HIPAA Compliance Handbook

Complete Guide to Healthcare Data Protection

anonym.legal

Updated: February 2026

Executive Summary: Healthcare Under Siege

Healthcare data breaches cost an average of **$7.42 million**—the highest of any industry for **14 consecutive years**. With 96% of ransomware attacks now involving data exfiltration, protecting PHI isn't just about avoiding fines—it's about survival.

Key Statistics (2025):
- $7.42M: Average healthcare data breach cost (IBM 2025)
- 710: Large breaches reported to HHS OCR
- 62M: Individuals affected by healthcare breaches
- 96%: Ransomware attacks with data exfiltration
- 192.7M: Records exposed in Change Healthcare breach

Chapter 1: HIPAA Overview

HIPAA (Health Insurance Portability and Accountability Act) establishes national standards for protecting sensitive patient health information. The law consists of three main rules:

Privacy Rule

Establishes standards for protecting PHI and gives patients rights over their health information. Covers use, disclosure, and access to protected health information.

Security Rule

Sets standards for protecting electronic PHI (ePHI). Requires administrative, physical, and technical safeguards to ensure confidentiality, integrity, and availability.

Breach Notification Rule

Requires covered entities to notify affected individuals, HHS, and sometimes media following a breach of unsecured PHI. Notification must occur within 60 days.

Chapter 2: The 18 PHI Identifiers

Under HIPAA Safe Harbor, these 18 identifiers must be removed for data to be considered de-identified:

1. **Names**: Full name, maiden name, aliases
2. **Geographic Data**: Street address, city, state, ZIP (except first 3 digits if population >20,000)
3. **Dates**: Birth date, admission date, discharge date, death date, all ages over 89
4. **Phone Numbers**: Home, work, mobile, fax numbers
5. **Fax Numbers**: All fax numbers associated with the individual
6. **Email Addresses**: Personal and work email addresses
7. **Social Security Numbers**: Full or partial SSN
8. **Medical Record Numbers**: MRN, chart numbers, internal patient IDs
9. **Health Plan Beneficiary Numbers**: Insurance member IDs, policy numbers
10. **Account Numbers**: Financial account numbers linked to healthcare
11. **Certificate/License Numbers**: Professional license numbers, certifications
12. **Vehicle Identifiers**: License plates, VINs associated with the individual
13. **Device Identifiers**: Serial numbers of implants, medical devices
14. **Web URLs**: Personal websites, social media profiles
15. **IP Addresses**: Network addresses linked to individuals
16. **Biometric Identifiers**: Fingerprints, voiceprints, retinal scans
17. **Full-Face Photos**: Any image showing facial features
18. **Unique Identifying Codes**: Any code that could identify an individual

Chapter 3: Safe Harbor De-Identification

The Safe Harbor method provides a straightforward path to de-identification by removing all 18 identifiers listed above. This is the most commonly used method.

Requirements:

- ■ Remove or generalize all 18 identifier types
- ■ Ensure no actual knowledge that residual information could identify an individual
- ■ Document the de-identification process
- ■ Establish policies for handling re-identification codes (if used)

Date Handling:

Dates can be generalized to year only. For ages over 89, aggregate as '90+'. Relative dates (days from admission) are permitted.

Geographic Handling:

ZIP codes can be retained if the first 3 digits represent an area with population >20,000. Otherwise, report as '000'. City and state can often be retained for population >20,000.

Chapter 4: Expert Determination Method

An alternative to Safe Harbor, Expert Determination requires a qualified statistical or scientific expert to determine that re-identification risk is 'very small'.

Requirements:

- Qualified expert applies statistical/scientific methods
- Risk of re-identification is 'very small'
- Expert documents methods and results
- Covered entity retains documentation

Expert Determination is more flexible but requires ongoing expert involvement and documentation. Most organizations prefer Safe Harbor for its simplicity.

Chapter 5: Technical Safeguards

Technical safeguards are the technology and policies for protecting ePHI:

Access Control (Required)

- Unique user identification for each user
- Emergency access procedures documented
- Automatic logoff after inactivity
- Encryption/decryption mechanisms

Audit Controls (Required)

- Hardware, software, and procedural audit mechanisms
- Regular review of audit logs
- Investigation of suspicious activity

Integrity Controls (Required)

- Mechanisms to authenticate ePHI
- Detection of unauthorized alterations

Transmission Security (Required)

- Integrity controls during transmission
- Encryption (addressable but strongly recommended)

Chapter 6: Administrative Safeguards

Security Management Process

- Conduct regular risk analysis
- Implement risk management measures
- Apply sanctions for violations
- Review information system activity

Workforce Security

- Authorization and supervision procedures
- Clearance procedures for PHI access
- Termination procedures (access revocation)

Training Requirements

- Security awareness training for all workforce
- Training on policies and procedures
- Periodic refresher training
- Specialized training for security personnel

Chapter 7: Physical Safeguards

Facility Access Controls

- Contingency operations procedures
- Facility security plan
- Access control and validation
- Maintenance records for security systems

Workstation Security

- Workstation use policies defined
- Physical workstation security measures
- Screen positioning to prevent viewing
- Clean desk policy for PHI documents

Device and Media Controls

- Disposal procedures for devices with ePHI
- Media re-use procedures
- Accountability tracking for devices
- Data backup and storage procedures

Chapter 8: Business Associate Agreements

A Business Associate Agreement (BAA) is required before sharing PHI with any vendor or partner who will access, create, receive, maintain, or transmit PHI on your behalf.

