Data Security

Foundational Curricula:
Cluster 9: Quality, Safety & Security
Module 17: Data Protection and Security in eHealth
Unit 2: Data Security
FC-C9M17U2

Curriculum Developers: Angelique Blake, Rachelle Blake, Pauliina Hulkkonen, Sonja Huotari, Milla Jauhiainen, Johanna Tolonen, and Alpo Värri

49/60

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Unit Objectives

- Identify the current mechanisms for providing secure messaging between healthcare providers and consider how requirements may change in the future
- Describe privacy and security requirements pertaining to the retention and destruction of health records
- Describe how data encryption plays a role in privacy and security rules, policies and best practice
- Explain breaches of confidentiality
- Describe the concepts of prevention of data loss/data theft, and maintenance of data integrity
- Describe ethical and security issues including accountability of staff, healthcare providers and managers and the confidentiality, privacy and security of patient data

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Data security

- **Data security** means protecting digital data from unauthorized access and data corruption.
- Data security can be can be put into practice for example by data masking, data erasure, backups or authentication.

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

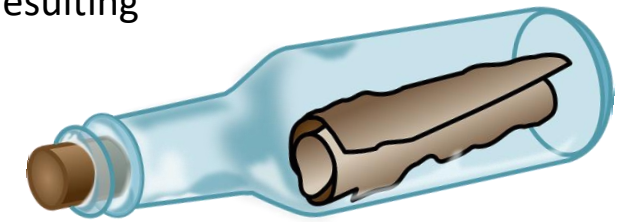
Mechanisms for Health Information Exchange

Directed Exchange ("push"):

- Describes the push of health information from a sender to a known receiver
- Generally recognized as an effective, secure and encrypted communication mechanism
- Pushed health information arrives with the recipient only after the sender initiates transfer
- Works in scenarios in which there is a known information gap and known information source

Query-based Exchange ("pull"):

- Providers access a secure record locator service to search for a patient using identifiers such as name, birthdate, address, and phone number. Audit records are maintained to identify who has accessed the patient health record.
- If information is pulled from a centralized patient health record, there is room for patients to gain more ownership over who can get access to it, resulting in a more patient-driven health information system
- Effects of moving towards a pull system of data access need to be considered carefully, as it results in a shift in the burden of responsibility



This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Retention and destruction of health records

Health records must be:

Identified in a manner that permits their accurate identification as candidates for destruction or other disposition as identified on the record retention schedule

Dated with sufficient accuracy to permit the disposition of records that have reached the expiration of their retention period

Segregated, physically in the case of paper records and discrete electronic data objects, to ensure that that objects due for destruction can be separated and disposed of without undue effort or cost

Disposed of in a legally compliant and ethical manner

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552 EUUSEHEALTHWORK

The Five Rights of Data Administration

Right Time

- Data should be available when it is needed

Right Route

- Data should be accessible regardless of the users location or device they are accessing the data

Right Person

- Ensure that unauthorized persons cannot access the data

Right Data

- Prevent unauthorized tempering or accidental corruption of data

Right Use

- Ensure only the information that is necessary is provided

(Symantec)

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Data encryption

- Data encryption means making the data unreadable unless the reader has a specific code or key to encrypt the data
- Encryption is a method to protect PHI
- HIPAA Security Rule was designed to protect electronic health data and it applies to PHI data. It relates to HIPAA Privacy Rule.

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Breaches of confidentiality

- Health care professionals need to respect their patients confidentiality
- Breaches of confidentiality in clinical practice may be caused because of carelessness, indiscretion or sometimes even maliciously
- Risk assessment of a breach (hhs.gov):
  - What kind of and the extent of the health information has been exposed and the risk of a identification of a patient;
  - Who has done the breach and to whom is the target
  - If the protected data has actually been viewed
  - How the data has been used and what it may cause

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Prevention of data loss and maintenance of data integrity

Management controls

- Long-run policy decision on how information technology shall be used in the organization
- Direction and scope of the security

Operational controls

- Address personnel security, physical security, and the protection of production inputs and outputs
- Guide the development of education, training, and awareness programs for users, administration and management
- Address hardware and software systems maintenance and integrity of data

Technical controls

- Tactical and technical implementations of security
- Access Control: passwords and two-factor authentication
- Audit trails: records who accessed information, what changes were made and when
- Encryption: information can not be read or understood without a specific code
- Firewalls, Antimalware

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552 EUUSEHEALTHWORK

Ethical issues in a digital world

Personal interaction versus spatially distributed process

- The issue is to use information that has been generated by unknown others and that has been technologically mediated, to rely on the assurance that the storage and transmission of health data does not violate their confidential nature.

Accountability and the ethics of work

- With the distributed character of ICT supported healthcare more and more actors are included.
  The notion of accountability needs to be extended to more and more workers.
- Current electronic record designs make nurses and doctors responsible for the production of standardized 'transportable' data for these multiple secondary purposes. Elaborate coding for administrative
  purposes may be in conflict with the information needed in the immediate clinical care situation. (Wagner, 2001)

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Ethical issues in a digital world (cont'd)

Standardization and 'situated action'

- The issue is that checklists and practice protocols e.g. *Patterns of symptoms* may be conducive to thinking in simple measures such as 'averages', and to synthesize data in ways that comply with images of regularity. This may reduce the tolerance for discrepancy and variation.

Expert cultures versus citizens' access to their own health data

- An issue to be considered here is about which form of access to provide. A patient reading on the screen the information the health professional enters in the system, changes the nature of the information and potentially also the situation of trust.

(Wagner, 2001)

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Unit Review Checklist

- ❑ Identify the current mechanisms for providing secure messaging between healthcare providers and consider how requirements may change in the future (RB03)
- ❑ Describe privacy and security requirements pertaining to the retention and destruction of health records (RB10)
- ❑ Describe how data encryption plays a role in privacy and security rules, policies and best practice (RB11)

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552 EUUSEHEALTHWORK

Unit Review Checklist

- ❑ Explain breaches of confidentiality (RL02)
- ❑ Describe the concepts of prevention of data loss/data theft, and maintenance of data integrity (RL05)
- ❑ Describe ethical and security issues including accountability of staff, healthcare providers and managers and the confidentiality, privacy and security of patient data (RL01)

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552 EUUSEHEALTHWORK

Unit Review Exercise/Activity

1. How you can prevent the data breaches in your position?
2. What the data breach might cause to it's target?
3. How could a patient privacy be violated as a result of the release of information?

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Unit Exam

1. If data is encrypted a person without a specific code or key cannot read it.
   a) True
   b) False
2. Data breach risk assessment evaluates
   a) Possible harm to it's target
   b) Possible harm to the person who does the breach
   c) Possible cause of the breach
   d) All of the above

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK

Unit Exam (cont'd)

3. Directed Exchange is an information exchange that provides a one-way flow of information.
   a) True
   b) False
4. Can responsibility for privacy and confidentiality be shifted to the technology?
   a) True
   b) False

This work is produced by the EU*US eHealth Work Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 727552
EUUSEHEALTHWORK