

HIPAA: Review & Apply

Use this as a retrieval checklist after the lessons. Explain the reasoning before checking the rule.

Five questions before sharing information

1. Is this identifiable information about health, care, or payment for care?
2. Who is requesting it, and what identity or authority should be verified?
3. What permits or requires this use or disclosure?
4. Does minimum necessary apply, and what information is needed?
5. What safeguards, patient preferences, and documentation apply?

Core distinctions

- **HIPAA is a federal statute.** HHS regulations put its requirements into practice.
- **Covered entity vs. business associate:** most dispensing pharmacies qualify through electronic claims. A business associate handles PHI for the pharmacy outside its workforce. A prescriber receiving information for treatment does not become its business associate merely because of that disclosure.
- **Privacy vs. security:** the Privacy Rule protects spoken, printed, and electronic PHI. The Security Rule requires safeguards for electronic PHI.
- **De-identification:** removing a name alone is insufficient. Safe Harbor requires removal of specified identifiers and no actual knowledge that remaining information could identify the patient.
- **Safeguards:** administrative safeguards manage people and processes; physical safeguards protect places and equipment; technical safeguards control electronic access and activity.
- **Security goals:** confidentiality protects who can see information; integrity protects its accuracy; availability lets authorized staff obtain it when needed.

Permission and scope

Treatment, payment, and health care operations (TPO) are important permitted purposes. They are not the only reasons HIPAA permits sharing. If no permitted or required reason applies, obtain a valid written authorization before sharing. An acknowledgment of receiving a privacy notice is not an authorization.

Minimum necessary: take reasonable steps to limit information to the purpose when the standard applies. Exceptions include disclosures to or requests by providers for treatment, disclosures to the patient, valid authorizations, required HHS enforcement disclosures, disclosures required by law, and required HIPAA administrative-simplification compliance. The treatment disclosure/request exception does not allow unrestricted internal browsing.

Incidental use or disclosure: limited secondary exposure during an otherwise permitted activity, with reasonable safeguards and minimum necessary where applicable. Giving a prescription bag to the wrong patient is not permitted merely because it was accidental.

If someone requests information for a legal proceeding, refer the request to the pharmacy's privacy officer.

Patients and people helping them

- A **personal representative** has legal authority to act for the patient in relevant health care decisions. Verify that authority and its limits. Being a spouse or neighbor does not automatically authorize a full history.
- Share information directly relevant to a caregiver's involvement. Use patient agreement or non-objection when applicable; professional judgment can support best-interest sharing when the patient is absent or unable to decide.
- A neighbor collecting lisinopril may receive relevant counseling. The errand does not authorize unrelated medication information.
- PHI generally remains protected for 50 years after death. Representative access and limited sharing with people previously involved in care are different rules.

Patient requests: follow the steps

For access, confirm identity and authority; identify requested records in the **designated record set**; determine format and delivery; respond on time; apply only permitted fees; and follow required denial procedures. Dispensing histories and relevant billing records generally belong in the record set.

Allowed copying fees do not include searching, retrieving, or verifying identity. A patient's requested unencrypted email can be honored after explaining risk, confirming the preference, and verifying the destination.

Patient-request deadlines

Request	Initial limit	Extension
Access	30 calendar days after receipt.	One extension of up to 30 days.
Amendment	60 calendar days after receipt.	One extension of up to 30 days.
Accounting	60 calendar days after receipt.	One extension of up to 30 days.

For each extension, provide written reasons and a completion date within the initial period. Amendment follows required acceptance or denial procedures; an accepted correction does not automatically erase history.

Honor qualifying paid-in-full restrictions on health-plan payment/operations disclosures unless sharing is legally required. Accommodate reasonable confidential-communication requests without requiring the patient to explain why.

Accounting and privacy notices

An **accounting of disclosures** reports specified sharing, not every record access. It can cover the previous six years or a shorter period. Each entry includes date, recipient name and address if known, a description of PHI, and purpose or a qualifying written request. Common exclusions include TPO, sharing with the patient, authorizations, permitted incidental disclosures, and permitted involvement-in-care disclosures. The first accounting in any 12-month period is free.

Provide the **Notice of Privacy Practices (NPP)** by the first time the pharmacy provides care to a patient, with the emergency exception. Electronic delivery is possible with the patient's agreement; a paper copy remains available. Meet posting duties too. Attempt written acknowledgment; document the attempt and refusal if unsuccessful, and continue service.

Incident response and notification

For unauthorized access, use, or sharing, stop continuing exposure, address patient safety, promptly report internally, and document facts. A breach is presumed unless an exception applies or a documented assessment demonstrates low probability that PHI was compromised.

Assess **information involved; unauthorized recipient; actual acquisition or viewing; and steps reducing exposure**. Do not wait for financial or reputational harm. Exceptions require their full conditions: good-faith unintentional authorized-work access/use; specified inadvertent authorized-to-authorized sharing; or a good-faith belief that the recipient could not retain the information.

Notification rules apply to **unsecured PHI**, meaning information not protected using an HHS-specified method such as appropriate encryption or destruction. A password alone does not establish that protection.

Breach notification: recipients and deadlines

Recipient	Requirement
Affected individuals	Without unreasonable delay; no later than 60 calendar days after discovery.
HHS: 500 or more people	Without unreasonable delay; no later than 60 days after discovery, with individual notices.
HHS: fewer than 500 people	Log and report no later than 60 days after the discovery calendar year ends.
Prominent media	More than 500 affected residents in one state or jurisdiction; without unreasonable delay, no later than 60 days after discovery.
Business associate to pharmacy	Without unreasonable delay; no later than 60 days after discovery. The agreement may require faster reporting.

Sixty days is an outer limit, not permission to wait. Individual notice explains what happened, PHI involved, protective steps, the pharmacy's response, and contact information. For insufficient contact information: fewer than 10 people permits alternative written, telephone, or other notice; 10 or more requires homepage posting for at least 90 days or qualifying major media, plus a toll-free number for at least 90 days.

Disposal and consequences

Keep information secure through disposal and observe retention duties. Paper must become unreadable and not reconstructable. Labeled bottles may be held in opaque bags in a secure area for appropriate destruction; public trash is different. Electronic storage needs a method suited to the device; deleting files alone is insufficient.

Civil tiers: (1) did not know and would not have known through reasonable diligence; (2) reasonable cause without willful neglect; (3) willful neglect corrected within the required period; (4) willful neglect not corrected. Reasonable cause means knew or should have known, without conscious failure or reckless disregard. Willful neglect means conscious failure or reckless disregard. Learn the tiers, not dollar amounts.

Criminal maximum imprisonment: basic knowing violation, one year; false pretenses, five years; specified commercial advantage, personal gain, or malicious harm, ten years. Fines can also apply. OCR handles civil privacy/security/breach enforcement; DOJ prosecutes criminal violations. No direct patient lawsuit under HIPAA, but separate state-law claims may exist.

Background only: transactions/code sets, NPI, expert determination, NPP-content groups, and specialized accounting rules provide context. Bring unresolved questions to class Monday, November 2. Full linked sources appear in the module.