Southern California Renal Disease Council, Inc.
ESRD Network 18

Preventing Security Violations at Your Facility

Svetlana Lyulkin, Data Manager

Preventing Security Violations WebEx

Los Angeles, CA

October 2011

Objectives

1. To eliminate any confusion as to what information can be sent to Network 18, and what is considered a Security Violation.
   - All New & Current facility staff will learn how and why it is important to protect Patient Information.
   - Identify HIPAA & CMS Security Regulations.
2. To hold all facility staff accountable.
   - Learn what PHI/PII are.
3. To train all facility staff.
   - Understand why Emailing, Mis-sending, and Sending Unrequested PHI/PII are Security Violations.
4. To 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 and Security Rules

- **The Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and 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 health records, and to request corrections.

- **The 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.

- **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. <u>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."</u>

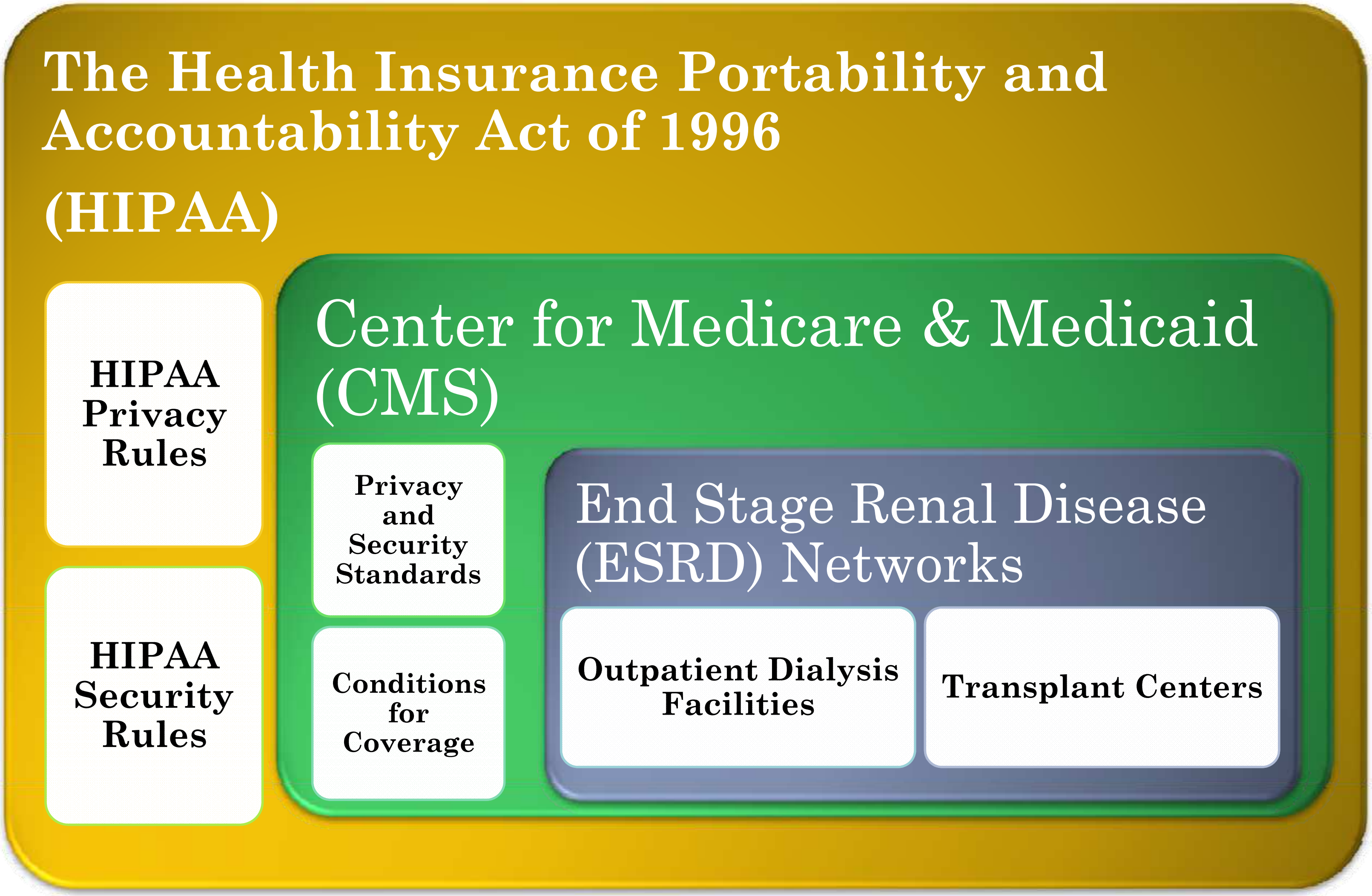
3.2.2 Data Storage and Transmission:

"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 <u>**MUST**</u> immediately report this finding to your supervisor and Security Point of Contact (*Data Manager at Network 18*). The Security Point of Contact will call the QualityNet Help Desk to initiate the [security violation] report."

