency, or automatic compliance.

3. Rule-Level Coverage

HIPAA provision	Title	Rule group	Mapped GAISSF controls	Coverage
160.103	Definitions	General Provisions	0	Not Addressed
160.203	General rule and exceptions	Preemption	0	Not Addressed
164.105	Organizational requirements	General Requirements	0	Not Addressed
164.306	Security standards: general rules	Security Rule	0	Not Addressed
164.308(a)(1)	Security management process	Administrative Safeguards	24	Partially Addressed
164.308(a)(2)	Assigned security responsibility	Administrative Safeguards	7	Partially Addressed
164.308(a)(3)	Workforce security	Administrative Safeguards	6	Partially Addressed
164.308(a)(4)	Information access management	Administrative Safeguards	0	Not Addressed
164.308(a)(5)	Security awareness and training	Administrative Safeguards	3	Partially Addressed
164.308(a)(6)	Security incident procedures	Administrative Safeguards	10	Partially Addressed
164.308(a)(7)	Contingency plan	Administrative Safeguards	1	Partially Addressed
164.308(a)(8)	Evaluation	Administrative Safeguards	3	Partially Addressed
164.308(b)	Business associate contracts and arrangements	Administrative Safeguards	8	Partially Addressed
164.310(a)	Facility access controls	Physical Safeguards	7	Partially Addressed
164.310(b)	Workstation use	Physical Safeguards	6	Partially Addressed
164.310(c)	Workstation security	Physical Safeguards	0	Not Addressed
164.310(d)	Device and media controls	Physical Safeguards	1	Partially Addressed
164.312(a)	Access control	Technical Safeguards	1	Partially Addressed
164.312(b)	Audit controls	Technical Safeguards	2	Partially Addressed
164.312(c)	Integrity	Technical Safeguards	16	Partially Addressed
164.312(d)	Person or entity authentication	Technical Safeguards	1	Partially Addressed
164.312(e)	Transmission security	Technical Safeguards	1	Partially Addressed
164.314	Organizational requirements	Security Rule	0	Not Addressed
164.316	Policies, procedures and documentation	Security Rule	10	Partially Addressed
164.502	Uses and disclosures of PHI: general rules	Privacy Rule	6	Partially Addressed

HIPAA provision	Title	Rule group	Mapped GAISSF controls	Coverage
164.504	Organizational requirements	Privacy Rule	11	Partially Addressed
164.506	Uses and disclosures for treatment, payment, operations	Privacy Rule	0	Not Addressed
164.508	Uses and disclosures requiring authorization	Privacy Rule	0	Not Addressed
164.514	Other requirements relating to uses and disclosures	Privacy Rule	1	Partially Addressed
164.520	Notice of privacy practices	Privacy Rule	0	Not Addressed
164.522	Rights to request privacy protection	Privacy Rule	0	Not Addressed
164.524	Access of individuals to PHI	Privacy Rule	0	Not Addressed
164.526	Amendment of PHI	Privacy Rule	16	Partially Addressed
164.528	Accounting of disclosures	Privacy Rule	0	Not Addressed
164.530	Administrative requirements	Privacy Rule	13	Partially Addressed
164.532	Transition provisions	Privacy Rule	0	Not Addressed
164.534	Compliance dates	Privacy Rule	0	Not Addressed
164.400-414	Breach notification requirements	Breach Notification Rule	4	Partially Addressed
160.300-552	Compliance, investigations and penalties	Enforcement Rule	5	Partially Addressed

4. GAISSF-to-HIPAA Mapping Register

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						legal permissions, and evidence sufficiency remain separate.
D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	164.310(d)	Device and media controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-02	MODEL EXTRACTION RESISTANCE	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI

GAISSTF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-02	MODEL EXTRACTION RESISTANCE	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-02	MODEL EXTRACTION RESISTANCE	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-03	BEHAVIORAL DRIFT DETECTION	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-03	BEHAVIORAL DRIFT DETECTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-03	BEHAVIORAL DRIFT DETECTION	164.526	Amendment of PHI	P	Medium	HIPAA-specific

