Code of Ethics in Healthcare to ensure the Privacy and Security of the Patients

Posted on May 22, 2018

Introduction

Privacy and security are ethical foundations of healthcare because patients must be able to seek care, disclose sensitive information, and trust that records will be used appropriately. The original essay correctly recognizes confidentiality, patient rights, and cyber risk, but it repeatedly calls the law “HIPPA” and incorrectly suggests that HIPAA was enacted to ensure the provision of healthcare. The correct name is the Health Insurance Portability and Accountability Act of 1996. Its Administrative Simplification provisions led to national standards governing certain health information and transactions. The HIPAA Privacy Rule regulates uses and disclosures of protected health information by covered entities and business associates, while the Security Rule requires administrative, physical, and technical safeguards for electronic protected health information. HIPAA does not cover every health application, employer, school, or consumer device. Ethical practice therefore extends beyond minimum legal compliance and requires respect for autonomy, confidentiality, fairness, patient safety, transparency, and responsible technology governance. (National Institute of Standards and Technology) (National Institute of Standards and Technology, 2024)

Why Confidentiality Matters

Clinical care depends on accurate information. Patients may withhold details about symptoms, medications, mental health, substance use, sexual health, violence, finances, or family circumstances when they fear exposure. Incomplete information can lead to unsafe diagnosis or treatment.

Confidentiality also protects dignity and autonomy. Health information can affect employment, relationships, insurance, reputation, and personal safety. The ethical duty is not merely to avoid embarrassment; it is to respect the patient’s control over deeply personal information while recognizing justified uses for treatment, payment, operations, public health, and legal obligations.

Privacy, Confidentiality, and Security

Privacy concerns a person’s interests and rights regarding information and personal space. Confidentiality concerns the obligation of someone who receives information to limit its use and disclosure. Security concerns safeguards that protect information from unauthorized access, alteration, loss, or disruption.

These concepts overlap but are not identical. Encryption may secure a database while an authorized employee uses information for an unethical purpose. A strong privacy policy may fail if technical systems are insecure. Effective governance must address all three.

Who HIPAA Covers

The HIPAA Privacy Rule applies to health plans, healthcare clearinghouses, and healthcare providers that conduct specified transactions electronically. It also creates obligations involving business associates that perform certain functions using protected health information. HIPAA does not automatically apply to every organization that holds health-related data. (U.S, “Department Health Human Services”, source 1)

Employers acting in their employment role, many wellness applications, social platforms, life insurers, and some direct-to-consumer services may fall outside HIPAA even when the data feel medical. Other federal or state laws may apply. Patients should not assume that a product is HIPAA regulated merely because it advertises health services. (U.S, “Department Health Human Services”, source 2)

The Privacy Rule

The Privacy Rule establishes standards for protected health information in any form held by regulated entities. It limits uses and disclosures without authorization while allowing defined activities such as treatment, payment, healthcare operations, and certain public-interest purposes.

The Rule gives individuals rights to inspect and obtain copies of records, request amendment, receive certain accounting of disclosures, request restrictions, and request confidential communications. Rights have procedures and exceptions, so organizations should explain them clearly rather than promising absolute control.

The Security Rule

The Security Rule focuses on electronic protected health information. It requires administrative, physical, and technical safeguards to protect confidentiality, integrity, and availability. Administrative safeguards include risk analysis, risk management, workforce training, incident procedures, contingency planning, and assigned security responsibility. Physical safeguards address facilities, workstations, and devices. Technical safeguards address access control, audit controls, integrity, authentication, and transmission security.

The current rule is risk based and contains required and addressable implementation specifications. “Addressable” does not mean optional without analysis. A regulated entity must assess whether the measure is reasonable and appropriate and document an equivalent alternative or why it is not

reasonable and appropriate.

Ethical Principles

Autonomy supports meaningful patient participation in decisions about information and care. Beneficence requires using information to promote patient welfare. Nonmaleficence requires reducing harm from exposure, identity theft, discrimination, clinical error, or unavailable systems. Justice requires fair treatment and attention to groups who may be disproportionately harmed by surveillance or data misuse.

Professional integrity requires honesty about limitations and conflicts. A clinician should not access a record out of curiosity, even when technical access exists. Ethical permission is narrower than system capability.

Minimum Necessary Use

The HIPAA minimum-necessary standard generally requires reasonable efforts to limit protected health information to what is needed for the purpose, subject to exceptions such as many treatment disclosures. The principle is also ethically useful beyond its exact legal scope.

Role-based access should prevent a billing employee from seeing unnecessary clinical detail and prevent a clinician from browsing records unrelated to care. Organizations should review access when roles change and monitor unusual activity.

Consent and Authorization

Clinical consent, HIPAA authorization, and general agreement to terms are different concepts. Authorization is required for certain uses and disclosures outside those permitted by the Privacy Rule and must contain specified elements. Consent to treatment does not automatically justify unrelated marketing or research use.

Information should be presented in understandable language. Patients cannot make meaningful choices when forms are vague, bundled, or designed to discourage refusal. Ethical transparency goes beyond obtaining a signature.

Patient Access and Correction

Access to records can improve understanding, coordination, and error detection. Patients may identify incorrect medications, outdated diagnoses, demographic errors, or missing information. Organizations

should have reliable procedures for identity verification, secure delivery, and timely response.

An amendment request does not require a provider to erase a professional judgment simply because the patient disagrees. The process should preserve record integrity while allowing the patient's statement and correcting factual errors where appropriate.

