Top 5 Common HIPAA Violations

At DPH, all workforce members are required, under the HIPAA Privacy Rule, to protect and keep confidential any personal health information. HIPAA violations can result in substantial fines to a healthcare institution and provider ranging from $100 to $1.5 million. Healthcare providers can also be at risk for sanctions or loss of license.

**Mishandling of Medical information**

A very common HIPAA violation is the mishandling of patient information. We have experienced a number of privacy incidents due to staff giving documents that include **protected health information (PHI)** to the wrong patient. These PHI documents include discharge summaries, physician orders, lab requisitions, appointment slips, etc.

Please take precautions before giving PHI documents to your patients. Ask the patient to identify themselves and their date of birth to insure that you have the right patient before handing them the document.

If you inadvertently provide the PHI to the wrong patient, please request that the document be returned and immediately notify your supervisor and/or the privacy officer.

**Unauthorized access of patient information (Snooping)**

Employees accessing patient information when they are not authorized is another common HIPAA violation. Whether it is out of curiosity, spite, or as a favor for a relative or friend, this is illegal and can cost the hospital substantially in penalties.

Individuals may be subject to fines and even prison time, loss of privileges, impact to their professional license and termination of employment.

Reference to: [User Agreement for Confidentiality, Data Security and Electronic Signature](#)

**Employee disclosing patient information**

Employees gossiping about a patient to friends or coworkers is also a HIPAA violation. All staff should be mindful of their environment, restrict conversations regarding patient to private places and avoid sharing any patient information with family and friends without patient authorization.

Reference to: [C1.0 Authorization for Use and Disclosure of PHI](#)

**Lost or stolen electronic devices**

Theft of PHI through lost or stolen laptops, desktops, smartphones, and other devices that contain patient information can result in a HIPAA violation. The necessary safeguards should be put into place such as password protection and ENCRYPTION. Check with your IT support to ensure your devices are encrypted.

**Social media**

Posting patient photos and information on social media is a HIPAA violation. While it may be harmless if the patient name is not mentioned, someone may recognize the patient and know the doctor’s specialty, which is a breach of the patient’s privacy.

Any use of social media to share patient information without authorization is considered a violation of HIPAA law.

Reference to: [C12.0 HIPAA Compliance: Social Media Policy](#)

**Report a Privacy Breach:**

- Privacy Hotline: (855) 729-6040
- Email: compliance.privacy@sfdph.org
- Refer to: [B1.1 Reporting of Unlawful or Unauthorized Access of PHI](#)

The Office of Compliance & Privacy Affairs (OCPA) also provides consultation on all privacy related questions. Please feel free to contact us.