

7.4c Privacy and Security

10x10 – Introduction to Biomedical Informatics & Artificial Intelligence
William Hersh, MD, FACMI, FAMIA, FIAHSI
Copyright 2026, All Rights Reserved



HIPAA privacy and security

[Privacy Rule](#)

[Security Rule](#)

Enforced by [HHS Office for Civil Rights \(OCR\)](#)

[Patient rights](#)

- Get data, check data, see who has seen it

[FTC Health Breach Notification Rule](#)

- Applies to health apps and similar technologies not covered by HIPAA

HIPAA not only US law or regulation governing privacy

Common Rule

- Governs rights of subjects participating in human research, updated in 2017 (Menikoff, 2017)
- Followed by many federal agencies – HHS rule governing human subjects research is [45 CFR 46](#)

Family Educational Rights and Privacy Act (FERPA)

- Prevents disclosure of personally identifiable information without approval of parents or (if over 18) student

Genetic Information Nondiscrimination Act (GINA)

- Prohibits discrimination based on genetic information in health coverage and employment

Some important newer privacy laws (Comparison – Kucera, 2021)

European General Data Protection Regulation (GDPR) (Haug, 2018; Burgess, 2020; de Kok, 2023) – went into effect in 2018

Applies to all personal data, with additional protections for highly sensitive data, including health data

“Controllers” and “processors” must

- Safeguard privacy and implement security to highest levels
- Disclose all data processing
- Allow deletion under certain circumstances

Guide to sharing open healthcare data under GDPR (de Kok, 2023)

California Consumer Privacy Act (CCPA)

– went into effect 2020; revised in 2023

Principles – rights to (from Fact Sheet)

- Know what information collected, shared, sold, and used
- Delete personal information held by businesses
- Opt out of sale of personal information
- Non-discrimination in price or service when privacy right exercised
- Correct personal information
- Limit use and disclosure

HIPAA Privacy Rule

Applies to “covered entities” (CEs) – any entity that bills electronically

- Healthcare providers
 - Clinicians, hospitals, clinics, etc.
- Health plans
 - HMOs, insurance companies, etc.
- Healthcare clearinghouses
 - Billing services

Patient must authorize any disclosure, with the exception of “treatment, payment, or operations” (TPO), i.e., does not preclude healthcare providers from sharing data for patient care, a not-uncommon misunderstanding (Houser, 2007)

Physician oaths of privacy – not new

Oath of Hippocrates, 5th century BC

- “All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and never reveal.”

Declaration of Geneva, 20th century

- “I will respect the secrets which are confided in me, even after the patient has died.”

What is covered?

Protected Health Information (PHI)

- Collected from patient and created by CE
- Individually identifiable health information as defined by HIPAA Privacy Rule

Extends to business associates (BAs)

Applies to personal health records and apps when implemented by CEs and BAs

De-identified information (as defined in rule) is not covered

Pre-emption

- HIPAA trumps state law if state law is less protective of privacy and security, but state laws that go beyond the HIPAA protections are not nullified by HIPAA and must be followed

Identifiers in PHI (“safe harbor” if removed)

Name

Address (street address, city, county, zip code)

Names of relatives

Names of employers

E-mail address

Fax number

Telephone number

Birth date

Finger or voice prints

Photographic images

Social security number

Internet protocol (IP) address

Any vehicle or device serial number

Medical record number

Health plan beneficiary number

Account number

Certificate/license number

Web URL

Any other unique identifying number, characteristic, or code

Key privacy compliance areas

Notice of privacy practices

Authorization

Business associates

Allowable disclosures

De-identification of data

Marketing and fundraising

Physician and staff training

Breaches and penalties

Notice of privacy practices (NPP)

Patient has right to

- Adequate notice of privacy practices
- Uses and disclosures of PHI
- Description of individual rights
- CE's legal duties

One problem is readability of NPP forms comparable to medical journal articles and beyond 80% of US adults (Breese, 2005)

