PHARM TECH BASICS · ONE-PAGER

HIPAA in the Pharmacy

What PHI is, who must protect it, minimum necessary, sharing without authorization, patient rights, family and pickup, the counter and the phone, disposal, the Security Rule, breaches, and card numbers and SSNs

21 sources + more detail
pharmtechbasics.com/sheets/pharm-hipaa.html
checked Nov 2026

1 The words that matter

TERM	MEANING	IN THE PHARMACY
PHI (protected health information)	Health or payment information that identifies a patient, in any form: spoken, paper or electronic	A name with a drug, a label, a claim, a profile, a phone message
Covered entity	A health plan, a clearinghouse, or a provider that sends standard electronic transactions such as claims	Any pharmacy that bills insurance electronically
Workforce	Employees, volunteers and trainees under the pharmacy's control, paid or not	Technicians, students, cashiers, drivers
Business associate	An outside company that handles PHI for the pharmacy; needs a written contract	Software vendor, billing service, shredding company
Minimum necessary	Use, share or ask for only the PHI the task needs	Does not apply when sharing with a provider for treatment

EXAM TIP HIPAA (1996, expanded by the HITECH Act of 2009) has three rules a technician meets: the Privacy Rule (all PHI, any form), the Security Rule (electronic PHI only) and the Breach Notification Rule. The HHS Office for Civil Rights enforces them.

2 Sharing PHI without the patient's written authorization

ALLOWED FOR	PHARMACY EXAMPLE
Treatment	Calling the prescriber, transferring a prescription, checking interactions
Payment	Billing a claim, a prior authorization, coordination of benefits
Health care operations	Quality review, audits, training staff
The patient	Telling the patient about their own prescriptions
People involved in care	Family or a friend, if the patient does not object (next section)
Required by law or public interest	State-required reports, FDA adverse events and recalls, board of pharmacy inspections; court orders and police requests only under set conditions

EXAM TIP Authorization is needed for marketing (most often a message a third party pays the pharmacy to send) and for any sale of PHI. A refill reminder for a drug the patient already takes is not marketing, as long as any outside payment is only what it costs to send.

3 Family, pickup, phone and counter

- Patient present: share with family or a friend if the patient agrees, does not object when asked, or clearly does not mind.
- Patient absent: the pharmacist may share what is directly relevant to that person's role, if it is in the patient's best interest.
- Pickup: HIPAA lets the pharmacy use professional judgment to let someone else pick up filled prescriptions. ID and signature rules come from pharmacy policy and state law.
- Voicemail: leave the least, such as the patient's name, the pharmacy and a callback number. A patient may ask to be called at another number or by another method.
- Counter: lower your voice, keep screens and bags turned from the line, and offer a private area. Incidental overhearing despite these steps is not a violation.

SAFETY Send to the pharmacist or privacy official: police, subpoenas, lawyers, media, an unknown caller asking for details, a parent asking about a minor, or a patient asking to restrict sharing. Never confirm that someone is a patient to a person with no role in their care.

4 Patient rights

RIGHT	RULE
Notice of Privacy Practices	Given no later than the first service, with a good-faith try at a written acknowledgment; posted in the pharmacy and on its website if it has one
Access (see and get a copy)	Act within 30 days, one 30-day extension; a reasonable cost-based fee only
Amendment	Act within 60 days, one 30-day extension; may deny if the record is accurate and complete
Accounting of disclosures	Up to 6 years back; within 60 days; first one free each 12 months; leaves out treatment, payment, operations and disclosures the patient authorized
Restriction	Pharmacy may refuse most requests, but must agree when a patient who paid in full for an item asks that the health plan not be told (unless a law requires it)
Confidential communications	Must honor reasonable requests for another address or phone; no reason needed

5 Disposal, security and breaches

- Paper with PHI (labels, vial and bag stickers, receipts, faxes, hard copies) is shredded or destroyed so it cannot be read or put back together. Marking out is not destruction.
- Electronic media are wiped or destroyed before reuse or disposal.
- Security Rule: administrative, physical and technical safeguards. Use only your own login, lock or log off the screen, never share passwords.
- Breach: notify each patient without unreasonable delay and no later than 60 calendar days after discovery. For 500 or more, HHS is told at the same time (media too if over 500 in one state); fewer go in a yearly report to HHS.

SAFETY Report a suspected breach to the privacy official at once (a bag given to the wrong patient, a misdirected fax, a lost device). The 60-day clock starts on the first day any workforce member (other than the person who caused the breach) knew, or with reasonable diligence would have known.

6 Card numbers and Social Security numbers

- SSNs, card numbers, driver's license numbers and addresses are personally identifiable information (PII). Collect them only when needed and never write them on scrap paper.
- Medicare cards now carry a Medicare Beneficiary Identifier, not the SSN; CMS says to protect it like an SSN.
- Card verification codes (the 3 or 4 digits on the card) may not be stored after the payment is approved, even if the customer agrees (PCI DSS, an industry rule).

MORE Who HIPAA covers, and what is not PHI

A health care provider is a covered entity only if it sends health information electronically in a standard transaction, such as a claim or an eligibility check. Federal regulations define health care to include dispensing a drug or device under a prescription, so a pharmacy that bills insurance electronically, which is nearly every pharmacy, is covered. A cash-only pharmacy that never sends a standard transaction would fall outside HIPAA, though state privacy law and board rules still apply.

MORE Disclosures for the public interest

HIPAA lists purposes for which PHI may be shared without authorization or a chance to object. Each one permits a disclosure; it does not require one. Where another law, such as a state's reporting law, requires the report, that law creates the duty. In a pharmacy, these requests are handled by the pharmacist or privacy official, with a written record, because most of them must appear in an accounting of disclosures.

For education and exam preparation only. Not medical advice; follow current guidelines and your institution's protocols. Pharm Tech Basics is an independent study aid not affiliated with any certifying body.