### Information/Data Governance Project

HIMT 2150 Healthcare Statistics Andrew Bruce Watkins

### **Outline**

- 01. Explain the purpose of data/information governance in healthcare.
- 02. List the **eight principles of data governance.**
- 03. Explain the **principle of accountability** and the **importance of audits.**
- **04**. Explain the **principle of transparency**.
- 05. Explain the **principle of integrity.**
- **06**. Explain the **principle of protection**.
- **07**. Explain the **principle of compliance**.
- 08. Explain the principle of availability.
- 09. Explain the **principle of retention.**
- 10. Explain the **principle of disposition.**

The purpose of data/information governance in healthcare.

### **GOVERNANCE**

is defined as

"the action or manner of governing, relating to the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions."

O1 The purpose of **data/information governance** in healthcare.

- → Information/data governance is defined by AHIMA as "the overall management of the availability, usability, integrity, and security of the data employed in an organization or enterprise."
- → Information that is **complete**, **current**, and **correct** is necessary for any healthcare organization to achieve its goals. Enactment of an **information governance program** indicates an organization's engagement with its information as a vital resource.

#### **Information Governance:**

- Improves quality of care, patient safety, and population health.
- Increases operational efficiency and effectiveness, and reduces costs and risk.
- Helps manage and control information by supporting the organization's activities and ensuring compliance with its duties.
- Establishes policy, prioritizes investments, values and protects information assets, and determines accountabilities for managing information.
- Promotes objectivity through robust, repeatable processes insulated from individual, organizational, political, or other biases, and then protects information with suitable controls.
- By following **IG** principles, organizations conduct their operations effectively, while ensuring compliance with legal requirements and other duties and responsibilities.

### O2 The **eight principles** of **data governance**.

- → THE PRINCIPLE OF **ACCOUNTABILITY**
- → THE PRINCIPLE OF **TRANSPARENCY**
- → THE PRINCIPLE OF **INTEGRITY**
- → THE PRINCIPLE OF **PROTECTION**
- → THE PRINCIPLE OF **COMPLIANCE**
- → THE PRINCIPLE OF **AVAILABILITY**
- → THE PRINCIPLE OF **RETENTION**
- → THE PRINCIPLE OF **DISPOSITION**

The principle of accountability and the importance of audits.

03

### **ACCOUNTABILITY**

is defined as

"being called to account for one's actions."

- In leadership roles, **accountability** refers to "the acknowledgment and assumption of responsibility for actions, products, decisions, and policies including the administration, governance, and implementation within the scope of the role or employment position and encompassing the obligation to report, explain and be answerable for resulting consequences."
- **The principle of accountability**, as pertains to information governance in healthcare, refers  $\rightarrow$ to the duty of an organization to appoint a senior leader to supervise the information governance program and assign information management duties to qualified employees.
- **Audits** are an important part of accountability as they represent the organization's  $\rightarrow$ commitment to meeting its obligations to both internal and external parties. Audits help guide the organization towards continued improvement in the pursuit of its goals.

## The **principle of transparency**.

04

### **TRANSPARENCY**

is defined as

"the condition of being transparent."

- → In terms of behavior, **transparency** is defined as "operating in such a way that it is easy for others to see what actions are being performed."
- The principle of transparency, in terms of information governance in healthcare, refers to the duty of an organization to document its information governance operations such that they are capable of being proven as true or real. The documentation generated by these operations must be accessible, within reason, to its employees as well as any requisite individuals or groups requiring them.
- The importance of maintaining organizational **transparency** cannot be overemphasized. As the IGPHC states, "the clearest and most durable evidence of the organization's operations, decisions, activities, and performance are its records and information."

## The principle of integrity.

05

### **INTEGRITY**

is defined as

"the quality of being honest and having strong moral principles; moral uprightness."

→ The principle of integrity, with regards to information governance in healthcare, refers to the duty of an organization to establish an information governance program that can maintain the authenticity and reliability of that organization's information. As stated by AHIMA's IG Task Force, "integrity of information is directly related to the organization's ability to prove that information is authentic, timely, accurate, and complete."

