# HIPAA Compliance Guide

**Document ID:** COM-IR-005 **Last Updated:** March 2024 **Owner:** Legal & Compliance **Applies To:** Employees Handling Healthcare Customer Data

---

## Overview

The Health Insurance Portability and Accountability Act (HIPAA) establishes requirements for protecting healthcare information. This guide covers NovaTech's HIPAA compliance program for customers in the healthcare industry.

---

## HIPAA Applicability

### When HIPAA Applies

HIPAA applies when NovaTech: - Serves healthcare customers (covered entities) - Processes Protected Health Information (PHI) - Acts as a Business Associate

### Covered Entities

Our healthcare customers include: - Healthcare providers (hospitals, clinics, doctors) - Health plans (insurance companies) - Healthcare clearinghouses

### Business Associate Status

When we process PHI on behalf of covered entities, we are a **Business Associate** and must comply with HIPAA.

---

## Protected Health Information (PHI)

### What is PHI?

Protected Health Information is individually identifiable health information, including:

| Category | Examples |
|---|---|
| Demographics | Name, address, birthdate, SSN |
| Health conditions | Diagnoses, symptoms, medications |
| Healthcare provision | Treatment records, test results |
| Payment information | Insurance, billing records |
| Identifiers | Medical record numbers, device IDs |

### Electronic PHI (ePHI)

PHI stored or transmitted electronically has additional protections under the Security Rule.

### PHI vs. De-identified Data

De-identified data (per HIPAA standards) is not PHI and not subject to HIPAA.

---

## HIPAA Rules

### Privacy Rule

Governs use and disclosure of PHI: - Minimum necessary standard - Patient rights - Notice requirements - Authorization requirements

### Security Rule

Requires safeguards for ePHI: - Administrative safeguards - Physical safeguards - Technical safeguards

### Breach Notification Rule

Requires notification when PHI is compromised: - Individual notification - HHS notification - Media notification (large breaches)

---

## Business Associate Agreement (BAA)

### When Required

BAA required before processing PHI for healthcare customers.

### NovaTech BAA

Our standard BAA is available for Enterprise customers: - Contact: legal@novatech.com - Available for: Enterprise plan customers - Includes: Required HIPAA provisions

### BAA Requirements

| Element | Description |
|---|---|
| Permitted uses | How we may use PHI |
| Safeguards | Security measures required |
| Reporting | Breach notification obligations |
| Subcontractors | Sub-BA requirements |
| Access | Patient access facilitation |
| Return/destruction | End of agreement procedures |
| Audit | Compliance verification |

---

## Administrative Safeguards

### Security Management

| Requirement | Implementation |
|---|---|
| Risk analysis | Annual security risk assessment |
| Risk management | Remediation of identified risks |
| Sanction policy | Employee accountability |
| Information system activity review | Regular log review |

### Workforce Security

| Requirement | Implementation |
|---|---|
| Authorization | Role-based access control |
| Clearance procedures | Background checks |
| Termination procedures | Access revocation process |

### Information Access Management

| Requirement | Implementation |
|---|---|
| Access authorization | Documented approval process |
| Access establishment | Least privilege principle |
| Access modification | Change management |

### Security Awareness and Training

| Requirement | Implementation |
|---|---|
| Security reminders | Regular communications |
| Malware protection | Endpoint security |
| Log-in monitoring | Failed login alerts |
| Password management | Password policy enforcement |

### Security Incident Procedures

| Requirement | Implementation |
|---|---|
| Response procedures | Incident response plan |
| Reporting | Internal reporting process |

### Contingency Plan

| Requirement | Implementation |
|---|---|
| Data backup | Regular encrypted backups |
| Disaster recovery | DR plan and testing |
| Emergency mode operation | Business continuity |
| Testing | Annual DR testing |
| Criticality analysis | Data criticality assessment |

### Evaluation

| Requirement | Implementation |
|---|---|
| Periodic evaluation | Annual compliance review |

### Business Associate Contracts

| Requirement | Implementation |
|---|---|
| Written contracts | BAAs with all sub-BAs |

---

## Physical Safeguards

### Facility Access Controls

| Requirement | Implementation |
|---|---|
| Contingency operations | Facility access during emergencies |
| Facility security plan | Physical security measures |
| Access control | Badge access, visitor logs |
| Maintenance records | Documentation of repairs |

### Workstation Use

| Requirement | Implementation |
|---|---|
| Workstation use | Acceptable use policy |
| Workstation security | Screen locks, secure locations |

