Health Information Management Basics

Foundational Curricula:
Cluster 4: Informatics
Module 6: Health Information Management
Unit 1: Health Information Management Basics
FC-C4M6U1

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

15/60

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

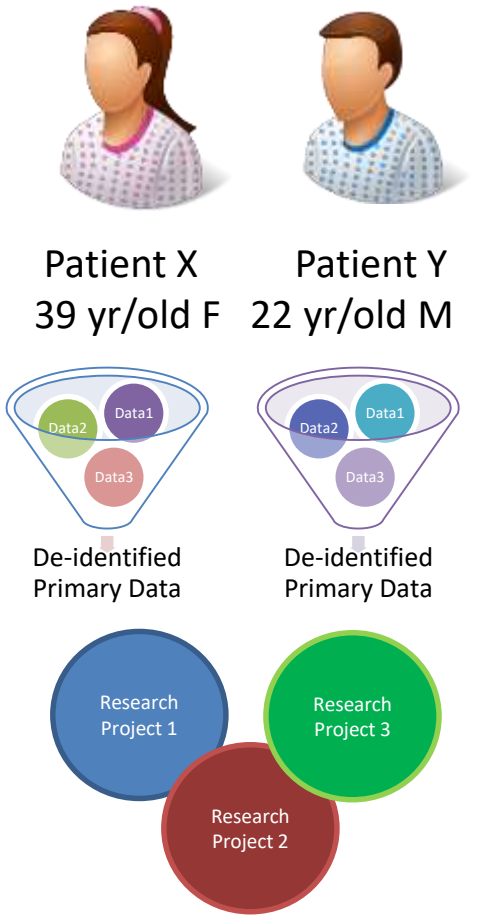
Unit Objectives

- Describe the process for locating and retrieving information in the electronic health record
- Describe consumer and patient access to electronic health information
- Identify the concepts of primary and secondary uses of health data
- Describe and identify circumstances in which health information may be used
- State the concepts of "single-sign on", activating a patient's record, and the safety precautions that need to be observed when working with multiple open applications or records simultaneously
- Identify access protocols for entry to an electronic health record
- Define protected health information (PHI)
- Explain the differences between health information and protected health information
- Explain the need to keep PHI confidential at all times, according to organizational policies and procedures

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

What is Primary Health Data?

- **Primary data**: In most cases, personal health data comes from a patient directly or from other sources on the patient's behalf, for the main reason of giving the patient health care. This is called the "primary purpose" ("primary" means "first"). This is data that is actively collected from a specific patient for a specific reason (such as a care visit or EMR entry), study or diagnosis
  - patients, providers, institutions and other data sets may be identified or may have identifiable information associated with the data
- Examples:
  - Patient data in an EMR
  - Data entered on Patient X regarding participation in a cancer drug
  - Patient Y participates in an asthma research project and does a cycling ergometry test
    - In both of these examples, the data is collected for a specific purpose, although normal health data is stored for further use
    - When the data is de-identified (any identifying data is removed), it can be utilized as ***secondary use of de-identified primary data***
    - In research studies the data is not available for third party use without asking permission (unless it has been utilized as secondary use of de-identified data)
    - Depending on regulations, personal information may be destroyed after a certain period of time (e.g., 5 years after the project is finished)



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

What is Secondary Health Data?

- **Secondary data**: Health data can also be used for secondary (additional or less essential) purposes such as health system planning, management, quality control, public health monitoring, program evaluation, or downstream research
- Sometimes health information will be “de-identified” or “anonymized” before it is used for these secondary purposes
- Secondary data is quantitative data that has previously been collected by someone else (the primary user) for a different purpose to the secondary user
- Examples:
  - censuses (lists) and statistics of patients
  - information collected by government departments
  - organizational records
  - data that was originally collected for other research purposes
    - Secondary data is often inexpensive and readily available
    - It usually includes larger sample sizes, since the data is collected in routine work

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

How Primary Data Becomes Secondary Data

- A consumer's EHR is a **primary** type of data source
- When data is taken from the health record and then used for purposes such as databases and registries, it is considered a secondary data source
  - Examples of registries include birth, cancer, or cardiac registries
- Secondary data includes original primary data that has been taken from an EHR, research project, drug study, or other primary source, that is now used to:
  - Protect and enhance public health
  - Develop security and confidentiality algorithms and test de-identification routines
  - Conduct additional research (re-use of data)
  - Develop and apply decision support for health care providers
  - Improve patient safety and quality
  - Educate and credential healthcare providers and assess training activities, etc.

