Health Insurance Portability and Accountability Act (HIPAA): an Overview

What We Know

› The Health Insurance Portability and Accountability Act of 1996 (HIPAA) safeguards the access of working Americans and their families to health insurance and protects the right of patients to privacy with regard to information related to their healthcare\(^1\,2\,7\,10\,12\,13\)
  • HIPAA has been updated numerous times since 1996; the most significant change is the 2013 final Omnibus Rule, which was enacted to implement the Health Information Technology for Economic and Clinical Health (HITECH) Act\(^6\,13\)
  • HIPAA is a process-oriented standard that assesses and manages risks from the impact of a privacy violation and provides general recommendations to mitigate identified risks\(^8\)
    – HIPAA contains standards that prevent unauthorized access of protected health information (PHI; any information in paper or electronic form that can lead to the identification of a patient, including the patient’s medical record and payment information) and require notification in the event of a security breach\(^14\,16\)
    – Medical records contain information that can be used in identity theft\(^9\)
  • HIPAA provisions
    – limit the ability of an employer to deny or restrict access to the employer’s group insurance plan because of a preexisting condition\(^1\,12\)
      - The employer can deny or restrict coverage for a medical condition only if medical advice, diagnosis, or treatment was recommended or received during the 6 months prior to the date of enrollment in the employer’s health plan; if the patient has a chronic condition but no new medical advice, diagnosis, or treatment were recommended or received during the 6 months prior to the date of enrollment, the condition is not considered a preexisting condition that affects insurance coverage
      - If a preexisting condition is identified, payment for care related to the condition can be restricted or denied only for a period of 12–18 months
    – allow the employee to transfer and continue health insurance coverage if the employee changes jobs or loses employment, as long as there is not a significant break in coverage of at least 63 days\(^2\)
      - The Consolidated Omnibus Budget Reconciliation Act (COBRA) allows employees who have recently lost employment to purchase continued insurance benefits for a limited period of time\(^1\,11\)
    – reduce health care fraud and waste\(^2\)
      - The 2003 HIPAA Privacy Rule establishes regulations safeguarding all PHI, whether written, oral, paper, or electronic\(^15\)
    – Under the HIPAA Privacy Rule
      - healthcare providers can disclose or share PHI for treatment, payment, or healthcare operations, and only with those personnel or organizations that have a need to know; generally PHI can be disclosed or shared with family members and others...
with the patient’s consent, but can also be disclosed or shared with others who need to know the information without patient consent (e.g., when the patient lacks the capacity to consent)\(^{(5,7,10,14)}\)

- HIPAA establishes exceptions that allow the disclosure of PHI without consent or authorization of the patient for public purpose, including instances when it is required by law, for public health surveillance, and in cases of abuse or intimate partner violence\(^{(2)}\)

- In addition, PHI can be disclosed to relatives when the patient is not able to authorize or object to the disclosure (e.g., when the patient is impaired due to mental illness, is unconscious, or under influence of drugs) and the healthcare provider determines it is in the best interest of the patient\(^{(14)}\)

- patients have the right to request access to their PHI\(^{(2)}\)
- patients must be notified of any breach in the privacy of their PHI\(^{(2,13)}\)
- the healthcare organization is required to:
  - document policies and procedures that are in place to safeguard the privacy and security of PHI\(^{(2,13)}\)
  - track the disclosure of information\(^{(5)}\)
  - train staff regarding HIPAA regulations and review competence of healthcare professionals\(^{(2,13)}\)
  - formally designate a privacy officer to maintain compliance with HIPAA regulations and establish compliance programs\(^{(2)}\)
  - implement contracts for business associates (e.g., persons working on behalf of the organization with whom the organization shares PHI) to promote their compliance with HIPAA regulations\(^{(5)}\)

