Office for Civil Rights, HHS
National Institute for Standards and Technology
Conference
Safeguarding Health Information:
Building Assurance through HIPAA Security

Data Integrity in an Era of EHRs, HIEs, and HIPAA: A Health Information Management Perspective

Dan Rode, MBA, CHPS, FHFMA
Vice President, Advocacy and Policy
American Health Information Management Association

AHIMA

Data Integrity: What we'll cover

- What is "data integrity" in healthcare?
- How does data integrity fit with EHRs, HIEs, and HIPAA?
- Data flow in a provider organization
- Data from external sources
- Data within an organization (enterprise) system
- Enter the Consumer (Patient)
- Data to external sources
- Conclusions
- Questions

AHIMA

Achieving Data Integrity: AHIMA

- 84-year old non-profit association of health information management (HIM) professionals
- Offering Eight professional credentials
- 64,000 + members/ 40 employer types/ close to 120 different functions related to HIM and informatics
- HIM: collection, abstraction, coding, reporting, transfer, storage, analysis, and protection of health information
- Standards for: data collection, use and exchange, classifications and terminologies, privacy and security, and education of the profession

AHIMA

Achieving Data Integrity: AHIMA

- <u>Active in issues related to:</u>
  - Clinical data and documentation
  - Implementation of ICD-10-CM/PCS classifications
  - Adoption, implementation, and effective use/ management of electronic health records, and health information exchange
  - Confidentiality, privacy, and security of health information wherever it exists
  - HIM workforce education
  - Health Information Management Profession recognition

AHIMA

Achieving Data Integrity: AHIMA

Principles:

- **The Individual**
- **Data Integrity**
- **Data Confidentiality**

- ***Quality health through quality data***

AHIMA

Data Integrity: What is "data integrity?"

- "Trustworthiness of information over its entire life cycle" – Wikipedia
- Data reflects the "what" from beginning to end
- From onset (encounter, visit, admission) to primary and secondary uses of the same data
- As data structure might change, the data continues to reflect the what.
- Uniform, trustworthy, complete, unchanged meaning, secure

AHIMA

Data Integrity: EHRs, HIEs, and HIPAA

§164.304 – Definitions:

"Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner."

AHIMA

Data Integrity: EHRs, HIEs, and HIPAA

§164.306 Security standards:

General rules.

(a) ***General requirements. Covered entities must do the following:***

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

AHIMA

Data Integrity: EHRs, HIEs, and HIPAA

<u>§164.308 Administrative safeguards;</u>

(a) A covered entity must, in accordance with §164.306: (1)(i) ***Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations. (ii) Implementation specifications: (A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.***

AHIMA

Data Integrity: EHRs, HIEs, and HIPAA

<u>§164.312 Technical safeguards</u>:
A covered entity must, in accordance with §164.306:
(c)(1) ***Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.***

(e)(1) ***Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.***
(2) ***Implementation specifications:***
(i) ***Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.***

AHIMA

Data Integrity: EHRs, HIEs, and HIPAA

§164.314 Organizational requirements:

(2) ***Implementation specifications (Required).***
(i) ***Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will—***
(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

AHIMA

Data Integrity: EHRs, HIEs, and HIPAA

§164.314 Organizational requirements.

(2) ***Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—***

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

AHIMA

Data Flow In Provider Organizations: Transitioning

Notes

↓

Records (limited standards)

↓

Hybrid: Paper & Electronic

↓

Electronic

↓

Electronic (standards*)

Privacy and Security

Confidentiality

* Transactions, Terminologies/Classifications, and Meta Data

Achieving Data Integrity: Information Flow

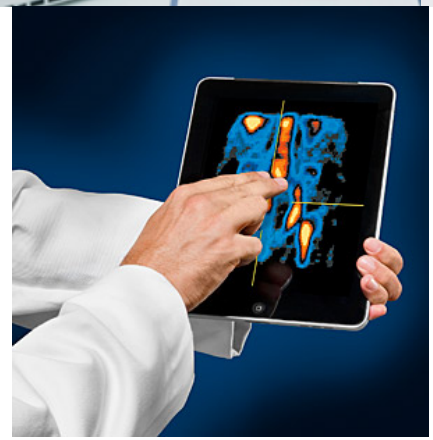
- Treatment or diagnostic service
  - complaints/orders & testing/treatments
- "Recording*" of notes/orders/results/discharge
- Collection and storage of information
- "Primary data," used for care & decision making