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

Privacy, Confidentiality and Security of Data

- Patients are entitled to:
  - Know what data is stored
  - See and use the data when they require it
  - Know who has handled their data
  - Keep their health information private

Healthcare organizations and the workforce need to make sure data stays secured

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

Privacy, Confidentiality and Security of Data (cont'd)

- In the context of personal information, concepts of privacy are interwoven with those of confidentiality and security
- However, although privacy is often used interchangeably with the terms confidentiality and security, they have *distinct* meanings

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

Privacy, Confidentiality and Security of Data (cont'd)

- **Privacy** addresses the question of who has access to personal information and under what conditions
  - Privacy is concerned with the collection, storage, and use of personal information
  - Privacy examines whether data can be collected in the first place, as well as the justifications, if any, under which data collected for one purpose (primary) can be used for another (secondary) purpose
- **Confidentiality** safeguards information that is gathered in the context of a private relationship, such as between a healthcare provider or researcher and a patient
  - It also addresses the issue of how to keep information exchanged in that relationship from being disclosed to third parties
  - Most eHealth workers need to sign a confidentiality form upon hire
- **Security** can be defined as "the procedural and technical measures required: (a) to prevent unauthorized access, modification, use, and dissemination of data stored or processed in a computer system, (b) to prevent any deliberate denial of service, and (c) to protect the system in its entirety from physical harm" (Turn and Ware, 1976)
  - Security helps keep health records safe from unauthorized use

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

Single Sign-On

- **Single sign-on (SSO),** as you have learned in Module 2 Unit 3, is logging on and authentication to multiple independent software simultaneously with one set of credentials
- With one authentication profile, the user, an eHealth worker, logs on to several related software within a healthcare organization or enterprise, even though the software are technically independent
  - In a healthcare context, you could access, for example, patient health record and medical image record with the same user credentials
  - this can include a username and password, but in best cases includes a two-part, biometric or other type of logon including facial scan, retinal scan, fingerprint or other type of identifier or combination of identifiers
- Best practices for single sign-on, however, only allow access to multiple applications with ONE ACTIVE PATIENT at a time

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

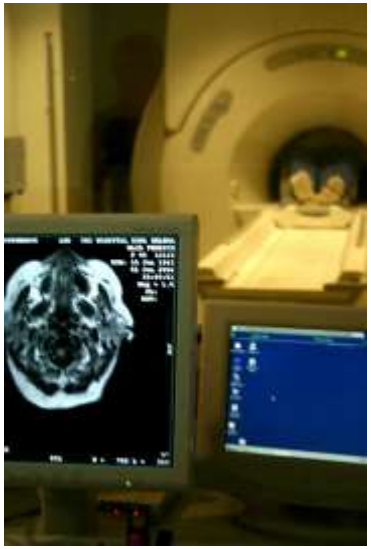
Single Sign-On

- Some benefits of SSO include:
  - no need to enter or remember multiple usernames and passwords; when two-step authentication is used, such as fingerprint and barcode, there is no need for even a password entry at all
  - assistance with compliance with different regulatory requirements, such as privacy and security measures
  - an opportunity to gain insights into when and where users spend the majority of their time, and performance and usability statistics

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

Single Sign-On (cont'd)

- However, as with any technology, some safety precautions also need to be followed when using SSO, including:
  - users should always ensure they are entering data on the correct patient, by using two-factor identification before entry into a record, and only keep one active patient open at a time
  - data should not be copied from one folder or database into another (a direct import system should be utilized for this)
  - all logs from modifications and access must be available for audit purposes
  - consider the computing power required for each file; reduce the number of files open in case of the computer crashes or re-boots



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

Activating the Patient's Record

- One always needs to ensure safety and security measures are observed when activating a patient's record
- Activating a patient's record involves:
  - Opening up a patient's account so you can work with it
  - This can be accomplished by selecting a patient directly from a list of patients, and adding the correct patient to your current patient's list
  - It can also be done by searching for a patient directly using one or more of the patient identifiers, such as name, birth date/age, gender, etc.
  - The steps for activating depend on which EMR you are using

