





Common HIPAA Violations *and How to Avoid Them*

Insider Snooping

-  Accessing health records of patients for any reason other than treatment, payment, or healthcare operations, as permitted by the HIPAA Privacy Rule.
-  Organizations can easily identify misuse and take appropriate actions by tracking which medical records are accessed using an EHR system.





Sending Protected Health Information (PHI) to Wrong Contacts

-  Patient information is accidentally sent to the wrong person, either through mail, email, or via fax.
-  Always double check the address or phone number before reaching out to a patient with sensitive information, and verify the patient information before sharing details over the phone if the patient has called in.





Removing PHI from a Healthcare Facility

-  Emailing PHI to personal email accounts or downloading PHI onto unauthorized devices in order to access that information remotely.
-  Create clearly defined policies for accessing PHI on personal or mobile devices, and verify all employees have been educated on these guidelines.




Inadvertent Sharing


 Employees accidentally sharing sensitive patient information.

- 
- Do not share or discuss PHI with others who shouldn't have access to it, including co-workers.
 - Avoid accessing patient records unless needed for work.
 - Minimize the chances of others overhearing patient information.
 - Never leave PHI unattended.
 - Secure all paper documents containing PHI by placing in a locked drawer or cabinet when not in use.
 - Cover charts so patient names are not visible.
 - Close and log out of computer applications containing patient information.
 - Never email PHI data




Failure to Evaluate Business Associates


 Entrusting PHI with a business associate or third-party vendor that is not HIPAA-compliant.

- 
- Carefully vet all vendors and outline security and privacy expectations in detail. All third parties should undergo a thorough review before procurement, and agreements should be updated as requirements or processes change.



Failure to Perform an Organization-Wide Risk Analysis

 Irregularly performing risk analyses and an indeterminate amount of vulnerabilities to the confidentiality, integrity, and availability of PHI.

- 
- Conducting a well-planned and well-executed risk analysis benefits the whole organization. Risks that are identified during the assessment should be prioritized and addressed in a reasonable time frame.

