

# From Hallways to Inboxes

Privacy is Everyone's Business



Protecting patient privacy is more than a legal requirement; it's a commitment to respect, trust, and quality care. Each of us, regardless of role or department, has a responsibility to safeguard protected health information (PHI). Even the smallest slip, such as an overheard conversation or misdirected email, can lead to an inappropriate release of information. When we all stay alert and informed, we not only protect patient information, but also the trust our community places in us. This month, we are focusing on practical tips and best practices to recognize risks and prevent breaches before they occur.

## Watch Your Words: Keep Conversations Confidential

It's easy to let your guard down during a quick hallway exchange or an informal chat in the breakroom. However, when conversations involve PHI, they must be treated with the same level of care as written records. Conversations should only take place in private areas, away from patients, visitors, and other unauthorized staff members. Even a well-meaning update about a patient's condition can lead to inappropriate disclosure. Take a moment to assess your surroundings. If it's not private, it's not a good place to talk.

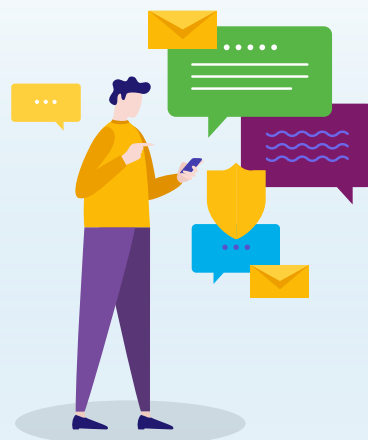
**Privacy Practice:** Step into an empty office or schedule secure check-ins for any conversations involving PHI, instead of discussing details in open areas.



## Think Before You Send: Email with Care

Email is a fast and convenient tool, but when used too quickly or without proper care, it can be a major source of privacy incidents. Before hitting send on an email containing PHI, take a few seconds to double-check the recipient's address, verify that encryption is in place, and ensure the content is appropriate. A simple typo in the email address can lead to a privacy violation with significant consequences for both the patient and our organization. Always follow the rule: check twice, click once.

**Privacy Practice:** Save commonly used, verified addresses in your contacts, and confirm that any attachments are correct before sending.



## Handle with Care: Don't Leave Paper PHI Behind

While electronic data gets much of our attention, printed materials are equally vulnerable. Whether it's lab results or discharge instructions, printed patient information can easily be forgotten on printers, fax machines, or shared desks. These documents can be easily accessed or viewed by passing individuals, resulting in unauthorized access. Make it a point to always pick up your documents immediately, verify they are in your possession before moving on to another task, and always confirm paperwork is for the correct patient before handing it over to another team member.

**Privacy Practice:** Use a cover sheet when faxing documents to add a layer of protection and indicate confidentiality.



## Know Before You Share: Verify and Validate Every Request

Handling patient requests for information, such as inquiries from family members or law enforcement, requires careful attention to privacy rules and regulations. All record requests should go through the Health Information Management (HIM) department, which is responsible for verifying authorization, ensuring documentation is complete, and processing disclosures in accordance with legal and regulatory requirements. If you're ever unsure about whether a situation qualifies as a request for records or PHI, it's always better to pause and ask before proceeding.

**Privacy Practice:** Be alert to informal requests. A passing question like, "Can you tell me how my aunt is doing?" may seem innocent, but it still requires formal release procedures.



Patient privacy isn't something we think about once and move on; it's part of our everyday responsibilities. By integrating small, careful habits into our routines, we help to create a safe environment for every patient in our care. Protecting privacy also means staying alert to risks, asking questions when you're unsure, and knowing where to turn for help. Together, we are building a security and privacy culture rooted in integrity, accountability, and respect.