Information Security Compliance Guidance

Tom Consalvo, SBUMC Information Security Officer

What is Information Security?

Information Security assures that systems and applications operate effectively and provide appropriate confidentiality, integrity and availability. (C.I.A.)

Why is it important?

We are federally and state mandated to adhere to both HIPAA Security and New York State Cyber Security Policies and Procedures to keep e-PHI (electronic Protected Health Information) or patient data safe.

If we do not do this fines or imprisonment may occur.

What are some forms of security breaches?

- Sharing your password
- Allowing someone to log on as you or logging them on as yourself to view restricted data.
- Leaving your session unattended while performing a task.
- Placing patient data on a local hard drive or removable media drive (CD, USB, External hard drive, etc)
- Misdirected/misdialed faxes

The effects of a security breach:

- Loss of revenue or other hospital assets
- Legal liability, including fines, criminal prosecution
- Tarnished name and bad press
- Suspension or termination

Preventing Potential Breaches:

- NEVER share your password – Treat it like your toothbrush!!
- Access ONLY the information necessary to perform your work related responsibilities.
- Do NOT snoop and do NOT discuss patient information for any purposes unrelated to treatment, payment or the health care operations of Stony Brook Medical Center.

Email Security:

- Never send Patient Data in an email.
- If you feel you must send confidential data in an email please call the help desk (4-4357), we have other options.