-- - - -

- Data exchange for "outside" care/referrals
- Public Health and other data collections or research
- Reimbursement

AHIMA

Data Integrity: Information Flow



AHIMA

Data Integrity: Documentation Challenges

Age-old issues:

- What to collect?
- How to collect it?
- How to use it?
- Who wants it?
- Who can I give it to?
- How long do I keep it?

Data Integrity: Documentation Questions

- What to collect?
  - The information I need to treat/diagnose.
  - The information my colleagues need.
  - The information a referral may need.
  - The information I may have to give for external purposes:
    - reimbursement
    - quality / quality measurement
    - public health
    - population health
    - research
  - Patient / Consumer
- Information I need for quality care!

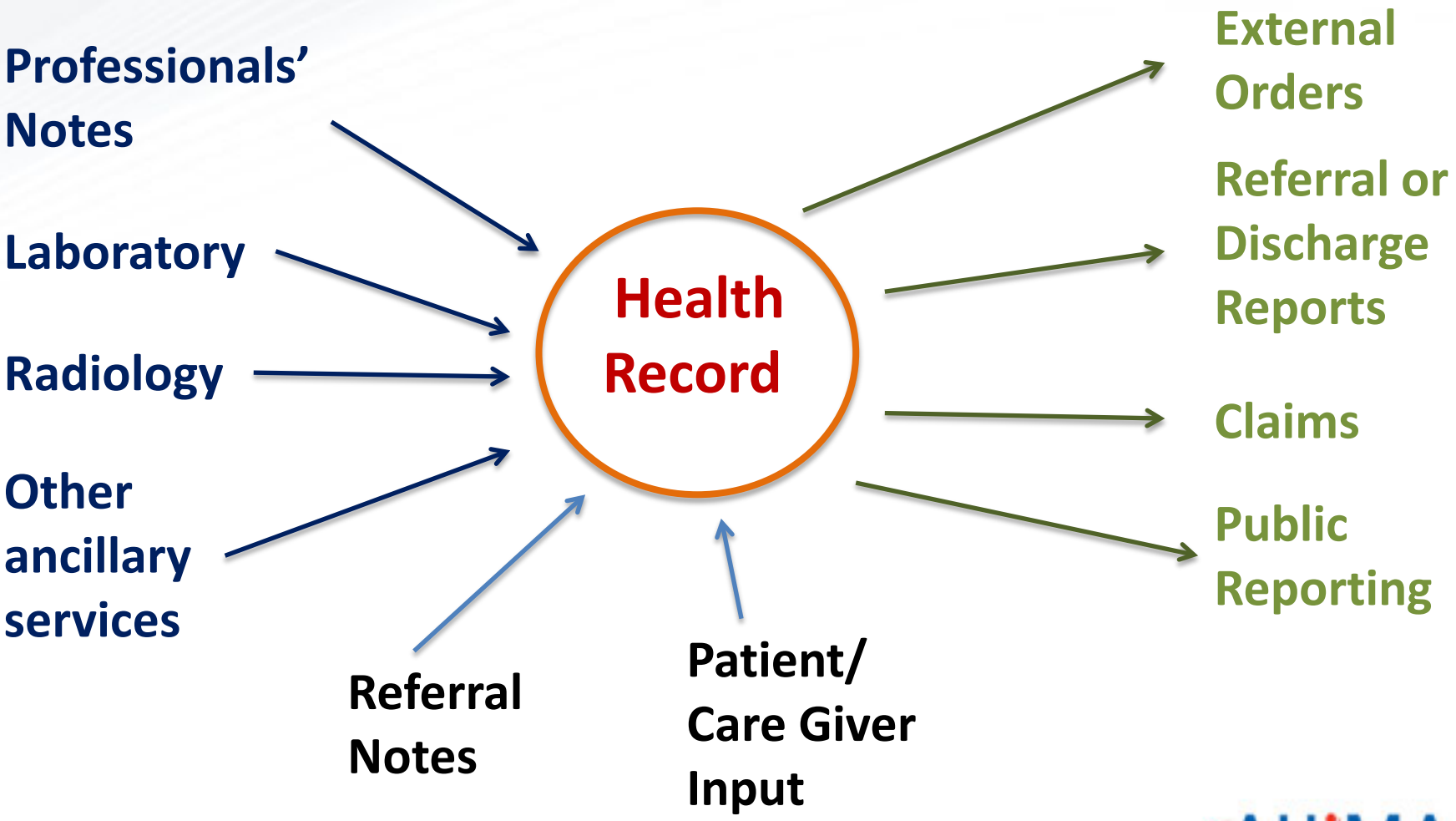
AHIMA

Data Integrity: Documentation

- How to collect it?
  - Hand written notes
  - Dictation
  - Scribe
  - Concurrent recording
  - Formats (electronic)

Innovation!!!