- The 2003 HIPAA Security Rules establishes safeguards regulating PHI in electronic form (ePHI) specifically, which includes any communication in electronic form and electronic health records (EHRs).\(^{(13,15)}\) (For more information, see the Evidence-Based Care Sheet: Health Insurance Portability and Accountability Act (HIPAA): Data Communication and Security)
- Under the HIPAA Security Rule, there must be administrative, physical, and technical safeguards in place to maintain the security of PHI\(^{(10)}\)
  - ePHI must be encrypted (i.e., electronically scrambled and able to be deciphered only by specific individuals) to prevent impermissible access
- The Health Information Technology for Economic and Clinical Health (HITECH) Act, a component of the American Recovery and Reinvestment Act of 2009 (ARRA), was enacted to strengthen HIPAA provisions to safeguard the privacy and security of PHI and to promote enforcement efforts\(^{(2,10)}\)

–mandate the use of uniform identifier standards to be used on all health insurance claims and data transmissions\(^{(10)}\)
- The National Center for Health Statistics (NCHS) developed an ICD 10th revision clinical modification (ICD-10-CM) for morbidity purposes in the United States. The ICD-10-CM is the updated version and replacement for the ICD-9-CM, volumes 1 and 2, for coding and classifying mortality data from death certificates. The ICD-10-CM is effective October 1, 2015.\(^{(3)}\) (For more information, see the Evidence-Based Care Sheet: Health Insurance Portability and Accountability Act (HIPAA): Privacy and Death)
- The National Provider Identifier (NPI) is assigned to healthcare providers, the Federal Employer Identification Number (EIN) is assigned to employer-provided health insurance, and the National Health Plan Identifier is assigned to the specific insurance plan and the organizations that administer health insurance plans
–create civil and criminal penalties for violation of HIPAA regulations\(^{(10)}\)

 › The final omnibus rule for HIPAA released in January 2013\(^{(4)}\)
  - incorporates changes to HIPAA required by the HITECH Act
  - requires notification of breaches in unsecured data
  - amends the HIPAA privacy rule to increase the privacy protections for genetic information
  - increases civil penalties associated with the HIPAA Enforcement Rule as follows:
–$100–$50,000 per violation if the provider did not recognize there was a breach, to an annual maximum of $1.5 million
–$1,000–$50,000 per violation if there was reasonable cause for the breach, to an annual maximum of $1.5 million
–$10,000–$50,000 per violation if there was willful neglect in causing the breach but the breach was corrected in 30 days, to an annual maximum of $1.5 million
–$50,000 per violation if there was willful neglect in causing the breach and the breach was not corrected in 30 days, to an annual maximum of $1.5 million

HIPAA also prevents insurance companies from denying access to health insurance because of the presence of a preexisting condition\(^{(1,7)}\)

Compliance with the HIPAA Privacy Rule has been in effect since April 14, 2003. As of April 2018, the Office for Civil Rights (OCR) has received over 180,192 HIPAA Privacy Rule complaints, which have triggered 891 compliance reviews; 96% of these cases (111,465) have been resolved\(^{(2,15)}\)

**What We Can Do**

› Learn about HIPAA so you understand your patients’ rights under HIPAA and can accurately assess the ways in which your facility complies with HIPAA; share this information with your colleagues

› Collaborate with your facility’s education department to provide education for all employees regarding HIPAA, particularly the privacy and security requirements

---

**Coding Matrix**

References are rated using the following codes, listed in order of strength:

- **M** Published meta-analysis
- **SR** Published systematic or integrative literature review
- **RCT** Published research (randomized controlled trial)
- **R** Published research (not randomized controlled trial)
- **C** Case histories, case studies
- **G** Published guidelines
- **RV** Published review of the literature
- **RU** Published research utilization report
- **GI** Published quality improvement report
- **P** Legislation
- **PGR** Published government report
- **PFR** Published funded report
- **PP** Policies, procedures, protocols
- **X** Practice exemplars, stories, opinions
- **GI** General or background information/texts/reports
- **U** Unpublished research, reviews, poster presentations or other such materials
- **CP** Conference proceedings, abstracts, presentation

---

**References**