GHS Genesee HEALTH SYSTEM

Hope and health in the community

Genesee Health System

Corporate Compliance

HIPAA Security

Mark Childress

Chief Information Officer

Corporate Compliance
HIPAA Security

Purpose of HIPAA Security

Protected Health Information (PHI) refers to individually identifiable health information that can be linked to a particular person. Specifically, this information can relate to:

- The individual's past, present or **future physical or mental health or condition**,
- The **provision** of health care to the individual, or,
- The past, present, or future **payment** for the provision of health care to the individual.

Common identifiers of health information include names, social security numbers, addresses, and birth dates (including GHS case numbers).

Genesee HEALTH SYSTEM
Hope and health in the community

Corporate Compliance
HIPAA Security

- Do NOT share your password with ANYONE!
- **YOU are responsible for protecting your User ID and password**
- Sharing your password violates the HIPAA Security Rule and GHS policy
- Licensed health professionals might also be violating civil and/or criminal licensure law by sharing their password
- All CHIP access is tracked

Corporate Compliance
HIPAA Security

- ***Never*** log in to an EMR using someone else's User ID and password – nor use an EMR while someone else is logged in
- Logging in to an EMR with another User's ID and password, violates the HIPAA Security rule, GHS policy and maybe even **criminal law** - especially if the staff you impersonate is a doctor or other licensed health professional
- Only access PHI if you have a legitimate **job related** need to do so

Corporate Compliance
HIPAA Security

Protect the data!!!

- Update anti-virus and system files at least weekly
- Shield your screen from public view
- Do not store PHI on portable devices, unless encrypted
- Use strong passwords and do not write them down
- Do not email unencrypted PHI over the Internet
- Always be alert when online
- Use Minimum Necessary rules

Recent security lapses…

- One of the largest HIPAA violation penalties was imposed on the health insurer Premera Blue Cross. Premera Blue Cross was investigated over a data breach in which the protected health information of 10,466,692 individuals was obtained by hackers.
  - During the investigation, OCR discovered multiple potential violations of the HIPAA Security Rule. Premera Blue Cross had failed to conduct a comprehensive risk analysis, had not reduced risks to the confidentiality, integrity, and availability of ePHI to a reasonable and appropriate level, and had implemented insufficient hardware and software controls.
- In February 2017, an unencrypted laptop computer from Lifespan Health System was stolen from an employee’s vehicle. The laptop contained the ePHI of 20,431 patients.
  - OCR investigated the breach and discovered systemic noncompliance with the HIPAA Rules. Lifespan had conducted a risk analysis and determined encryption was required for its mobile devices due to the high risk of data exposure but failed to implement encryption on mobile devices. The movement of the devices in and out of its facilities was not tracked and there was no comprehensive inventory of mobile devices. OCR also found that there was no business associate agreement between Lifespan Corporation and Lifespan ACE.

Corporate Compliance
HIPAA Security

Remember - protect the data!

- Set up a secure password – and ***DO NOT*** **SHARE IT**!
- Do not EVER log in using someone else's User ID and password!
- Shield screens from unauthorized view
- Do not save PHI on portable devices, unless encrypted
- Do not email unencrypted PHI over the Internet
- Be cautious

And always ask questions if in doubt!