



Fast Facts for HIPAA Privacy

- Federal HIPAA regulations were strengthened by the **Health Information Technology and Economic Recovery (HITECH)**, signed into law in 2009. On a national level, as more charts are converted to electronic medical records, greater precautions are needed to prevent fraud and identity theft.
- **Now, fines for privacy breaches are higher, and privacy audits are more frequent.** Complaints can turn into criminal lawsuits investigated by the Department of Justice and by the Office of Civil Rights.
- **However, the HITECH Privacy Rule does not require you to obtain authorization before sharing information for treatment, payment, or operations (TPO).** Share the **minimum amount necessary** for TPO purposes. Sometimes the minimum amount may be the entire chart.
- **The Privacy Rule does not require you to eliminate all “incidental” disclosures.** Incidental means information others may overhear or see during the course of providing treatment. Reasonably safeguard and appropriately limit how protected health information is used and discussed.
- **New HITECH guidelines seek a “Harm Threshold” to be met for the definition of privacy breach.** Each privacy complaint is investigated, analyzed, and documented; however, it may not reach the definition of a privacy breach if no substantial harm resulted. For example, if a breach occurs (e.g. wrong fax) when a person inadvertently errors within the scope of their duties, and it is not further used or disclosed (e.g. wrong fax shredded), then there is no harm to patient.
- **New with HITECH, patients must be notified in writing of substantiated privacy breaches within 60 days of breach.** The letter must include: what PHI was disclosed, how it happened, all that is being done to investigate the circumstances and to prevent reoccurrence, and provide guidance about how to protect against further breach consequences. Remember, notification is necessary only when there is likelihood of substantial harm to patient as result of a breach.
- **What are the consequences of losing a laptop or CD that places more than 500 individuals’ personal information at risk of disclosure?** HITECH mandates that prominent media outlets be notified regarding breaches effecting 500+. You must notify the Secretary of Health and Human Services (HHS). HHS posts a list on the HHS website identifying the agencies involved in a breach of more than 500 individuals.
- **The Privacy Rule does not cut off communication between nurses, physicians, and the families of patients.** As long as the patient has given oral or written permission, the Privacy rule permits staff to share information with family and friends. When in doubt, document what was disclosed and for what purpose, reflecting that the disclosure serves the patient’s best interests.