Healthcare entity's requirements for obtaining NPP consent include

- "Good faith effort" to obtain acknowledgement during first provision of in-person service
- Failure to obtain is not penalized (per Bush administration revision)

Other aspects of privacy practices

Must be written in plain language

Practices/organizations must state they preserve the right to change notice of privacy practices

There must be a complaint process

Practices/organizations must designate a privacy officer

Examples of Notice of Privacy Practices (NPP)

- Models from [ONC OCR](#) and [OHSU](#)

Authorizations

Providers must obtain an authorization before disclosing PHI for purposes other than TPO

They may not condition treatment on an individual's authorization

CEs must make “reasonable safeguards” to limit the use or disclosure of PHI to the minimum amount necessary

Non-TPO disclosure governed by [Minimum Necessary standard](#)

Business associates (BAs)

Agents, contractors, or others doing work on behalf of a CE and using or disclosing PHI, such as

- Billing companies
- Vendors (with access to PHI)

BAs required to sign a Business Associate Agreement (BAA) with CE

In original HIPAA, had to obtain “satisfactory assurances” of privacy protections for BAs, but in HITECH Omnibus Rule, BAs now directly accountable to HHS for compliance

PHI cannot be put on a system from a vendor with whom CE does not a BAA – example from OHSU

- Residents from two different departments using Google Docs spreadsheet to track patients (McGee, 2013)
- OHSU does not have BAA with Google for such use
- Led to policy restricting use (also of Dropbox) for patient and student (FERPA) data



Allowable non-TPO disclosure – research

Protection of clinical research is purview of HHS [Office for Human Research Protections \(OHRP\)](#)

Most human research requires approval by an Institutional Review Board (IRB) and consent of subjects

- Some exemptions, most notably study of “existing data” [45CFR46.101(b)(4)], although all PHI governed by HIPAA
- Omnibus Rule allows
 - Compound authorizations – multiple functions in one consent
 - Use for future research projects if adequately described

Allowable non-TPO disclosures – other

Public health

- Can be disclosed to public health agencies for public health activities
- Also allowed for child abuse reporting, exposure to communicable diseases, and workforce surveillance
- CEs may disclose immunization data to a school with oral consent of parent or guardian

Other

- Law enforcement
- Decedents – clarified in Omnibus Rule
 - CEs may disclose to family members as long as consistent with previously expressed preferences
 - Disclosure restrictions cease after 50 years
- Cadaveric tissue donation

Disclosure of de-identified data

Privacy Rule allows de-identification of data for disclosure via two methods

- Expert determination – person with appropriate knowledge can apply statistical principles to determine risk of re-identification is “very small” (Malin, 2011)
- Safe harbor – removal of PHI identifiers
 - Biggest challenge for de-identification via safe harbor is textual documents – best current approaches use deep learning (Sepas, 2022)
 - Also concerns for re-identification for using other data, e.g., claims data (Ross, 2022)

OCR detailed [guidance on de-identification](#)

Marketing and fundraising

Marketing is defined as “a communication about a product/service that encourages recipients of the communication to purchase/use the product/service”

- Using PHI for marketing requires authorization from the individual

Is not marketing for providers if disclosure involves

- Therapy recommendation
- Appointment notification
- Prescription refills

CEs also have rights for fundraising, allowing it to be targeted using PHI

- Patients have right to opt out

Physician and staff training

Practices/organizations must

- Designate a Privacy Officer
- Develop policies and procedures
- Provide privacy training to workforce
- Develop a system of sanctions for employees who violate the Privacy Rule

Breaches and penalties

Enforced by OCR

Breach is “acquisition, access, use, or disclosure of PHI in a manner not permitted” – exceptions include

- Workforce member who unintentionally accessed or used in good faith
- Inadvertent disclosure between two individuals in same CE or BA
- When CE has good-faith belief that unauthorized person would not reasonably be able to retain PHI

Penalties higher for “willful neglect,” i.e., offender knew about violation or was recklessly indifferent

Breaches and penalties

Omnibus Rule strengthened timelines and penalties

CE must notify all individuals without delay and no later than 60 days after discovery