### Device and Media Controls

| Requirement | Implementation |
|---|---|
| Disposal | Secure media destruction |
| Media re-use | Data wiping procedures |
| Accountability | Asset tracking |
| Data backup and storage | Encrypted storage |

---

## Technical Safeguards

### Access Control

| Requirement | Implementation |
|---|---|
| Unique user identification | Individual user accounts |
| Emergency access | Break-glass procedures |
| Automatic logoff | Session timeouts |
| Encryption | ePHI encryption |

### Audit Controls

| Requirement | Implementation |
|---|---|
| Audit logging | Comprehensive logging |
| Log review | Regular audit log review |
| Log retention | 6+ year retention |

### Integrity

| Requirement | Implementation |
|---|---|
| Data integrity | Checksums, validation |
| Authentication | Data origin verification |

### Transmission Security

| Requirement | Implementation |
|---|---|
| Integrity controls | TLS, integrity checking |
| Encryption | TLS 1.2+ for all transmissions |

---

## Breach Notification

### Definition of Breach

Unauthorized acquisition, access, use, or disclosure of PHI that compromises security or privacy.

### Notification Requirements

| Breach Size | Notification Timeline |
|---|---|
| <500 individuals | Annual report to HHS |
| 500+ individuals | 60 days to HHS, media, individuals |

### Notification Content

Required elements: - Description of breach - Types of information involved - Steps individuals should take - Steps we're taking - Contact information

### NovaTech Process

1. Discover potential breach
2. Assess if PHI involved
3. Notify affected customer immediately
4. Support customer's notification obligations
5. Document all actions

---

## HIPAA-Compliant Features

### Available in Enterprise Plan

| Feature | Description |
|---|---|
| Encryption at rest | AES-256 encryption |
| Encryption in transit | TLS 1.2+ |
| Access controls | RBAC, MFA required |
| Audit logging | Comprehensive activity logs |
| Backup encryption | Encrypted backups |
| Data residency | US data centers |
| BAA | Business Associate Agreement |
| Dedicated support | HIPAA-trained support |

### Configuration Requirements

For HIPAA compliance: 1. Enable all security features 2. Configure audit logging 3. Implement access controls 4. Enable encryption 5. Sign BAA

---

## Employee Requirements

### Who Must Comply

Employees with access to healthcare customer data: - Customer Success team members - Support engineers - Engineering (with PHI access) - Sales (contract handling)

### Training

Required training: - HIPAA fundamentals - Handling PHI appropriately - Breach reporting

### Access Limitations

- Minimum necessary access
- No PHI in emails or Slack
- Use only approved systems

---

## Vendor Management

### Sub-Business Associates

Our HIPAA-compliant sub-processors: - AWS (infrastructure) - Google Cloud (backup) - Datadog (monitoring - no PHI)

### Vendor Requirements

Before engaging vendors for PHI processing: 1. Security assessment 2. BAA execution 3. Compliance verification 4. Ongoing monitoring

---

## Audit and Compliance

### Internal Audits

| Activity | Frequency |
|---|---|
| Access review | Quarterly |
| Log review | Monthly |
| Policy review | Annual |
| Risk assessment | Annual |

### External Audits

- SOC 2 Type II (includes HIPAA controls)
- Customer audits (with notice)

### Documentation

Maintain for 6 years: - Policies and procedures - Training records - Audit logs - Incident reports - BAAs

---

## Incident Response

### PHI Incident Process

1. **Identify** - Suspect PHI exposure
2. **Contain** - Stop unauthorized access
3. **Report internally** - Security + Legal immediately
4. **Assess** - Determine if breach occurred
5. **Notify customer** - Within 24 hours
6. **Support notification** - Help customer meet obligations
7. **Remediate** - Fix root cause
8. **Document** - Complete incident record

### Contact Points

- Security incidents: security-urgent@novatech.com
- HIPAA questions: compliance@novatech.com
- Legal review: legal@novatech.com

---

## Resources

- **HIPAA Training:** learn.novatech.com/hipaa
- **BAA Requests:** legal@novatech.com
- **Compliance Questions:** compliance@novatech.com
- **HHS Guidance:** hhs.gov/hipaa

---

## Related Documents

- Information Security Policy (IT-SEC-001)
- Incident Response Plan (IT-SEC-020)
- Data Classification Policy (IT-SEC-015)
- Vendor Assessment Process (COM-INT-015)

---

*Review Cycle: Annual Next Review: March 2025*