Required BAA Elements:

- ■ Description of permitted uses and disclosures
- ■ Prohibition of unauthorized use/disclosure
- ■ Safeguards requirement
- ■ Reporting obligations for breaches
- ■ Subcontractor requirements
- ■ Access to PHI for patient rights requests
- ■ Amendment procedures
- ■ Accounting of disclosures
- ■ Compliance with Security Rule
- ■ Termination provisions

Chapter 9: Breach Response Timeline

Critical: You have 60 days to notify affected individuals after discovering a breach.

Immediate (0-24 hours):

- Contain the breach and prevent further access
- Document everything (who, what, when, where)
- Preserve evidence for investigation
- Notify internal incident response team

Short-term (1-14 days):

- Conduct risk assessment (was PHI compromised?)
- Determine scope (how many individuals affected?)
- Identify affected individuals
- Prepare notification content

Notification (within 60 days):

- Notify affected individuals (mail or email)

- Notify HHS via breach portal
- If >500 affected: notify prominent media outlet
- Document all notifications sent

Chapter 10: OCR Audit Preparation Checklist

Be prepared for an HHS Office for Civil Rights (OCR) audit with this checklist:

Documentation Ready:

- ■ Current risk analysis (within 12 months)
- ■ Risk management plan and evidence of implementation
- ■ Policies and procedures (reviewed annually)
- ■ Business associate agreements (all current)
- ■ Training records for all workforce members
- ■ Incident response procedures
- ■ Breach notification records
- ■ Sanction records (if any)

Technical Evidence:

- ■ Access control logs and user lists
- ■ Audit log samples
- ■ Encryption evidence (at rest and in transit)
- ■ Backup and disaster recovery testing records
- ■ Penetration test results
- ■ Vulnerability scan reports

Chapter 11: De-Identification Implementation

Implementing a de-identification program requires careful planning:

Step 1: Inventory PHI Data

Identify all systems, databases, and documents containing PHI. Map data flows to understand where PHI is created, stored, and transmitted.

Step 2: Choose De-Identification Method

Safe Harbor is recommended for most organizations due to its clarity and simplicity. Expert Determination may be appropriate for complex research use cases.

Step 3: Implement Technical Controls

- Deploy automated PII detection tools
- Configure anonymization rules for each identifier type
- Test de-identification on sample data
- Validate that all 18 identifiers are addressed

Step 4: Document and Monitor

- Document de-identification procedures
- Train staff on proper handling
- Monitor for PHI leakage
- Conduct periodic audits

Chapter 12: How anonym.legal Supports HIPAA

anonym.legal provides comprehensive PHI detection and de-identification:

- **All 18 HIPAA Identifiers**: Detect and anonymize every PHI category
- **48 Languages**: Support for diverse patient populations
- **Reversible Encryption**: AES-256-GCM for authorized re-identification
- **Zero-Knowledge Auth**: Your encryption keys stay private
- **German Data Residency**: 100% EU infrastructure, GDPR compliant
- **Desktop App**: Process files locally, minimal cloud exposure
- **API Integration**: Integrate into existing healthcare workflows
- **Audit Trail**: Complete records for compliance documentation

Start your HIPAA compliance journey at **https://anonym.legal**

Appendix A: 18 Identifiers Quick Reference

#	Identifier	Example	Action
1	Names	John Smith	Remove or pseudonymize
2	Geography	123 Main St	Remove; keep state if >20K pop
3	Dates	DOB: 01/15/1985	Year only; 90+ for ages >89
4	Phone	(555) 123-4567	Remove completely
5	Fax	(555) 123-4568	Remove completely
6	Email	john@example.com	Remove completely
7	SSN	123-45-6789	Remove completely
8	MRN	MRN-12345	Remove or pseudonymize
9	Health Plan ID	HP-987654	Remove or pseudonymize
10	Account #	Acct-111222	Remove completely
11	License #	NPI-1234567	Remove completely
12	Vehicle ID	ABC-123	Remove completely
13	Device ID	SN-12345	Remove completely
14	URLs	facebook.com/john	Remove completely
15	IP Address	192.168.1.1	Remove completely
16	Biometrics	Fingerprint	Remove completely
17	Photos	Face image	Remove or blur
18	Other IDs	Custom codes	Remove or pseudonymize

Appendix B: Sample BAA Clauses

Include these key provisions in your Business Associate Agreements:

Permitted Uses:

> "Business Associate may use or disclose PHI only as permitted by this Agreement or as required by law. Any use not specifically authorized is prohibited."

Safeguards:

> "Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI as required by the HIPAA Security Rule."

Breach Notification:

> "Business Associate shall report to Covered Entity any use or disclosure of PHI not permitted by this Agreement, including any Security Incident or Breach, within 24 hours of discovery."

Termination:

> "Upon termination, Business Associate shall return or destroy all PHI received from Covered Entity. If return or destruction is not feasible, protections of this Agreement shall extend to such PHI."

Appendix C: Breach Notification Template

Individual Notification Letter Template:

[Organization Letterhead]
[Date]

Dear [Patient Name],

We are writing to inform you of a security incident that may have affected your protected health information.

What Happened:
[Brief description of the incident]

Information Involved:
[Types of PHI affected: name, DOB, SSN, medical record numbers, etc.]

What We Are Doing:
[Steps taken to investigate and prevent future incidents]

What You Can Do:

- Review your health insurance statements for unfamiliar charges
- Request a free credit report at annualcreditreport.com
- Consider placing a fraud alert on your credit file

For More Information:
Contact our Privacy Officer at [phone] or [email]

We sincerely apologize for any inconvenience this may cause.

Sincerely,
[Privacy Officer Name]
[Title]

This handbook is provided for informational purposes only and does not constitute legal advice. Consult with a qualified healthcare compliance professional for specific guidance.