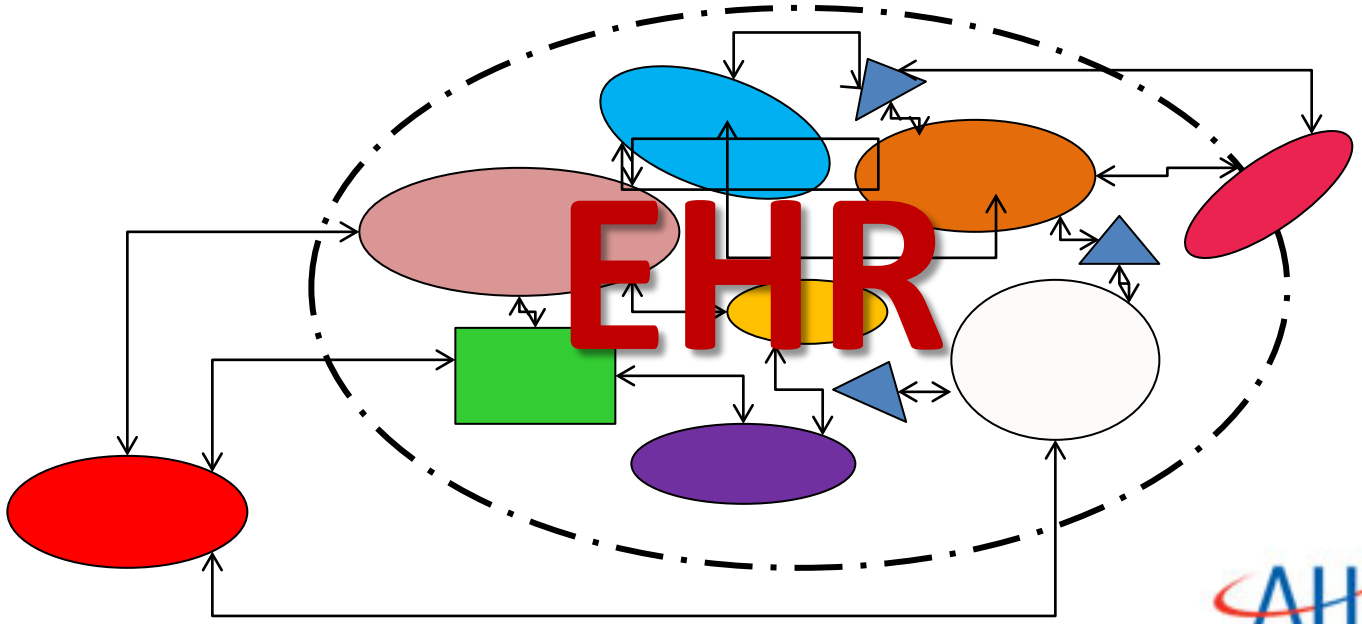
Data Integrity: Collection



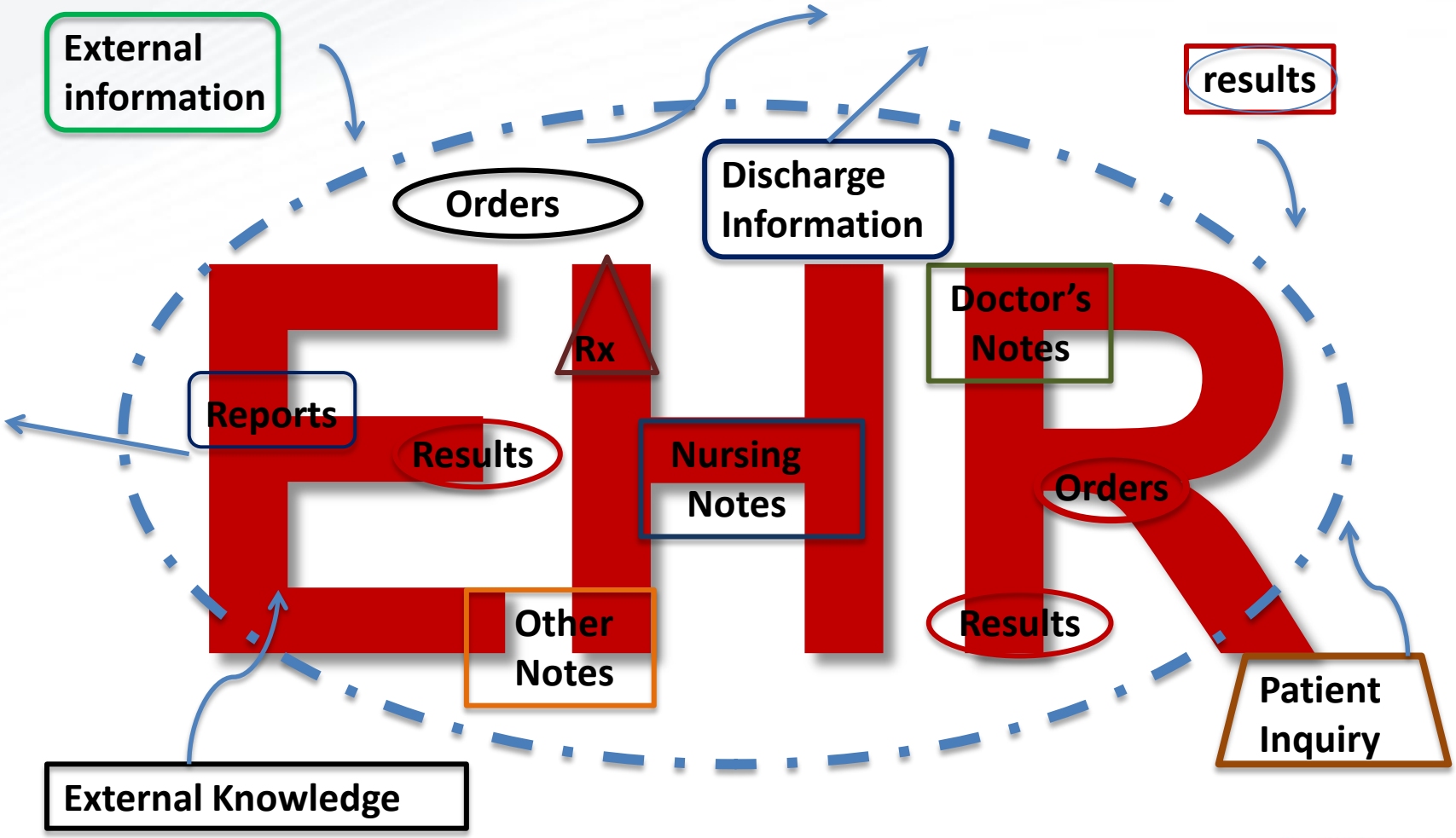
AHIMA

Data Integrity: Collection

- Electronic order entry
- Electronic health records <u>systems</u>
  - Hybrid systems
  - "Collect once use many times"
  - Enterprise or local
  - Integration
    - Where did the data come from?