HIPAA, CMS, ESRD Networks, & ESRD Facilities



The Health Insurance Portability and Accountability Act of 1996

(HIPAA)

HIPAA Privacy Rules

HIPAA Security Rules

Center for Medicare & Medicaid (CMS)

Privacy and Security Standards

Conditions for Coverage

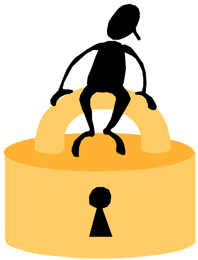
End Stage Renal Disease (ESRD) Networks

Outpatient Dialysis Facilities

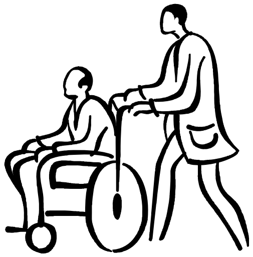
Transplant Centers

What is PHI & PII?

- **(PII) Personally Identifiable Information:**
  - Name;
  - Social Security Number;
  - Birthday;
  - Contact Information.



- **(PHI) Protected Health Information:**
  - Insurance Information;
  - Prescriptions;
  - Medical Records/Forms/Facility Logs.

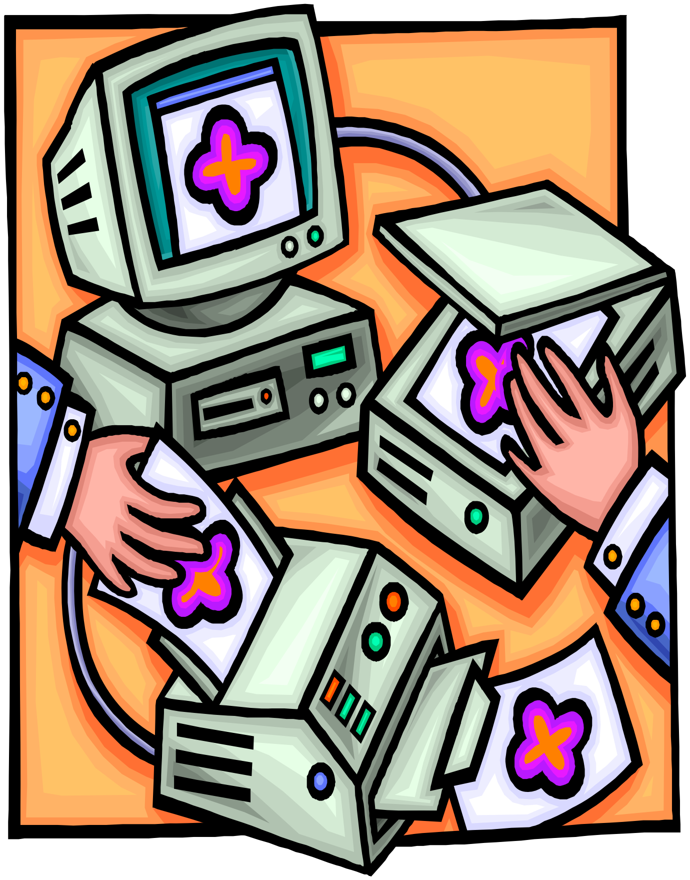


What are the Responsibilities of the Facility?

- Facility Staff **Must Protect** Patient Information.
- Security Violations can result in:
  - CMS notification;
  - Medical Director involvement;
  - Sanctions against facility.

What are the 3 Common CMS Security Violations?

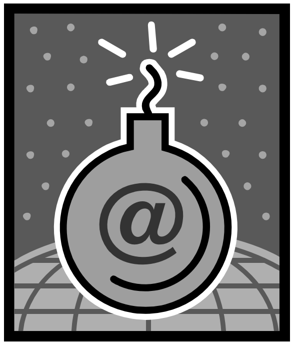
1. **Emailed PII/PHI**
2. **Unrequested PII/PHI**
3. **Mis-Sent PII/PHI**