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-03	BEHAVIORAL DRIFT DETECTION	164.308(a)(6)	Security incident procedures	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementat ion specification s, reasonablen ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementat ion specification s, reasonablen ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						remain separate.
D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						ion specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-08	MODEL MERGE ATTACK DETECTION	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						evidence sufficiency remain separate.
D1-CTL-08	MODEL MERGE ATTACK DETECTION	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-08	MODEL MERGE ATTACK DETECTION	164.308(a)(6)	Security incident procedures	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-08	MODEL MERGE ATTACK DETECTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						permissions, and evidence sufficiency remain separate.
D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	164.310(b)	Workstation use	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	164.310(b)	Workstation use	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-03	JAILBREAK RESISTANCE TESTING	164.310(b)	Workstation use	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-03	JAILBREAK RESISTANCE TESTING	164.308(a)(8)	Evaluation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-03	JAILBREAK RESISTANCE TESTING	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	164.310(b)	Workstation use	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION	164.310(b)	Workstation use	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementat ion specification s, reasonablen ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementat ion specification s, reasonablen ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-06	CROSS-CONTEXT	164.310(b)	Workstation use	P	Medium	HIPAA-

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
	HIJACKING MITIGATION					specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D2-CTL-06	CROSS-CONTEXT HIJACKING MITIGATION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-01	LEAST AGENCY ENFORCEMENT	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION	164.308(a)(6)	Security incident procedures	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						separate.
D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-04	EMBODIED AI SAFETY CONTROLS	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	164.308(a)(8)	Evaluation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation

GAISSTF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	164.308(a)(1)	Security management process	P	Medium	HIPAA- specific applicability, PHI/ePHI scope, required- versus- addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	164.400-414	Breach notification requirements	P	Medium	HIPAA- specific applicability, PHI/ePHI scope, required- versus- addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						sufficiency remain separate.
D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	164.312(e)	Transmission security	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	164.308(b)	Business associate contracts and arrangements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						and evidence sufficiency remain separate.
D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	164.308(b)	Business associate contracts and arrangements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-03	MODEL HUB & REGISTRY VETTING	164.308(b)	Business associate contracts and arrangements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-03	MODEL HUB & REGISTRY VETTING	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	164.308(b)	Business associate contracts and arrangements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						legal permissions, and evidence sufficiency remain separate.
D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	164.312(b)	Audit controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	164.308(a)(6)	Security incident procedures	P	Medium	HIPAA-specific applicability, PHI/ePHI

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	164.308(b)	Business associate contracts and arrangements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentati

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	164.308(a)(8)	Evaluation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	164.308(b)	Business associate contracts and arrangements	P	Medium	HIPAA-specific

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	164.530	Administrative requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	164.316	Policies, procedures and documentation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	164.308(b)	Business associate contracts and arrangements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementat ion specification s, reasonablen ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementat ion specification s, reasonablen ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
D5-CTL-01	HARMFUL CONTENT BLOCKING	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-01	HARMFUL CONTENT BLOCKING	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-01	HARMFUL CONTENT BLOCKING	164.502	Uses and disclosures of PHI: general rules	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-02	PII LEAKAGE PREVENTION	164.502	Uses and disclosures of PHI: general rules	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-02	PII LEAKAGE PREVENTION	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						remain separate.
D5-CTL-02	PII LEAKAGE PREVENTION	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-02	PII LEAKAGE PREVENTION	164.514	Other requirements relating to uses and disclosures	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-03	COPYRIGHT DETECTION	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						ion specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-03	COPYRIGHT DETECTION	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-03	COPYRIGHT DETECTION	164.502	Uses and disclosures of PHI: general rules	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						evidence sufficiency remain separate.
D5-CTL-03	COPYRIGHT DETECTION	164.308(a)(6)	Security incident procedures	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-04	AI WATERMARKING ROBUSTNESS	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-04	AI WATERMARKING ROBUSTNESS	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-

