

Unauthorized Access of Patient Files – Even Your Own – Can Land You in Hot Water

By Vickie Saucedo, Director of Corporate Responsibility, and Patricia Perry-Williams, Information Security Officer

Seton is expanding audits of COMPASS user access to comply with federal rules. The audits began on Jan. 1 and will be conducted periodically.

HIPAA training is mandatory upon hire and again once a year. Abusing access can result in disciplinary action. Additionally, violators face stiff financial penalties and prison time depending on the circumstance.

CRIMINAL PENALTIES

ACTION	FINE	PRISON TERM
Obtaining/disclosing PHI	Up to \$50,000	Up to 1 Year
Obtaining/disclosing PHI under "false pretenses"	Up to \$100,000	Up to 5 Years
Obtaining/disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm	Up to \$250,000	Up to 10 Years

To avoid violating Seton access policies:

- **Do not share, copy, release, sell, loan, review, alter or destroy patient health information except as authorized by Seton policy.** Specifically:
 - Do not disclose or discuss patient health information with others, including co-workers, friends or family who are not authorized to access that information.
 - Do not access or view patient health information unless necessary to perform a required job function.
 - **Do not access patient records of family members** (including children, whether or not minors), **relatives, friends, co-workers, acquaintances, celebrities or well-known individuals** except in the normal course of performing a valid job duty. (All medical record information requests, including those related to minor children, must be made through the Health Information Management department.)
 - **Do not access your own patient record.** Associates must follow Seton's process of requesting their own medical record information through the Health Information Management department and not through COMPASS.
- Refer improper inquiries about patient health information from other personnel to your manager or a member of your chain of command.

To properly audit, Seton may log, review and otherwise use information stored on or passing through its systems to enforce our Information Security standards. Seton may also capture user activity such as websites visited.