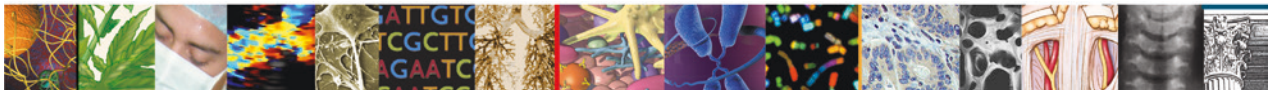


The NEW ENGLAND JOURNAL of MEDICINE

Perspective

NOVEMBER 24, 2022

FUNDAMENTALS OF HEALTH LAW

Privacy and Security — Protecting Patients' Health Information

Sharona Hoffman, J.D., L.L.M., S.J.D.

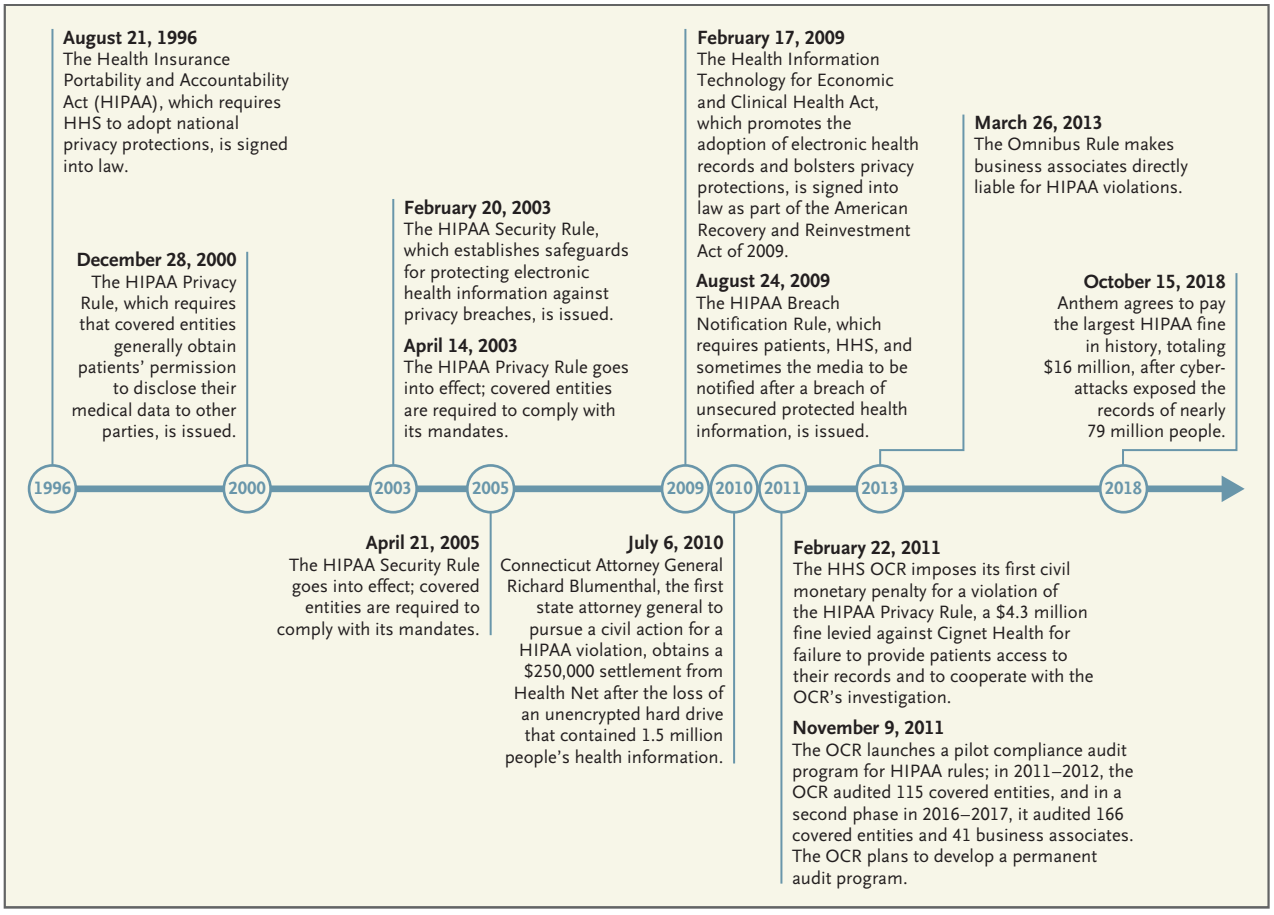
Careless conduct in a medical practice's waiting room led to an investigation by the Department of Health and Human Services (HHS) into privacy violations. A staff member had discussed HIV testing with a patient in front of other patients, and computer screens displaying patient data were clearly visible to people in the waiting area. In other, more egregious, privacy breaches, health care workers impermissibly viewed Britney Spears' psychiatric hospitalization records, and a researcher illegally gained access to the medical records of his supervisor, his coworkers, and several celebrity patients after learning that he was being fired.[1]