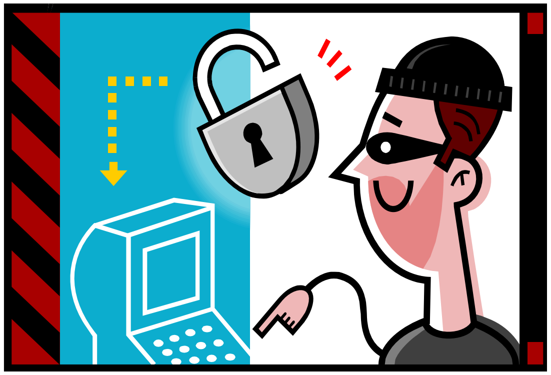


Why Emailing PII/PHI is a Security Violation

- CMS does not consider Email a Secure Method for Sending PII/PHI

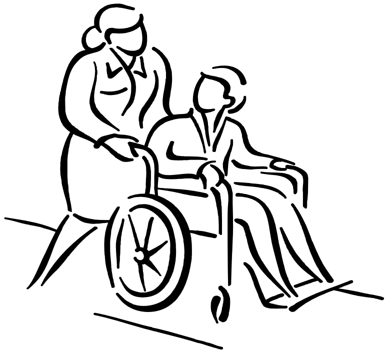
- Why are Emails Not Secure?
  - Easy to hack into/intercept;
  - Easy to mass email;
  - Easy to send to wrong recipient.

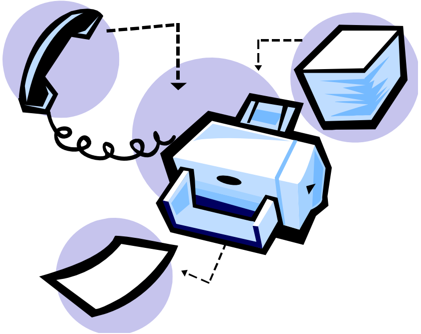




Why Unrequested or Mis-Sent PII/PHI is a Security Violation

- **It compromises a Patient's PHI/PII.**
- Patient did not authorize this info to be sent to the Network.
- Unauthorized Disclosure of PII/PHI is ILLEGAL.
- Medical records are put **at risk** when sent to the wrong recipients.





What are Common Security Violations?

- Patient Lists
- Treatments Logs
- Birth/Death Certificates
- Medical Records
- Social Security Cards
- Driver Licenses
- Insurance Cards
- Prescriptions
- Internal Facility/Hospital Forms/Calendars

DO NOT SEND IT IF THE NETWORK DID NOT REQUEST IT

What Should Facilities Send to the Network

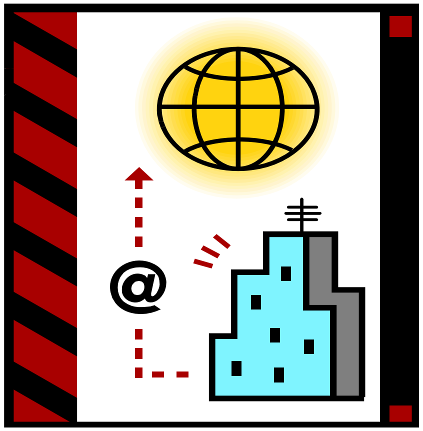
- **ONLY SEND WHAT IS REQUESTED:**
  - CMS-2728/2746 Forms;
  - Monthly PARs;
  - Monthly Fistula First Reports;
  - Other Reports **As Requested**.

DO NOT attach unrequested/supplementary documents

BY FAX OR MAIL ONLY -- NEVER EMAIL PHI/PII

What are the Effects of a Security Violation?

- Breaking of HIPAA;
- Violation of Patient Rights;
- Jeopardize Patient Information;
- PII/PHI ending up on the World Wide Web;
- Security Violation Notification to CMS;
- Can potentially lead to Facility Sanctions.



How Can Facilities Prevent Security Violations?

- Do NOT Email and PHI/PII.
- Only Send what IS REQUESTED.
- Confirm Correct Document BEFORE Sending.
- Confirm Correct Recipient Info BEFORE Sending.
  - Fax Number/Speed Dial.
  - Mailing Address.
  - Recipient Availability.
- Keep all Fax Confirmations for Reference.

Useful Resources

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

Southern California Renal Disease Council, Inc.
ESRD Network 18

Svetlana Lyulkin, MBA
Data Manager
SLyulkin@nw18.esrd.net

6255 Sunset Boulevard, Suite 2211 • Los Angeles • California • 90028
(323) 962-2020 • (323) 962-2891/Fax • www.esrdnetwork18.org

Log Sheet
"Preventing Security Violations"

Provider # ______________________

Facility Name ____

Date	Name	Job Title

Update and Fax to Network 18 at (323) 962-0127
Keep a copy for Facility Records