Cybersecurity as Patient Safety

Healthcare cyber incidents can delay surgery, disrupt medication systems, divert ambulances, expose records, and undermine public trust. Cybersecurity is therefore a patient-safety issue, not only an information-technology concern. HHS healthcare cybersecurity performance goals emphasize high-impact practices that reduce common risks and improve resilience. (U.S, "Department Health Human Services", source 3)

Organizations should maintain accurate asset inventories, use multifactor authentication, manage vulnerabilities, restrict privileges, segment networks, protect backups, monitor activity, and test incident response. Security controls should include clinical leaders because downtime and recovery decisions affect care.

Risk Analysis and Risk Management

The Security Rule requires an accurate and thorough assessment of risks and vulnerabilities to electronic protected health information. A generic checklist is not enough. The analysis should identify systems, data flows, threats, existing controls, likelihood, impact, and priorities.

Risk management converts findings into action. Leaders should assign responsibility, deadlines, resources, and verification. Accepted risk should be explicitly documented by authorized decision-makers. Repeating an assessment without correcting known weaknesses does not protect patients.

Access Control and Authentication

Every workforce member should have a unique identity. Access should reflect role and need, and privileged accounts should be separated from ordinary activity. Multifactor authentication reduces risk from stolen passwords. Emergency access procedures should support care without creating a permanent bypass.

Shared accounts weaken accountability. Automatic logoff and device controls can reduce exposure, but they must be designed around clinical workflow so that staff do not create unsafe workarounds. Usability is part of security.

Audit and Monitoring

Audit logs can reveal inappropriate access, changes, exports, and failed authentication. Monitoring should focus on risk, such as access to celebrity records, unusually large downloads, or repeated access outside a person's role.

Monitoring must itself be governed ethically. Employees should understand policies, and investigations should respect due process. An alert is evidence for review, not proof of misconduct.

Mobile Devices, Telehealth, and Remote Work

Phones, laptops, messaging, telehealth, and remote access improve care but expand risk. Organizations should approve platforms, encrypt devices, manage updates, control local storage, and support secure authentication. Consumer messaging applications may not meet organizational requirements.

Telehealth privacy includes the patient's environment. Clinicians should confirm identity, explain who is present, use private spaces, and consider whether a patient can speak safely. Technical compliance does not eliminate interpersonal risk.

Artificial Intelligence and Secondary Use

AI systems may analyze records for documentation, prediction, imaging, scheduling, or decision support. Ethical review should examine accuracy, bias, explainability, security, data provenance, and human oversight. A vendor's claim of HIPAA compliance does not establish clinical validity or fairness.

Secondary uses of data for research, quality improvement, product development, or model training require careful legal classification and ethical evaluation. De-identification reduces risk but may not eliminate reidentification possibilities. Data minimization and contractual controls remain important.

Business Associates and Supply Chains

Healthcare organizations depend on cloud providers, billing companies, laboratories, consultants, device vendors, and other partners. Business associate agreements define HIPAA responsibilities but do not replace due diligence. Organizations should evaluate security, access, subcontractors, incident notification, data return, and termination.

A supplier outage or compromise can disrupt many providers at once. Contingency planning should account for concentrated dependencies and manual alternatives.

Breach Response

A suspected breach requires containment, preservation of evidence, legal and privacy analysis, risk assessment, notification decisions, and support for affected people. The organization should not delay operational response while debating terminology. Incident plans should identify who has authority and how clinical services will continue.

Communication should be accurate and understandable. Minimizing harm or blaming one employee can undermine trust. After-action review should address technical, procedural, and governance causes.

Ethical Culture

Policies work only when leaders model them. Senior clinicians and executives should not receive informal exceptions. Staff should have safe channels to report privacy concerns, mistaken disclosures, lost devices, or suspicious messages. Early reporting enables faster harm reduction.

Training should use realistic scenarios and explain the relationship between privacy, cybersecurity, and care. Punitive cultures encourage concealment, while no-accountability cultures allow repeated negligence. Just culture distinguishes human error, risky behavior, and intentional misconduct.

Limits of Compliance

Legal compliance establishes a floor, not the complete ethical standard. A disclosure may be legally permitted yet unnecessarily broad. A patient portal may meet technical requirements yet be inaccessible to people with disabilities or limited English. A data project may satisfy a contract while creating unfair surveillance.

Ethical governance asks whether the use is necessary, proportionate, transparent, secure, and fair. It also considers alternatives and patient expectations.

Conclusion

Privacy and security are essential to trustworthy healthcare. HIPAA does not provide healthcare coverage and does not regulate every holder of health data. Its Privacy Rule governs protected health information held by covered entities and business associates, while its Security Rule requires administrative, physical, and technical safeguards for electronic protected health information. Ethical practice extends further through autonomy, beneficence, nonmaleficence, justice, confidentiality, transparency, and professional integrity. Effective organizations limit access, conduct real risk

analysis, use strong authentication, monitor appropriately, protect backups, govern suppliers, prepare for incidents, and make patient access practical. Technology should improve care without converting vulnerability into surveillance or exposure. Privacy, cybersecurity, and patient safety are not separate projects; they are connected responsibilities that must be designed into healthcare operations and continuously reviewed.

References

U.S. Department of Health and Human Services. *The HIPAA Privacy Rule*. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

U.S. Department of Health and Human Services. *The HIPAA Security Rule*. https://www.hhs.gov/hipaa/for-professionals/security/index.html

National Institute of Standards and Technology. (2024). *SP 800-66 Rev. 2: Implementing the HIPAA Security Rule*. https://csrc.nist.gov/pubs/sp/800/66/r2/final

U.S. Department of Health and Human Services. *Healthcare and Public Health Cybersecurity Performance Goals*. https://hhscyber.hhs.gov/cybersecurity-performance-goals.html