Many state laws and several federal statutes protect health information in various contexts and to varying degrees. The most comprehensive legal provisions addressing medical privacy in the United States are regulations known as the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

HIPAA, which was enacted in 1996, required HHS to adopt national privacy protections. The resulting Privacy and Security Rules became effective in 2003 and 2005, respectively (see timeline). The Privacy Rule was amended by the 2009 Health Information Technology for Economic and Clinical Health Act, a federal law that aimed to increase the adoption of electronic medical records and enhance patient protections. There has been no landmark court decision interpreting the Privacy and Security Rules, largely because individual patients cannot bring lawsuits over HIPAA violations.

The HIPAA Privacy Rule establishes that, with some substantial exceptions, health care providers and other entities covered by the regulations (known as covered entities) must obtain patients' permission to disclose their medical data to other parties. This constraint applies to both electronic and hard-copy medical records. For example, before responding to an employer's request for information about an employee's illness or providing medical information to a relative other than a person's legally appointed health care proxy, physicians must obtain a signed HIPAA release form from the patient.

Covered entities must give patients notices describing their privacy practices that meet detailed content specifications, and providers should ask all patients who receive privacy notices to return signed acknowledgments of receipt. In addition, patients have the right to view and copy their



Key Events in U.S. Health Privacy and Security Regulation.

HHS denotes the Department of Health and Human Services, and OCR the Office for Civil Rights.

health records and request modifications to their records or restrictions on their use. For example, patients may request that providers not submit claims information to their insurer because they would prefer to pay for treatments out of pocket. In general, covered entities may deny requests for modification if the patient's record is correct and are not required to comply with requests for usage restrictions that will hinder treatment, payment, or health care operations. Covered entities that experience privacy breaches involving unsecured data, such as incidents in which hackers gain access to unencrypted records, must notify affected patients, HHS, and — when breaches involve the records of more than 500 people in a state or jurisdiction — media outlets.

The HIPAA Security Rule establishes administrative, physical, and technical safeguards for protecting electronic health information against privacy breaches. Administrative safeguards address security-management processes, workforce security, information-access management, security awareness and training, security-incident procedures, and contingency plans. For example, employees should be trained to refrain from discussing medical information with patients in waiting rooms and from looking at records for non–work-related purposes, such as for satisfying one's curiosity. Covered entities must appoint HIPAA security officers and conduct security risk assessments. HHS has issued useful guidance regarding risk analysis.[2]

Physical safeguards include tools for controlling access to facilities and devices and securing workstations. For instance, covered entities must ensure that unauthorized people do not have access to server rooms and cannot see health information displayed on computer monitors. Technical safeguards relate to

access-control procedures for electronic health information (e.g., encryption), audit activities, protection against improper modification or deletion of health information, and authentication procedures for employees seeking access to such information. Many organizations hire HIPAA-compliance consultants to help them implement security measures.

Although the Privacy and Security Rules provide meaningful protection to U.S. patients, such protection is not comprehensive; it is limited by several important boundaries and exemptions.[3] For instance, the rules do not govern many parties that handle private health information. Covered entities include health plans, health care clearinghouses (entities involved in billing processes), health care providers who transmit health information electronically for the purposes of HIPAA-relevant activities, and their business associates (parties that handle protected health information while working with or providing services to covered entities).

But many other parties — including employers that have health information about their employees, marketing companies, website operators, data brokers, and life, disability, and long-term care insurers — are not considered covered entities. Such parties may store and process large volumes of health information for activities such as administering employment-related health exams, managing insurance applications, and marketing health-related products. Yet they are not obligated to comply with HIPAA's provisions or implement HIPAA-mandated security measures.

Covered entities are permitted to disclose health information without patients' consent in certain circumstances, including for the purposes of treatment, payment, and health care operations. Accordingly, physicians can discuss cases with colleagues (including those at other institutions) and speak with nurses about patients and can allow clerical personnel to review patient records for billing, quality improvement, or other administrative purposes without informing patients. This exception does not apply to using identifiable patient records for research purposes, which generally requires obtaining consent. The regulations list other circumstances in which health care providers can or must share medical information, including in the absence of patient authorization. Examples include disclosures that are required by law and those that are necessary for public health activities or law-enforcement purposes.

The HIPAA regulations define protected health information as "individually identifiable health information" that is electronically or otherwise transmitted or stored. Consequently, deidentified data fall outside the regulatory scope.[4] Such data can be shared without patient permission and do not have to be stored according to the Security Rule's standards. The Privacy Rule considers health information to be deidentified if a qualified expert determines that there is a "very small" risk that it could be reidentified (i.e., connected to the patient). Alternatively, users can deidentify data by removing 18 specific items, including the patient's name, certain geographic details, dates (except the year), facial images, and telephone, fax, account, and social security numbers.