- The degree to which the **integrity** of an organization's information can be trusted depends on many factors, including:
  - duties and techniques for managing externally-sourced information
  - adherence to IG policies in the pursuit of legal and regulatory compliance
  - adequate employee training with regard to compliance
  - maintaining consistency in how information governance is carried out
  - implementing sufficient auditing and quality assurance programs.

## The **principle of protection.**

### **PROTECTION**

is defined as

"the action of protecting someone or something; the state of being protected."

- The principle of protection, in terms of information governance in healthcare, refers to the duty of an organization to insure that its information is guarded against corruption, loss or a breach, from its creation through retention and final disposition. The protection of this information must include systems and processes that meet the standards of pertinent laws, regulations, and an organization's policies.
- → It is of utmost importance that the organization's policies define and implement effective safeguard measures to maintain and protect their information. Compliance must be monitored and audits of the organization's storage and access processes must be performed.

## The principle of compliance.

07

### **COMPLIANCE**

is defined as

"the action or fact of complying with a wish or command."

- **The principle of compliance**, as pertains to information governance in healthcare, refers to the duty of an organization to comply with laws, regulations, standards, and organizational policies that regulate the maintenance and management of health information and/or other organizational information.
- Adhering to **the principle of compliance** influences processes for information management and governance such that an organization's integrity and legal standing rest upon its ability to demonstrate that it conducts its activities in a lawful manner and manages information risks effectively. The absence of information, or poor quality of information required to demonstrate this damages an organization's credibility and may impair its standing in legal matters or jeopardize its ability to conduct business.

# The **principle of availability.** 08

### **AVAILABILITY**

is defined as

"the quality of being able to be used or obtained."

- → As defined by AHIMA, **availability** is "the extent to which information is available, whenever and wherever it is needed."
- The principle of availability, with regards to information governance in healthcare, refers to the responsibility of an organization to manage information in a manner that ensures timely, accurate, and efficient retrieval. The way in which an organization manages its information has a significant impact on the customers' trust in the information, as well as the organization's operations.
- → Successful application of **the principle of availability** depends on an organization's ability to attend to many different demands, including data storage, interoperability, vendor relationships, employee turnover, metadata utilization, backups/conversion/migration, and routine disposition.

### The principle of retention.

09

### RETENTION

is defined as

"the continued possession, use or control of something."

- As defined by AHIMA, **retention** includes "the mechanisms for storing records, providing for timely retrieval, and establishing the lengths of time that various records (and/or) information (sets) will be retained by the healthcare organization."
- → **The principle of retention**, in relation to information governance in healthcare, refers to the obligation of a healthcare organization to maintain its information for the appropriate amount of time. Information records an organization's operations and is essential to effectively managing the organization. The maintenance of the information should consider the legal, regulatory, fiscal, operational, risk, and historical requirements.
- → The principle of retention includes the capability to properly retain relevant information, the capability to retrieve and access information, to control information volume through a well-defined information retention program, and the scheduled disposal of information once the retention period expires.

## The principle of disposition.

10

### **DISPOSITION**

is defined as

"the act or the power of disposing or the state of being disposed"

- In relation to the law, **disposition** is defined as "the action of distributing or transferring"  $\rightarrow$ property or money to someone, in particular by beguest."
- **The principle of disposition**, in terms of information governance in healthcare, refers to the  $\rightarrow$ duty of a healthcare organization to appropriately and securely dispose of information that it is no longer required to store or maintain, in accordance with the applicable laws and the organization's own policies.
- $\rightarrow$ This principle applies most importantly to protected health information such as patient health records and data. It also applies to many other types of information the organization might keep such as human resource information, financial records, and agreements. In addition, the organization should document and certify its disposition process. One of the few instances where the process of disposition should be halted is if the possibility of litigation or a regulatory action is anticipated.

HIMT 2150 Healthcare Statistics Andrew Bruce Watkins