Achieving Data Integrity: Collection



AHIMA

Data Integrity: Traditional Data Use

- Primary Care
- Referrals
- Claims:
  - Diagnostics and procedures
  - Parts of the record for “more” information
  - The entire record
  - Special Reports
  - Quality measurement reporting
- Public health
- Research
- Longitudinal data (?) and links

AHIMA

Data Integrity: EHR Data Use

- Primary Care
  - Decision support/analysis
- Referrals (standard reports or e-mail)
- Claims:
  - Diagnostics and procedures (expanded)
  - Attachments (parts (?) of the record) - 2016
  - Special reports (format or standard)
  - Quality measurement reporting
- Public Health
- Patient reports (standards)
- Analytics
- Decision support
- Registries and research

Data Integrity: Secondary Data Use

- Claims (HIPAA Standards)
  - Administrative data
  - Diagnoses and Procedure Codes
    - ICD-10, ICD-9-CM, CPT®
- Referrals (standard reports or e-mail)
- Quality measurement reporting
  - Treatment standards?
- Public Health reporting
- Health agency reports (analytics)
- Research
  - "Breakthroughs" – treatment standards
- "Meaningful Use" requirements

AHIMA

Data Integrity: Healthcare Data Standards

- Transaction Standards:
  - Administrative
    - US began using paper standards in 1970s
    - Electronic standard development began in 80s
    - Use of standards ➔ industry councils
    - HIPAA 1996 Legislation
    - HIPAA first proposed rule 1999 – 2002/2003
    - 8 of 10 Original HIPAA standards
    - ACA 2010 required uniform use of standards now underway!

Data Integrity: Healthcare Standards

- Transaction Standards:
  - Clinical
    - Internal communications – Health Level Seven
      - Various standards as needed 1987
    - 2003 President Bush State of the Union
      - HHS Secretary Thomas – standard EHR
  - Global Standards
    - HL7
    - ISO (215)
    - Pharmacy
    - Dental
    - Etc.,
    - And more to come

AHIMA

Data Integrity: Healthcare Standards

- Vocabulary Standards:
  - Common language across sites of services and geography
  - Classifications
    - World Health Organization (WHO) Family of International Classifications (FIC)
    - International Classification of Diseases
      - Turn of the 20th century
      - ICD-9-CM
        - Developed mid-70s use began 1979

AHIMA

Data Integrity: Healthcare Standards

- Vocabulary Standards:
  - Classifications
    - ICD-9-CM
      - Developed mid-70s use began 1979
      - CM (clinical modification-US)
      - Vol. 1&2 diagnoses Vol. 3 IP procedures
    - ICD-10
      - Developed by WHO-FIC in late 1980s based on US ICD-9-CM and ready 1991
      - Used by most industrial and many 3rd world countries

AHIMA

Integrity: Healthcare Standards

- Vocabulary Standards:
  - Classifications
    - ICD-10 used in US for mortality coding - 1999
    - ICD-10-CM and ICD-10-PCS
      - PCS: procedure classification system – developed in mid-1990s
      - CM: diagnoses clinical modification – developed in mid-1990s ready 1998
      - Both classifications updated yearly by HHS
      - Delayed implementation for many reasons
      - Final Rule 1/16/2009-effective 3/17/2009

AHIMA

Data Integrity: Healthcare Standards

- Vocabulary Standards:
  - Classifications
    - There are other classifications
    - International Classification of Functioning, Disability and Health (ICF)
    - Classifications allow the transmission of key information that is understood by all users without having to transmit major sections of the record.
    - Require uniform guidance

AHIMA

Data Integrity: Healthcare Standards

- Vocabulary Standards:
  - Terminologies
    - Machine language at a very granular level
    - Converts documentation into machine language but in a uniform manner
    - Systematized Nomenclature of Medicine--Clinical Terms International Classification of Functioning, Disability and Health (ICF) or SNOMED-CT
    - American College of Pathology transferred to
    - International Health Terminology Standards Development Organization (IHTSDO)

AHIMA

Data Integrity: Healthcare Standards

- Vocabulary Standards:
  - Terminologies
    - SNOMED-CT®
    - Laboratory reporting standards LOINC
    - Over 100 terminologies in US
    - National Library of Medicine (NLM "maps" or harmonizes several terminologies as well as terminologies and classifications

AHIMA

Data Integrity: Healthcare Standards

- Vocabulary Standards:
  - META DATA
    - Data behind the data
      - Who was the source of the data?
      - How old is the data?
      - What type of data is it?
      - Are there restrictions on the data?
      - Was the data modified?
      - Who touched the data?
    - Essentially no vocabulary exists.

