

HIPAA

Health Insurance Portability and Accountability Act, a 1996 Federal law that restricts access to individuals' private medical information.

The three main purposes of HIPAA are:

- 1) To protect and enhance the rights of consumers by guaranteeing the security and privacy of their protected health information (PHI).
- 2) To improve the quality of healthcare in the U.S.
- 3) To improve the efficiency and effectiveness of healthcare delivery.

Releasing Patient Information to an Unauthorized Individual.

An authorization form must be obtained from a patient before any of their PHI can be disclosed to a third party for a purpose other than one expressly permitted by the HIPAA Privacy Rule. *Disclosing Personal Health Information* for purposes other than *IS treatment, payment for healthcare, or healthcare operations* **is a HIPAA violation** if authorization has not been received from the patient in advance. Healthcare employees must ensure that prior to disclosing PHI to a third party that authorization has been obtained from the patient and information is not disclosed to any individual or company that is not included on the authorization form. Authorization forms are only valid if they have been signed by the patient or their nominated representative.

Ignorance of HIPAA regulations **is not** considered to be a justifiable defence by the Office for Civil Rights of the Department of Health and Human Services (OCR). The OCR will issue fines for non-compliance regardless of whether the violation was inadvertent or resulted from willful neglect.

HIPAA Enforcement Rule

The HIPAA Enforcement Rule governs the investigations that follow a breach of ePHI, the penalties that could be imposed on covered entities responsible for an avoidable breach of ePHI and the procedures for hearings. Although not part of a HIPAA compliance checklist, covered entities should be aware of the following penalties.

- A violation attributable to **ignorance** can attract a **fine of \$100-\$50,000**.
- A violation which occurred despite reasonable vigilance can attract a **fine of \$1,000-\$50,000**
- A violation due to **willful neglect** which is corrected within thirty days will attract a **fine of between \$10,000 and \$50,000**.
- A violation due to willful neglect which is not corrected within thirty days will attract the maximum fine of \$50,000.

EXAMPLES OF HIPPA VIOLATIONS

- Talking about a patient to someone that does not “need to know” such as your friends, family members or strangers.
- Having a friend or family member drive you to a patient’s house.
- Posting information about a patient on social media.
- Being in a public place and talking to or about a patient on the phone where information can be heard.
- Talking about a patient to another patient.
- Taking pictures of a patient on your personal equipment/phones.
- Talking about a patient to another staff member that is not their patient and has no need-to-know information.
- Giving out information about a patient to that patient’s friends or relatives whom the patient has not given permission for release of information.