When involves 500+ patients, must also be reported to local media and HHS OCR; latter adds to “Wall of Shame”

All breaches of <500 in annual report to OCR

- 2013 was bad year for OHSU, with four big breaches (McCann, 2013), resulting in \$2.7M fine and security prescriptions (Conn, 2016)

Penalties tiered based on violation category – up to \$50K per violation and \$1.5M per calendar year for each violation

- Did not know
- Reasonable cause
- Willful neglect – corrected and uncorrected

HIPAA Security Rule

Aligned with terminology of Privacy Rule

Aims to minimize specificity to allow scalability, flexibility, and changes in technology

For each covered entity (CE) and business associate (BA), requirements are either

- Required – must be implemented
- Addressable – if reasonable and appropriate to implement

As with HIPAA Privacy Rule, some modifications under HITECH Omnibus Rule

- Enforcement moved from CMS to OCR
- More emphasis on [risk analysis and assessment](#)

More recent note: [Cloud computing allowable](#)

General provisions

CEs and now BAs must

- Ensure confidentiality, integrity, and availability of electronic PHI that they create, receive, transmit, and maintain
- Protect against reasonably anticipated threats and hazards to such information
- Protect against reasonably anticipated uses or disclosures not permitted by Privacy Rule
- Ensure compliance by workforce

HIPAA Security Rule core requirements

Access control

- Assign a unique name and/or number for identifying users
- Tracking user identity and establish controls that permit only authorized users to access PHI

Emergency access

- Permit appropriate authorized users to access PHI during an emergency

Automatic log-off

- Terminate an electronic session after a predetermined time of inactivity

HIPAA Security core requirements (cont.)

Audit log

- Record all actions related to PHI as it is created, accessed, and exchanged
- Must also enable user to generate an audit log for a specific time period and to sort entries in the audit log according to the comprising elements

Data integrity

- Verification – Upon receipt of electronically exchanged health information, use standard (equal to or greater than SHA-1) to verify the information has not been altered
- Detection – Detect alteration of audit log

Authentication

- Verify that a person or entity seeking access to PHI is the individual/organization claimed and is authorized to access such information

Future of HIPAA and privacy and security laws

HIPAA not infrequently misunderstood, compromising exchange of information for optimal care (Berwick, 2018)

Law devised before current era of ubiquitous Internet and patient information access (Cohen, 2018)

Framework for use and protection of health data beyond HIPAA (National Committee on Vital and Health Statistics, 2019)

HIPAA also did not anticipate healthcare being awash in “de-identified” data (Mandl, 2021)

- May be more re-identifiable than we think
- Large commercial value; benefits for patients, researchers, and others less clear

“Human-centered” cybersecurity should engage users as partners, not enemies (Zimmermann, 2024)

How should HIPAA evolve?

(Bari, 2019)

Define IIHI inherently protected class of data

Create new definitions of IIHI custodians and processors

Establish individuals' right to access, amend, and delete IIHI

Codify the permitted uses of IIHI absent explicit, ongoing, and granular patient consent

Specify clear parameters for consumer-friendly and revocable consent

(Rosenbloom, 2019)

Align HIPAA right of individual access with health IT certification

Extend HIPAA individual right of access to non-CEs, e.g., mHealth and social media

Encourage EHR data and clinical note-sharing with patients

Recommendations of group of professional associations and non-profits call for consistency in privacy laws and types of data plus education and collaboration (Sirona, 2023)



Additional challenges going forward

Most overcome “myths” and “fallacies” around HIPAA, (Trang, 2025) e.g.,

- No such thing as “HIPAA-compliant”
- De-identified health data not really de-identified
- Health tech pledge apps not covered under HIPAA

Use of generative AI may violate HIPAA (Schoolcraft, 2026)

- PHI used in LLM prompts higher chance to be memorized than traditional search
- LLM use likely not governed by BAA
- Many healthcare organizations blocking access to LLM tools, including those for search and knowledge access, e.g., OpenEvidence