AHIMA

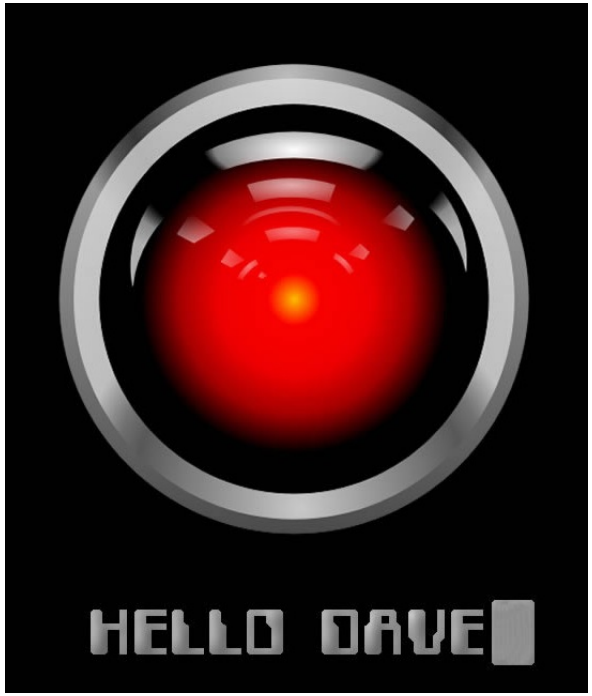
ata Integrity: Healthcare Standards

- Vocabulary must be based on standards in order to allow for interoperability.
  - Terminologies
  - Classifications
  - Meta Data
- "Translations" usually mean variation
- Data exchanged, internally or externally – allows for many uses, but with out standards cannot be trusted.
- Assuming the US moves ahead with the adoption and use of terminologies, classifications, and meta data we will have an electronic interoperable system

AHIMA

Data Integrity: Healthcare Standards

- There is still room for error even with standards
- Systems software must be tested and audited
- Vocabularies need to expand and be uniformly modified
- Vocabularies need governance and acceptance
- Moving to global classifications allows for more benefit to all nations and to the health of the world's population



AHIMA

Data Integrity: Healthcare Standards

- While it is important to have standard transaction standards, for data integrity we must standardize both the transaction standards and the vocabulary standards to provide:
  - patient safety
  - record legality or evidentiary support
  - accurate pubic health reporting
  - larger research analysis
  - better application of (UNIFORM) privacy rules and security applications
  - transfer of data to other systems

AHIMA

Achieving Data Integrity: Security

- Security became important with HIPAA
- HIPAA security rules permitted flexibility
- Security rules are more than just locking the data up or encrypting data/records.
- Security is providing protection <u>and back-up</u> for data and information
- Security is more than just systems – it also means addressing the people component of any system.
- Security is authentication.
- Security is testing
- Security includes matching data

AHIMA

Achieving Data Integrity: Privacy

- Without trust the health record will never be complete and the integrity of the data could be questioned.
- Trust will not be given unless there is no fear that the data could be used against the individual.
- We must address any inappropriate discrimination through the access to medical information no matter where the information or data exists.
- We must address any intentional or unintentional misuse of health information.
- When do we start?

