CODEX

CODING DECODED

HIPAA, HITECH & Fraud-Abuse Laws

Privacy, Security & Compliance Standards for Medical Coding

CODING DECODED

This guide covers the core HIPAA privacy and security provisions, how the HITECH Act strengthened HIPAA, and the federal fraud and abuse statutes that govern billing and referral practices.

1. HIPAA Privacy & Security Rule — Key Provisions

Quick-reference cards summarizing core HIPAA rules, real-world examples, and common violations.

HIPAA Privacy Rule — Patient Rights

Patients have the right to file complaints about privacy violations.

Example: *A hospital cannot share patient health details with a family member without patient consent unless legally permitted (e.g., emergencies).*

Violation Example: *A nurse discusses a patient's diagnosis in a public area, exposing private information.*

HIPAA Security Rule — Technical Safeguards

Technical safeguards include encryption, secure passwords, and multi-factor authentication.

Example: *A hospital encrypts patient records to prevent hackers from stealing data.*

Violation Example: *A healthcare worker leaves a computer open with patient data visible, allowing unauthorized access.*

HIPAA Breach Notification Rule

Purpose: Requires healthcare providers to notify patients if their PHI is breached or exposed.

Notification Requirements: If a breach affects more than 500 people, the provider must inform HHS and the media, and patients must be notified within 60 days. Smaller breaches (under 500 people) must be reported annually.

Example: *A hospital accidentally emails PHI to the wrong recipient. They notify affected patients and report it to HHS.*

Violation Example: *A healthcare provider does not inform patients about a hacking incident that exposed their medical data.*

HIPAA Enforcement Rule

Purpose: Sets penalties and fines for HIPAA violations.

Example: *A healthcare clinic fails to encrypt ePHI and suffers a data breach. They are fined $500,000 for failing security compliance.*

Violation Example: *A nurse shares a patient's medical history on social media. The hospital faces lawsuits and heavy fines.*

2. HIPAA Titles

HIPAA is divided into five titles, each with a unique purpose, such as health insurance protections, administrative rules, security of patient information, and tax-related provisions.

Title	Purpose
Title I: Health Insurance Portability	Protects health coverage when changing jobs, limits pre-existing condition exclusions.
Title II: Administrative Simplification	Privacy & security rules, electronic transactions, breach notifications.
Title III: Tax-Related Health Provisions	Medical Savings Accounts (MSAs), tax deductions for health insurance.
Title IV: Group Health Plan Requirements	Prevents discrimination in employer health plans, ensures renewability.
Title V: Revenue Offsets	Regulates tax treatment of healthcare benefits, prevents tax fraud.

3. HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009 to promote the adoption and meaningful use of Electronic Health Records (EHRs). The law strengthens HIPAA regulations, improves healthcare efficiency, and enhances data security.

Key Objectives of HITECH

- **Encourage EHR Adoption —** Encourages healthcare organizations to transition from paper-based records to electronic systems.
- **Improve Healthcare Quality —** Enhances patient safety and care coordination through better access to medical records.
- **Strengthen Data Security & Privacy —** Implements stricter HIPAA compliance measures to protect sensitive patient data.
- **Ensure Meaningful Use of EHRs —** Establishes criteria for healthcare providers to use EHRs effectively in improving patient outcomes.
- **Increase Penalties for Non-Compliance —** Introduces stricter penalties for HIPAA violations related to electronic health information.

4. How HIPAA and HITECH Are Related

The HITECH Act builds upon HIPAA by expanding its scope and strengthening compliance regulations, particularly for electronic protected health information (ePHI). Here's how they are connected:

- **Enhanced Privacy & Security Rules:** HITECH introduced stricter HIPAA enforcement, requiring covered entities and business associates (like companies doing medical coding in India) to protect ePHI.
- **Stronger Breach Notification Requirements:** HITECH mandated that organizations notify affected individuals and the Department of Health and Human Services (HHS) in case of a data breach.
- **Increased Penalties for Non-Compliance:** HITECH raised the fines for HIPAA violations.
- **Business Associate Liability:** Under HITECH, business associates (BAs) handling PHI must comply with HIPAA security rules.
- **Promoting EHR Adoption:** While HIPAA originally focused on privacy, HITECH emphasized electronic health information exchange, ensuring secure and meaningful use of EHRs.

Together, HIPAA and HITECH work to safeguard patient information while encouraging the use of health IT systems to improve care quality and efficiency.