An enormous amount of deidentified information is stored in databases that are used for research, quality-assessment, public health, and other nontreatment purposes. Government agencies at various levels and private enterprises have launched such "big data" initiatives. One of the best known initiatives is the National Institutes of Health "All of Us" research program, which aims to collect data from at least 1 million U.S. residents; another is the IBM Explorys Database, which contains electronic health record data. No matter how carefully an entity complies with HIPAA guidance, such deidentified data cannot be fully guaranteed to remain anonymous. There is always a small chance that attackers could use publicly available information, such as voter-registration records or news stories about patients, to reidentify records.

The Privacy Rule relaxes the data-deidentification requirements for circumstances in which having additional patient details might be necessary, such as in research contexts. It allows covered entities to share "limited data sets" for such uses without patient consent if recipients sign data-use agreements outlining specific restrictions and protections. Limited data sets have been stripped of most identifiers, but they retain information on dates and locations, though not patients' addresses.

The Privacy and Security Rules do not feature a private cause of action, which means that individual patients whose information was unlawfully disclosed cannot sue violators under the law. The HHS Office for Civil Rights (OCR) and state attorneys general offices are responsible for HIPAA enforcement. Violators

can be asked to take corrective action or pay fines and may very rarely face imprisonment. The medical practice that was careless about privacy in its waiting room was required to train its staff and reposition its computer screens. Dr. Huping Zhou, the former employee of the University of California at Los Angeles Health System who was found to have gained access to patient records 323 times after receiving a notice of employment termination, was fined and sentenced to 4 months in prison.

An audio interview with Dr. Hoffman is available at NEJM.org

Between April 2003 and February 2022, the OCR reportedly received more than 291,000 complaints about HIPAA violations.[5] The OCR has resolved the vast majority of these complaints and has required corrective measures in more than 29,000 cases. It has imposed fines or successfully pursued monetary settlements in only 106 cases, however, which have yielded a total of approximately $131.4 million.

The HIPAA Privacy and Security Rules provide patients with important protections and place substantial obligations on health care providers. At the same time, both patients and clinicians should understand the rules' limitations, and policymakers could consider regulatory modifications. Amid the proliferation of big data and increases in the number and types of entities processing health-related information, it will be particularly important to expand the range of entities that are required to protect patients' medical privacy and health-data security.

Disclosure forms provided by the author are available at NEJM.org.

The series editors are Erin C. Fuse Brown, J.D., M.P.H., Aaron S. Kesselheim, M.D., J.D., M.P.H., Debra Malina, Ph.D., Genevra Pittman, M.P.H., and Stephen Morrissey, Ph.D.

From Case Western Reserve University School of Law, Cleveland.

This article was published on November 19, 2022, at NEJM.org.

1. Brenner B. What is a HIPAA violation? 20 Catastrophic HIPAA violation cases. Naperville, IL: MedPro Disposal, June 2, 2017 (https://www.medprodisposal.com/8103/20-catastrophic-hipaa-violation-cases-to-open-your-eyes/).
2. Department of Health and Human Services. Guidance on risk analysis. July 2019 (https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html).
3. Hoffman S, Podgurski A. In sickness, health, and cyberspace: protecting the security of electronic private health information. Boston College Law Review 2007;48:331-86.
4. Hoffman S,Herveg J. Privacy and integrity of medical information. In: Orentlicher D,Hervey TK, eds. The Oxford handbook of comparative health law. New York: Oxford University Press, 2022:417-58.
5. Department of Health and Human Services. Enforcement highlights. 2022 (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html).

DOI: 10.1056/NEJMp2201676

Protecting Care for All — Gender-Affirming Care in Section 1557 and Beyond

Megan Lane, M.D., Anna R. Kirkland, J.D., Ph.D., and Daphna Stroumsa, M.D., M.P.H.

In August 2022, an estimated 9000 transgender or nonbinary (trans) Medicaid beneficiaries in Florida lost access to gender-affirming care, after the state's Agency for Health Care Administration banned its coverage.[1] This action reflects a national trend. Eight other states had already banned Medicaid coverage of gender-affirming care, and dozens of bills that would restrict access to such care have been introduced in about half of U.S. states, with a focus on young people since the beginning of 2020.[2] As states move to target trans people, access to necessary care will increasingly be blocked. But state bans on gender-affirming care would seem to violate Section 1557, the nondiscrimination clause of the Affordable Care Act (ACA), as well as other statutory and constitutional provisions, and are currently being challenged in courts.

As access to gender-affirming care is eroded in an increasing number of states, recent proposed regulations from the Biden administration for implementing Section 1557 would set a national standard for access to care, regardless of gender identity. Section 1557 applies to all health programs and activities receiving federal funds and all federally administered health programs, such as Medicaid and the ACA's health insurance marketplaces. The proposed rule affirms equal access to specialist care but also trans people's right to receive respectful care when obtaining ba-