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

Privacy, Confidentiality and Security When Accessing an EHR

- To maintain privacy, confidentiality and security in electronic health records, many protocols are followed when accessing an EHR, including:
  - **User Authentication: the verification of an active human-to-machine transfer** of credentials required to confirm a user's authenticity. This process logs the user on to the EHR and identifies the user within the record
    - for example: a nurse logs on with RFID (radio frequency identification) name badge and fingerprint, and is singly signed on to the EHR and all patient systems as Magda Berg, R.N., Unit 4, Central Hospital
  - **Audit trail**: (also called **audit log**) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event, such as the EHR

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

Privacy, Confidentiality and Security When Accessing an EHR (cont'd)

- **Firewall**: a network security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic. A firewall acts as a barrier between a trusted network, such as that which contains the EHR, and an untrusted network.
- **Encryption:** the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor

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

Health Information Versus Protected Health Information

- **Health information** means "any information, whether oral or recorded in any form or medium, that
  a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care **clearinghouse,** or an agency or organization which processes or facilitates the processing of health information received from another entity; and
  b) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."

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

Health Information Versus Protected Health Information (cont'd)

- Individually identifiable health information is a subset of health information. This type of health information identifies the individual or there is a reasonable basis to believe it can be used to identify the individual.
- The foremost example of identifiable health information is **protected health information (PHI)**. For example, a medical record, laboratory report, or hospital bill would be PHI if information contained within it includes a patient's name and/or other identifying information, including demographic information such as birthdate, address, etc.
  - When health information is de-identified, it is no longer protected health 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

Health Information Versus Protected Health Information (cont'd)

- Protected health information (PHI) means health information that is individually identifiable
  - Before doing research, the dataset that contains PHI is cleansed so that no individuals can be recognized by looking at the data:
    - Names and social/country/passport identifiers are replaced with an randomized identifier
    - Full birth date is replaced with day and month, measurements are removed, etc.
- De-identification is different than anonymization: D**e-identification** associates the link or key to a secure location, and the de-identified data can be passed forward to researchers for further scientific use. Anonymization means deletion of personal identifiers without a link to the original 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

Unit Review Checklist

- ❑ Described the process for locating and retrieving information in the electronic health record (AB03)
- ❑ Described consumer and patient access to electronic health information (AB02)
- ❑ Identified the concepts of primary and secondary uses of health data (AB01)
- ❑ Described and identified circumstances in which health information may be used (GL02)
- ❑ Stated the concepts of "single-sign on", activating a patient's record, and the safety precautions that need to be observed when working with multiple open applications or records simultaneously (AL04)
- ❑ Identified access protocols for entry to an electronic health record (AL01)
- ❑ Defined protected health information (PHI) (UL01)
- ❑ Explained the differences between health information and protected health information (AL03)
- ❑ Explained the need to keep PHI confidential at all times, according to organizational policies and procedures (AL02)

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. Name three examples of secondary data
2. Describe the patients rights in personal health data
3. Explain the single sign-on (SSO) process

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. Primary data can be best defined as:
   a) data collected during a SOAP review at a patient's first appointment
   b) data collected from Patient Mary B. as part of a new diabetic drug study
   c) The data of Patient Mary B., which may be given to registries, researchers, and others, to be used by for a different purpose than the original use
   d) data used for other purposes than those originally given to the original researcher
2. Secondary data can be best defined as:
   a) data collected from a family member in an emergency
   b) data collected from Patient Johannes B. during a sleep study
   c) de-identified data collected from Patients Mary B. and Johannes B. and aggregated into a new collection of data regarding populations in Europe
   d) data contained within Patient Mary B.'s and Patient Johannes B.'s electronic health records

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. Which of the following statements is true?
   a. Privacy of health records helps organizations determine which data can be collected on a patient
   b. Privacy of health records relates to the technical and mechanical measures required to keep a record safe
   c. Confidentiality statements are rarely required for eHealth workers
   d. Security measures include open dissemination of identified primary patient data to third parties with or without consent
4. Which of the following events occur during a single-sign on to a hospital's enterprise system?
   a. A single computer application is opened
   b. A username and six-digit password are always required
   c. Each application is accessed after a sequenced but separate logon
   d. You are simultaneously logged on to independent but linked software programs

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)

5. A software-based security system that uses rules to control incoming and outgoing network traffic describes which of the following terms?
   a. user authentication
   b. audit trail
   c. firewall
   d. encryption

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