HITECH Act and HIPAA Compliance

HITECH expanded HIPAA regulations by:

- **Requiring Business Associates (BAs)** to comply with HIPAA Security & Privacy Rules.
- **Mandating Breach Notification Rules,** where covered entities must notify affected individuals of data breaches.
- **Increasing Fines for Non-Compliance**

5. HITECH Compliance Best Practices

- **Maintain HIPAA & HITECH Training —** Regular staff training on privacy and security protocols.
- **Use Strong Access Controls —** Implement role-based access restrictions to limit exposure to ePHI.
- **Perform Regular Security Audits —** Conduct risk assessments to detect vulnerabilities.
- **Ensure Proper Documentation Practices —** Coders should adhere to security guidelines when handling patient information.
- **Monitor EHR Activity Logs —** Detect unauthorized access and suspicious activities.

6. Data Breach Notification Requirements

- **Individual Notification:** Individuals affected by a data breach should be notified within 60 days of discovering the breach.
- **HHS Notification:** The Department of Health & Human Services should be notified within 60 days.

Best Practices for Compliance

- **Develop an Incident Response Plan (IRP) —** Ensure the organization has a structured plan for handling breaches.
- **Regularly train staff —** Conduct ongoing HIPAA and HITECH training for employees.
- **Encrypt PHI and use access controls —** Reduce the risk of breaches by securing data.
- **Document all breach assessments and reports —** Maintain detailed records for audit purposes.
- **Engage legal and compliance teams —** Ensure breach notifications meet federal and state requirements.

7. Fraud & Abuse Laws

The “Big Five” Fraud & Abuse Statutes

The five main federal laws that apply to physicians/providers are:

- 1. Anti-Kickback Statute (AKS)
- 2. Physician Self-Referral Law (Stark Law)

- 3. False Claims Act (FCA)
- 4. Exclusion Authorities
- 5. Civil Monetary Penalties Law (CMPL)

Anti-Kickback Statute (AKS)

A federal law that makes it illegal to offer, pay, solicit, or receive anything of value in exchange for patient referrals for services paid by Medicare/Medicaid.

- Anything of value refers to cash, gifts, free rent, travel, discounts, perks, etc.
- **Covers both sides:** the person offering and the person accepting the payment.
- Intent matters — it must be knowing and willful.

Penalties:

- Criminal fines, imprisonment, civil fines up to $50,000 per kickback, exclusion from Medicare/Medicaid.

Safe Harbors:

- Legal exceptions if rules are met (e.g., employment contracts, fair-market leases, discounts, group purchasing).
- If an arrangement fits a safe harbor, it is protected.

Example:

- A lab pays doctors a fee for each Medicare patient they send for testing → Illegal referral kickback.
- A hospital pays a physician a documented fair-market salary as an employee → Allowed (safe harbor).

Stark Law (Physician Self-Referral Law)

Prohibits physicians from referring Medicare/Medicaid patients for certain services (“Designated Health Services”) to entities in which they or their family have a financial interest.

Strict liability — no intent is needed. If the referral and financial tie exist, it's a violation. Covers both ownership/investment and compensation arrangements.

Designated Health Services (DHS)

- Clinical labs
- Imaging (X-rays, MRI, CT)
- Physical/occupational therapy
- DME and supplies
- Home health, outpatient drugs, hospital services, etc.

Penalties:

- Denial of payment, refunds, civil fines ($15,000 per service), exclusion from programs.

Exceptions:

- In-office ancillary services (e.g., a group practice lab or X-ray).
- Academic medical centers.
- Bona fide employment or contracts at fair market value.

Example:

- A physician refers Medicare patients to an imaging center he owns → Violation.
- A group practice runs its own in-house lab for patients → Allowed under in-office ancillary exception.

FCA, Exclusion Authorities & CMPL

Law	Key Points
False Claims Act (FCA)	Illegal to submit false bills to Medicare/Medicaid. Covers deliberate fraud, ignorance, or unintentional errors. Penalties: 3× losses + fines per claim. Punishment: prison + criminal fines.

Law	Key Points
Exclusion Authorities	OIG can ban people or companies from Medicare/Medicaid services. Excluded = cannot bill or work in federal programs. Mandatory bans for fraud, patient abuse, and felony drug/healthcare crimes. Permissive (optional) bans, such as license revocations, apply for Anti-Kickback Statute violations or submitting false claims.
Civil Monetary Penalties Law (CMPL)	OIG can issue civil fines for violations including false claims, kickbacks, patient inducements, and lying on program applications. Penalties: $10k–$50k per violation + 3× damages + possible exclusion.

Note: *OIG = Office of Inspector General, Department of Health and Human Services (HHS).*

CODEX
CODING DECODED