Preventing Security Violations at Your Facility

Svetlana Lyulkin, MBA
Director of Information Management

HealthInsight
ESRD ALLIANCE | NETWORK 18
Serving Southern California

Objectives

- Educate facility staff on how and why it is important to protect patient information.
  - Understand why emailing, mis-sending, and sending unrequested PHI/PII are security violations.
  - Identify HIPAA and CMS security regulations.
- Ensure all facility staff are accountable.
  - Learn the difference between PHI and PII
- Prevent QARM and CROWNWeb-related security violations.
- Eliminate all facility security violations.
  - Learn steps to prevent security violations at your facility.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information, and it applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and it sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their own health records and to request corrections.

Source:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Source:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

CMS System Security Policy

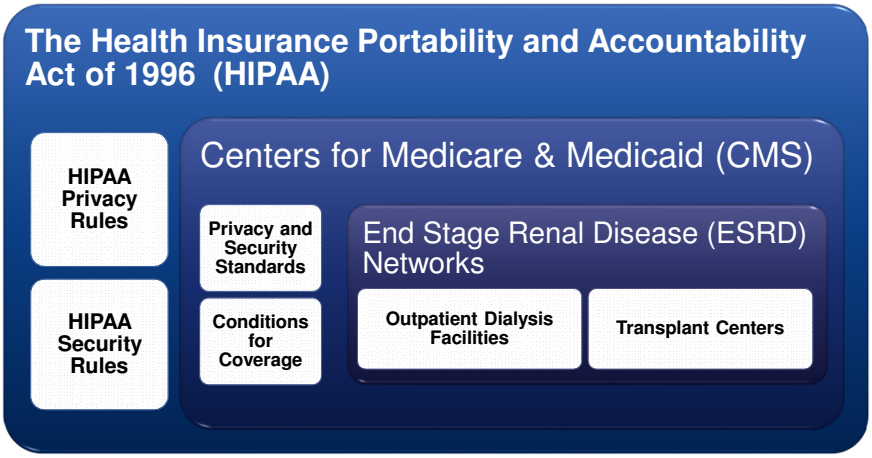
- 3.2 Quality Net Email and Internet Usage:
  - "Users are reminded it is inappropriate to reveal sensitive QualityNet Medicare information or any other material covered by existing QualityNet privacy policies and procedures on the internet. The Privacy Act of 1974, 5 U.S.C. 552A, protects personal privacy from invasion by Federal agencies and levies civil and criminal penalties for violations of the provisions of the Act. In addition, users releasing such privacy or sensitive information, whether or not the release is inadvertent, may be subject to the penalties provided in existing QualityNet policies and procedures."

CMS Security Policy (continued)

- 3.2.2 Data Storage and Transmission:
  - "It is not permissible to use the QualityNet **email resources** for transmission of QualityNet Privacy Act protected and/or other sensitive QualityNet information."
- 3.2.2.5 Sensitive Data:
  - "If you (Network 18 employee) receive an email message that discloses personal, sensitive, private date, PII/PHI or Medicare information, you **MUST** immediately report this finding to your supervisor and Security Point of Contact (*Data Director at Network 18*). The Security Point of Contact will call the QualityNet Help Desk to initiate the [security violation] report."

HIPAA, CMS, ESRD Networks, and ESRD Facilities

HealthInsight ESRD ALLIANCE | NETWORK 18



What are the Responsibilities of the Facility?

HealthInsight ESRD ALLIANCE | NETWORK 18

- Facility staff **must protect** patient information.
- Security violations can result in:
  - CMS notification;
  - Medical director involvement; and/or
  - Sanctions against facility.

What is PHI & PII?

- PHI (Protected Health Information):
  - Insurance information
  - Prescriptions
  - Medical records/forms/facility logs
- PII (Personally Identifiable Information):
  - Name/initials
  - Social Security number
  - Date of birth
  - Contact information

What are the Four Common CMS Security Violations?

- Emailed PII/PHI
- Shared QARM account info
- Unrequested PII/PHI
- Mis-sent PII/PHI

What about QARM?

- Each QualityNet Authorization and Role Management (QARM) applicant must apply through the CMS Enterprise Identity Management (EIDM) application process.
- Each QARM account holder must have his/her own:
  - Email address
  - User name
  - Password
- **Sharing any of the above will result in your account being locked or possibly disabled.**

What about CROWNWeb?

- Each patient has a unique CROWN UPI.
  - Example: 1800123456
  - Example: 2100123456
- The CROWN UPI can be safely e-mailed to the Network.

Why Emailing PII/PHI is a Security Violation

- CMS does not consider email a secure method for sending PII/PHI.
- Why are emails not secure?
  - Easy to hack into/intercept
  - Easy to mass email
  - Easy to send to wrong recipient

Why Unrequested or Mis-Sent PII/PHI is a Security Violation

- It compromises a patient's PHI/PII.
- Patient did not authorize this information to be sent to the Network.
- Unauthorized disclosure of PII/PHI is illegal.
- Patients' medical records are put at risk when sent to the wrong recipients.

What are the Effects of a Security Violation?

- Breaking HIPAA rules
- Violating patient rights
- Jeopardizing patient information
- PII/PHI ending up on the internet
- Security violation notification to CMS
- Potentially lead to facility sanctions

How Can Facilities Prevent Security Violations?

- Do NOT email PHI/PII.
- Only include the patient's CROWN UPI in e-mails.
- Never share email accounts, QARM login, or password.
- Only send what is requested.
- Confirm correct document before sending.
- Confirm correct recipient information before sending.
  - Fax number/speed dial
  - Mailing address
  - Recipient availability
- Keep all fax confirmations for reference.

Useful Resources

HealthInsight
ESRD ALLIANCE | NETWORK 18

- ESRD Network 18 website
  www.esrdnetwork18.org
- Health Insurance Portability and Accountability Act (HIPAA)
  www.hhs.gov/ocr/privacy
- CMS – End Stage Renal Disease (ESRD) Center
  www.cms.gov/center/esrd.asp
- CMS Conditions for Coverage
  www.cms.gov/CFCsAndCoPs/downloads/ESRDfinalrule0415.pdf

Log Sheet
"Preventing Security Violations"

HealthInsight
ESRD ALLIANCE | NETWORK 18

Provider # _____
Facility Name _____

Date	Name	Job Title

Update and Fax to Network 18 at 888.280.8669
Keep a copy for Facility Records

HealthInsight
ESRD ALLIANCE | NETWORK 18

Contact Information

Svetlana Lyulkin, MBA
Director of Information Management
SLyulkin@nw18.esrd.net