GAISSTF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-04	AI WATERMARKING ROBUSTNESS	164.502	Uses and disclosures of PHI: general rules	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	164.502	Uses and disclosures of PHI: general rules	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						permissions, and evidence sufficiency remain separate.
D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	164.312(c)	Integrity	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	164.530	Administrative requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	164.526	Amendment of PHI	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	164.502	Uses and disclosures of PHI: general rules	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	164.312(c)	Integrity	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	164.530	Administrative requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	164.526	Amendment of PHI	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	164.308(a)(2)	Assigned security responsibility	P	Medium	HIPAA-specific applicability,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	164.530	Administrative requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	164.316	Policies, procedures and documentation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-02	AUDIT TRAIL COMPLETENESS	164.308(a)(2)	Assigned security responsibility	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-02	AUDIT TRAIL	164.316	Policies, procedures	SP	Medium-High	HIPAA-

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
	COMPLETENESS		and documentation			specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-02	AUDIT TRAIL COMPLETENESS	160.300-552	Compliance, investigations and penalties	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-02	AUDIT TRAIL COMPLETENESS	164.530	Administrative requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-03	AI MODEL CARD COMPLETENESS	164.308(a)(2)	Assigned security responsibility	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-03	AI MODEL CARD COMPLETENESS	164.316	Policies, procedures and documentation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						separate.
D6-CTL-03	AI MODEL CARD COMPLETENESS	164.530	Administrative requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-03	AI MODEL CARD COMPLETENESS	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-04	AI INCIDENT RESPONSE READINESS	164.308(a)(2)	Assigned security responsibility	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-04	AI INCIDENT RESPONSE READINESS	164.530	Administrative requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-04	AI INCIDENT RESPONSE READINESS	164.400-414	Breach notification requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						sufficiency remain separate.
D6-CTL-04	AI INCIDENT RESPONSE READINESS	164.308(a)(6)	Security incident procedures	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	164.308(a)(2)	Assigned security responsibility	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	164.530	Administrative requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	164.504	Organizational requirements	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	164.316	Policies, procedures and documentation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						and evidence sufficiency remain separate.
D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	164.504	Organizational requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	164.308(a)(2)	Assigned security responsibility	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	164.308(b)	Business associate contracts and arrangements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	164.530	Administrative requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	164.308(a)(2)	Assigned security responsibility	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						legal permissions, and evidence sufficiency remain separate.
D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	164.308(a)(7)	Contingency plan	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	164.308(a)(1)	Security management process	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	164.530	Administrative requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	164.308(a)(5)	Security awareness and training	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	164.308(a)(3)	Workforce security	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H02	DEEPFAKE DETECTION TRAINING	164.308(a)(5)	Security awareness and training	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H02	DEEPFAKE DETECTION TRAINING	164.308(a)(3)	Workforce security	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H02	DEEPFAKE DETECTION TRAINING	164.530	Administrative requirements	P	Medium	HIPAA-specific

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H02	DEEPFAKE DETECTION TRAINING	164.308(a)(6)	Security incident procedures	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H03	OUT-OF-BAND AUTHENTICATION	164.312(d)	Person or entity authentication	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H03	OUT-OF-BAND AUTHENTICATION	164.308(a)(3)	Workforce security	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementat ion specification s, reasonablen ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H03	OUT-OF-BAND AUTHENTICATION	164.312(a)	Access control	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementat ion specification s, reasonablen ess, documentati on, breach analysis, legal permissions, and evidence sufficiency remain separate.