AHIMA

Data Integrity: Flow From External Sources

Data can flow (goal?) from external sources

- Health Information Exchange Organizations (HIEOs)
- Referring and referral sources
- "Other" ACOs? – Medical Homes?
- Public health and similar federal/state/local agencies
- Information sources
- Patients

Data Integrity: Flow To/From External Sources

- Compatibility
  - Transaction standards
  - Vocabulary standards
  - Translations?
  - Exchange notification (receipt)
  - Sequestering obligations and notification

AHIMA

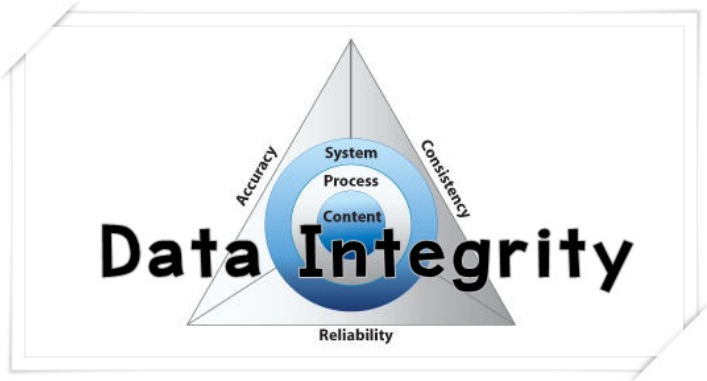
Data Integrity: Flow/To From External Sources

- Mechanisms
  - HIE
  - e-Mail
  - Enterprise system
  - Portals
  - Other – e.g. flash drives
  - HIEO data bases
  - Cloud computing?

AHIMA

Data Integrity: Flow/To From External Sources

- Identity and Security
  - Sender identity – authentication
  - Data stamping – meta data (standards?)
  - Storage and usability
    - Portal storage v EHRs?
  - Break the glass – follow-up with sender
  - Future use questions



AHIMA

Data Integrity: Enterprise/Organization Systems

- Providers data
  - Primary and secondary sources
  - ACOs
  - Administrative v clinical
  - External sources
- Validity/Integrity with in the system?
- Internal resource? Analysis? Decision support?
- Legal record (primary provider/enterprise)
  - Federal and multi-state requirements
  - Privacy and security implementation and compliance
- Data management v system management – data data governance

AHIMA

Data Integrity: Enter the Patient/Consumer

- Patient
  - Consumer
  - Caregiver
  - Other providers
  - External sources

Variances

- Information variation
- ACCESS!!!
  - Portals
  - Web sites
  - Personal Health Records (PHEs)
  - Compatible media
  - Privacy & security requirements
  - Understanding

AHIMA

Data Integrity: Data to External Sources

- Compatibility and standards issues
- Authentication and receipt
- Data configuration
  - *"collect once; use many times"*
- Data requirements – data v formulas
- HIPAA Standards and Coding Guidelines
- Translators
- Mapping
- Third Party Users
- Business Associates
- External privacy and security requirements
- Understanding of data use

AHIMA

Data Integrity: Conclusions

- Without data integrity – why bother friend?
- The use of standards is absolutely necessary to maintain integrity and make the data useful.
- Organizations (providers and others) must establish a data governance strategy and process to ensure data integrity and conformity as well as to facilitate confidentiality (privacy and security)

AHIMA

Data Integrity: Conclusions (continued)

- As an industry and community (government) we must:
  - establish public/private governance over standards of all kinds
  - adopt uniform:
    - privacy rules and regulation (across geographic lines)
    - authentication requirements across healthcare entities including patients/care givers
    - education on the use of data and how it benefits the patient, provider, and the community
    - technology and processes to meet patient access and privacy requirements.

AHIMA

Data Integrity: Conclusions (continued)

- As an industry we must:
  - Innovate to deal with the issues of data capture that ensures integrity, without significant burden to the provider
    - Let's innovate at the front end of the process as well as the back end!
  - Recognize the merger of clinical and administrative data – don't change the data!

AHIMA

Data Integrity: Conclusions (continued)

- As individuals and colleagues we must never forget:
  - Our goal is to ensure that proper and necessary health information is correct, accurate, complete and available to patients and their providers at any time in a uniform and understandable format and protected from inappropriate use, or discrimination against the patient, or their family.

AHIMA

Data Integrity: Questions

Dan Rode, MBA, CHPS, FHFMA
Vice President, Advocacy and Privacy
American Health Information Management Association
1730 M Street, NW, Suite 502
Washington, DC 20036
dan.rode@ahima.org
www.ahima.org

AHIMA