HIPAA Compliance Guidelines

Document ID: COM-IR-001 **Last Updated:** 2024-01-25 **Owner:** Legal & Compliance **Classification:** Internal

---

Overview

The Health Insurance Portability and Accountability Act (HIPAA) establishes standards for protecting sensitive patient health information. This guide applies when NovaTech handles Protected Health Information (PHI) for healthcare customers.

Applicability

When HIPAA Applies

HIPAA applies to NovaTech when we: - Process PHI on behalf of healthcare customers (Covered Entities) - Act as a Business Associate - Have signed a Business Associate Agreement (BAA)

NovaTech's Role

NovaTech is typically a **Business Associate** when: - Providing CloudForge infrastructure to healthcare organizations - Storing or processing PHI through our platforms - Providing support that may involve PHI access

Products with BAA Availability

Product	BAA Available	Notes
CloudForge	Yes	Enterprise plan only
DevPipeline	Yes	Enterprise plan only
SecureVault	Yes	All paid plans
DataLens	No	Not recommended for PHI

HIPAA Rules Overview

Privacy Rule

Governs use and disclosure of PHI: - Minimum necessary standard - Patient rights (access, amendment, accounting) - Notice of privacy practices

Security Rule

Requires administrative, physical, and technical safeguards: - Risk analysis - Access controls - Audit controls - Encryption

Breach Notification Rule

Requires notification after breach of unsecured PHI: - Individual notice - HHS notice - Media notice (if >500 individuals)

Protected Health Information (PHI)

What is PHI?

Individually identifiable health information that: - Is created or received by a covered entity - Relates to health condition, treatment, or payment - Identifies the individual (or could be used to identify)

Examples of PHI

- Patient names with medical records
- Social Security numbers with health data
- Medical record numbers
- Health insurance information
- Diagnosis or treatment information
- Appointment dates with patient identity

Not PHI

- De-identified data (18 identifiers removed)
- Aggregate statistics
- Employment records (for employer)

Administrative Safeguards

Risk Analysis

Required: Conduct thorough risk analysis

NovaTech performs: - Annual comprehensive risk assessment - Ongoing risk monitoring - Risk treatment planning - Documentation of all assessments

Workforce Security

Controls: - Background checks for employees with PHI access - Role-based access (minimum necessary) - Termination procedures for PHI access removal

Security Training

Required: Regular security awareness training

NovaTech provides: - HIPAA-specific training for relevant roles - Annual refresher training - Training documentation and tracking

Incident Response

Required: Policies for security incidents

NovaTech maintains: - Incident response plan including PHI breaches - Breach assessment procedures - Notification procedures (within required timeframes)

Physical Safeguards

Facility Access Controls

Controls: - Data centers with SOC 2 certification - Biometric access to secure areas - Visitor management - Environmental controls

Workstation Security

Controls: - Automatic screen lock - Privacy screens where appropriate - Clear desk policy - No PHI on shared workstations

Device and Media Controls

Controls: - Asset tracking - Secure disposal (NIST 800-88) - Encryption of portable devices - Media sanitization procedures

---

Technical Safeguards

Access Control

Requirement	NovaTech Implementation
Unique user identification	Individual accounts, no shared credentials
Emergency access	Break-glass procedures documented
Automatic logoff	Session timeout (15 min for PHI systems)
Encryption	AES-256 at rest, TLS 1.2+ in transit

Audit Controls

Required: Record and examine system activity

NovaTech provides: - Comprehensive audit logging - Log retention (minimum 6 years) - Regular log review - Audit trail protection

Integrity Controls

Required: Protect PHI from improper alteration

NovaTech implements: - Data validation - Checksums/hashing - Version control - Backup verification

Transmission Security

Required: Protect PHI during transmission

NovaTech ensures: - TLS 1.2 minimum (TLS 1.3 preferred) - Certificate management - Secure API endpoints - VPN for administrative access

---

Business Associate Agreements

BAA Requirements

Business Associate Agreements must include: - Permitted uses and disclosures - Safeguard requirements - Subcontractor requirements - Breach notification obligations - Termination provisions - Return/destruction of PHI

NovaTech's BAA Process

1. Customer requests BAA
2. Legal reviews customer's BAA or provides NovaTech template
3. Negotiate terms if needed
4. Execute BAA
5. Implement any customer-specific requirements
6. Document in customer record

Subcontractors

When NovaTech uses subcontractors who may access PHI: - BAA required with subcontractor - Same obligations flow down - NovaTech remains responsible for subcontractor compliance

---

Breach Response

Breach Definition

Unauthorized acquisition, access, use, or disclosure of PHI that compromises security or privacy (unless low probability of compromise).

Response Timeline

Action	Deadline
Risk assessment	Immediate
Internal notification	24 hours
Customer notification	Without unreasonable delay
HHS notification (if required)	60 days (via Covered Entity)

Response Process

1. **Contain:** Stop ongoing breach
2. **Assess:** Determine scope and risk
3. **Notify:** Inform affected parties per agreements
4. **Remediate:** Address root cause
5. **Document:** Complete incident documentation

Customer Responsibilities

Under BAA

Customers (Covered Entities) are responsible for: - Obtaining patient authorizations - Responding to patient rights requests - Breach notifications to individuals/HHS - Their own HIPAA compliance

Shared Responsibilities

Responsibility	NovaTech	Customer
Platform security		
Access management	Platform-level	User-level
Data encryption	Infrastructure	Application data
Audit logging	System logs	Application logs
Breach notification	To customer	To individuals/HHS

Compliance Verification

NovaTech's Evidence

- SOC 2 Type II report (includes HIPAA mapping)
- Annual penetration testing
- Vulnerability management program
- Employee training records
- Incident response testing

Customer Audits

Enterprise customers may: - Review SOC 2 reports - Request security questionnaires - Conduct virtual audits (with notice) - Review compliance documentation

---

Penalties

Civil Penalties

Violation Category	Penalty per Violation	Annual Maximum
Did not know	$100 - $50,000	$25,000
Reasonable cause	$1,000 - $50,000	$100,000
Willful neglect (corrected)	$10,000 - $50,000	$250,000
Willful neglect (not corrected)	$50,000	$1,500,000

Criminal Penalties

- Knowingly obtaining PHI: Up to $50,000 and 1 year
- Under false pretenses: Up to $100,000 and 5 years
- Intent to sell/harm: Up to $250,000 and 10 years

Resources

Internal

- HIPAA questions: compliance@novatech.com
- BAA requests: legal@novatech.com
- Security concerns: security@novatech.com

External

- HHS HIPAA guidance: hhs.gov/hipaa
- NIST HIPAA Security Toolkit
- OCR breach portal

Related Documents: Data Classification Policy (IT-SEC-005), Incident Response Plan (IT-SEC-020), SOC 2 Overview (COM-SC-001)