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
D7-CTL-H04	AI SOCIAL ENGINEERING IR	164.308(a)(5)	Security awareness and training	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H04	AI SOCIAL ENGINEERING IR	164.308(a)(3)	Workforce security	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D7-CTL-H05	AI-ENHANCED EXTERNAL ATTACK DEFENSE	164.308(a)(3)	Workforce security	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications

GAISSTF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-01	EU AI ACT RISK TIER MAPPING	164.316	Policies, procedures and documentation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-01	EU AI ACT RISK TIER MAPPING	164.308(a)(1)	Security management process	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						remain separate.
D8-CTL-01	EU AI ACT RISK TIER MAPPING	160.300-552	Compliance, investigations and penalties	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-02	ISO 42001 GAP ANALYSIS	164.316	Policies, procedures and documentation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-02	ISO 42001 GAP ANALYSIS	160.300-552	Compliance, investigations and penalties	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						ion specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-03	GPAI TECHNICAL DOCUMENTATION VERIFICATION	164.316	Policies, procedures and documentation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-03	GPAI TECHNICAL DOCUMENTATION VERIFICATION	160.300-552	Compliance, investigations and penalties	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specification S, reasonableness, documentation, breach analysis, legal permissions, and

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						evidence sufficiency remain separate.
D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	164.530	Administrative requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	164.400-414	Breach notification requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	164.316	Policies, procedures and documentation	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	164.308(a)(6)	Security incident procedures	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D8-CTL-05	NIST SP 800-218A COMPLIANCE CHECK	164.316	Policies, procedures and documentation	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						permissions, and evidence sufficiency remain separate.
D8-CTL-05	NIST SP 800-218A COMPLIANCE CHECK	160.300-552	Compliance, investigations and penalties	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT	164.310(a)	Facility access controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	164.310(a)	Facility access controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope,

GAISSE	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	164.310(a)	Facility access controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	164.308(a)(3)	Workforce security	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	164.310(a)	Facility access controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	164.308(a)(6)	Security incident procedures	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	164.526	Amendment of PHI	P	Medium	HIPAA-specific applicability,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	164.312(c)	Integrity	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	164.312(b)	Audit controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness,

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	164.310(a)	Facility access controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-06	ACTUATOR COMMAND VERIFICATION	164.310(a)	Facility access controls	P	Medium	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-07	PHYSICAL INCIDENT	164.530	Administrative	SP	Medium-High	HIPAA-

GAISSF	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
	EVIDENCE PRESERVATION		requirements			specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	164.400-414	Breach notification requirements	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	164.310(a)	Facility access controls	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications,

GAISSE	Control title	HIPAA	Provision	Rel.	Confidence	Rationale / residual gap
						reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.
D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	164.308(a)(6)	Security incident procedures	SP	Medium-High	HIPAA-specific applicability, PHI/ePHI scope, required-versus-addressable implementation specifications, reasonableness, documentation, breach analysis, legal permissions, and evidence sufficiency remain separate.

5. Implementation Guidance

- Confirm covered-entity/business-associate status, organizational boundaries, and all PHI/ePHI flows before applying the mapping.
- Treat required and addressable Security Rule implementation specifications according to the regulatory text and documented risk analysis.
- Maintain HIPAA-specific policies, business associate agreements, notices of privacy practices, individual-rights workflows, breach assessments, documentation, and any current rule-specific transition/compliance obligations.
- Validate state health-privacy law, FTC health-breach rules, 42 CFR Part 2, genetic-information requirements, contractual duties, and sector-specific obligations separately.

6. Notably Absent

No HHS endorsement; no HIPAA certification; no automatic safe harbor; no determination of covered-entity or business-associate status; no proof that all PHI uses/disclosures are lawful; no substitute for a HIPAA Security Risk Analysis; no treatment of the pending Security Rule NPRM as binding; and no claim that GAISSE evidence is automatically sufficient for HIPAA.

D9 mappings are additional/conditional. Where Physical AI or cyber-physical actuation is in scope, PAI-SF™ v1.0 may be used alongside GAISSF; CSX-PAISF-004 is mapping only and does not establish equivalence, evidence sufficiency, or automatic conformance.

7. Limitations

- Mapping does not establish HIPAA compliance.
- Covered entity or business associate status is not determined.
- PHI/ePHI scope and permitted uses/disclosures require legal analysis.
- State health privacy laws may impose additional duties.
- The 2024 Security Rule NPRM is not treated as binding. Current Privacy Rule obligations are subject to the 2025 partial vacatur and the remaining effective Notice of Privacy Practices modifications.

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute.