Nebraska Hospital Association

NHA Data Governance Guide

Nebraska Hospital Association Health Information & Data Council

First Edition: 6/21

A letter from the NHA Data Council

Dear Healthcare Leaders,

If your organization is anything like ours, we are inundated with data. It is created or comes from various sources. It is used for various purposes. It is stored in various places. The data elements may even have different definitions. It is insidious as it continues to accumulate on our desktop devices and our servers. But here is the question: How do we manage all of that data? How do we use it? Are additional data elements needed? How do we store it? How long do we keep it? How and when do we destroy it?

These are questions that I have been struggling to answer for our organization. As I studied this dilemma through research, I discovered that these are the types of questions that are answered by having a data governance plan. So, I did some more research, trying to find a model data governance plan for a healthcare organization. After searching high and low, I found no examples of such a plan. I asked my colleagues from both large and small organizations if they had such a plan and most told me that having a data governance plan was very important, but they also told me that they had tried to develop such a plan but got bogged down in the details and stopped trying to develop one.

At the first meeting of the NHA Data Council, I asked the members about their data governance plans and found that all had a pretty good idea about how data was managed in their organizations, no one had a formal plan. I then contacted the American Hospital Association and asked them about this issue and was told that across the nation, this was a problem.

Well, I am here to tell you that after much work and with the help of the NHA Data Council staff and members, we are publishing a Data Governance Guide. This is our first attempt at creating such a document so I am sure it will change and become more robust in the months to come as we all become more familiar with this topic. It is meant to be just what the title indicates. It is a guide to help you begin to write your own data governance plan and answer some of the questions posed about data above.

This guide is not an exhaustive compendium on all things related to data governance. Use what makes sense to you. Do your own research. See where the journey takes you. We are all learning together and as we learn, we will improve the content of this guide.

I would like to thank Margaret Woeppel, David DeVries and Brian Noonan as well as all of the members of the Data Council for their assistance in putting this guide together. I would also like to thank Gloria Kupferman from the AHA for her assistance. It was through some resources that she provided that our efforts really began to take shape.

Be well and enjoy your data governance journey.

Marty Fattig, CEO
Nemaha County Hospital

Nebraska Hospital Association Health Information and Data Council Members

Marty Fattig, Chair
Chief Executive Officer
Nemaha County Hospital
2022 13th Street
Auburn, NE 68305-1799
Phone: (402) 274-4366
Email: mfattig@nchnet.org

Nathan Albright
Market Analyst
Bryan Medical Center
1600 South 48th Street
Lincoln, NE 68506-1299
Phone: (402) 481-1111
Email: nathan.albright@bryanhealth.org

Aimee Black
Director of Quality & Safety
Nebraska Methodist Hospital
8303 Dodge Street
Omaha, NE 68114-4199
Phone: (402) 354-4000
Email: aimee.black@nmhs.org

Jill Divis
Senior Planning Analyst
CHI Health
12809 W Dodge Road
Omaha, NE 68154
Phone: (402) 343-4492
Email: jill.divis@chihealth.com

Chance Klasek
Chief Financial Officer
Jefferson Community Health & Life
2200 H Street
Fairbury, NE 68352-0277
Phone: (402) 729-3351
Email: chance.klasek@jchealthandlife.org

Brandon Kelliher
Chief Information Officer
Great Plains Health
601 West Leota Street
North Platte, NE 69103-1167
Phone: (308) 568-8000
Email: kelliherb@gphealth.org

Miles Loggie
Manager, Market Intelligence
Nebraska Medicine
987400 Nebraska Medical Center
Omaha, NE 68198-7400
Phone: (402) 552-2000
Email: mloggie@nebraskamed.com

Evette Blackburn
Marketing Director
Sidney Regional Medical Center
1000 Pole Creek Crossing
Sidney, NE 69162-2902
Phone: (308) 254-5825
Email: erparsons@sidneyrmc.com

Krista Trimble
Quality Improvement Coordinator
Pender Community Hospital
100 Hospital Drive
Pender, NE 68047-0100
Phone: (402) 385-3083
Email: krista.trimble@pchne.org

Chad Van Cleave
Vice President Finance/Chief Financial Officer
Columbus Community Hospital
4600 38th Street
Columbus, NE 68602-1800
Phone: (402) 564-7118
Email: cvancleave@columbushosp.org

George Wagaman
Planning & Innovation Strategist
CHI Health St. Elizabeth
555 South 70th Street
Lincoln, NE 68510-2494
Phone: (402) 219- 8000
Email: gwagaman@stez.org

Sean Wolfe
Chief Financial Officer
Community Hospital
1301 East H Street
McCook, NE 69001-1328
Phone: (308) 344-2650
Email: swolfe@chmccook.org

NHA Staff

Laura J. Redoutey
President
Nebraska Hospital Association
3255 Salt Creek Circle
Lincoln, NE 68504-4778
Phone: (402) 742-8140
Email: lredoutey@nebraskahospitals.org

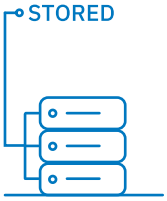
David Devries
Director of Health Data
Nebraska Hospital Association
3255 Salt Creek Circle
Lincoln, NE 68504-4778
Phone: (402) 742-8165
Email: ddevries@nebraskahospitals.org

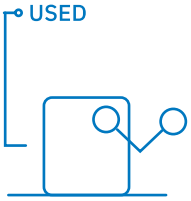
Michael Feagler
Vice President of Finance
Nebraska Hospital Association
3255 Salt Creek Circle
Lincoln, NE 68504-4778
Phone: (402) 742-8144
Email: mfeagler@nebraskahospitals.org

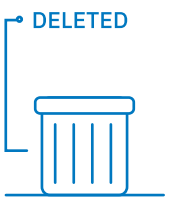
Margaret Woeppel
Vice President, Quality & Data
Nebraska Hospital Association
3255 Salt Creek Circle
Lincoln, NE 68504-4778
Phone: (402) 742-8145
Email: mwoeppel@nebraskahospitals.org

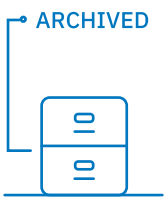
Table of Contents

Data governance determines how data is:









What is Data Governance?

HOW ORGANIZATIONS MANAGE AND INFLUENCE THE COLLECTION AND UTILIZATION OF DATA.

Data Governance "establishes and integrates a set of rules-policies, guidelines, principles and standards for managing the health system's highly valuable data assets."

AHIMA, Information Governance Toolkit 2.0

Data Governance provides the opportunity for a Health System to

- Improve data quality
- Lower data management costs
- Increase access to needed data
- Improve decision-making by healthcare leaders

Data Governance guides

- Decision rights
- Decision accountability

Data Governance determines how data is

- Valued
- Created
- Stored
- Used
- Archived
- Deleted

DATA GOVERNANCE ENCOURAGES CENTRALIZED DECISION MAKING AND THE BREAKING DOWN OF DATA SILOS WITHIN HEALTH SYSTEMS

Defining Data Governance for your Health System

How is Data Governance defined throughout the system?

The Health Information Technology (HIT) plan must **be consistently applied** across multiple operating units of your organization.

Leadership addresses interrelationship of health information technology plan throughout the organization and external environment.

3 essential elements for success (Stacey and Skinner)

- Alignment of purpose - HIT leadership and organizational leadership must agree that they are trying to achieve the same ends.
- Agreement to work jointly to develop goals and tactics to meet those ends by both leaderships.
- Agree to share responsibility and accountability for achieving the ends.

Does your data governance

- Support day to day operations?
- Increase your market share?
- Support quality assessment and improvement?
- Add value to your organization?

"Champions of data governance should be chosen from the right level and inclusive of frontline staff, not from IT."

NATHAN ALBRIGHT, Market Analyst, Bryan Health

HOW DOES YOUR DATA GOVERNANCE INTEGRATE WITH THE HEALTH SYSTEMS STRATEGIC PLAN?

Data Governance Council

Data Governance Participants

All data stakeholders who have a direct and indirect interest or stake in how data is created, collected, processed and manipulated, stored, made available for use or retired. Decisions should be made and championed by people who use the data, not just by, IT.

Key stakeholders and ad hoc representatives

- C- Suite Executives
- Information Technology
- Privacy
- Security
- Health Information Management
- Clinical Area Leaders and Front-Line Staff Users
- Quality
- Finance
- Planning
- Human Resources
- Operations
- Legal/Regulatory
- Risk Management
- Education

Why a Data Governance Council

- Need for an interdepartmental council to guide HIT decisions in a manner that benefits the organization as a whole and aligns with the health system strategic plan.
- Managers want to focus on of running the business therefore are risk averse in their decisions to minimize a bad outcome that will cost employment.
- Framework for data governance enables stakeholders to think and communicate about highly complex and sometimes ambiguous concepts.
- Program should be designed to make, collect and align rules to resolve issues and to monitor and enforce compliance while providing ongoing support to data stakeholders.

"Privacy and IT security staff should be included in the data governance council to ensure compatibility of data governance principles with data security and privacy."

MILES LOGGIE, Manager, Market Intelligence, Nebraska Medicine

Operations of Data Governance

- Setting priorities for focus
- Developing a set of value statements
- Establishing a roadmap for action
- Obtaining buy-in from stakeholders
- Implementing the roadmap
- Setting up a process to monitor, measure and report findings

Data Governance Council Charter

The charter requires a formalized set of goals, guiding principles and benefits of the Data Governance Council. The charter will serve as a road map to guide members.

Goals

- Enable better decision making
- Reduce operational friction
- Protect the needs of data stakeholders
- Train management and staff to adopt common approaches to data issues
- Build standard, repeatable processes
- Ensure transparency processes

Data Governance Institute 2020d

Location of data governance programs

- Business operations
- IT
- Compliance and privacy
- Data management

Responsibilities of Data Governance Council

1 Educate

- Membership of Data Governance Council
- Leadership
- Front Line

2 Understand

What is current infrastructure?

- Where is data being collected either electronically or manually?
- Is pertinent historical data being stored somewhere?
- Evaluate all system departments, units, locations for a complete list of current infrastructure.
- Are you accessing external data repositories (ex. NHA NHIS Data Portal)?
- Consider process mapping data locations and flow throughout the health system.

Develop sustainable momentum for long-term sustainability.

3 Evaluate

Evaluate current data needs throughout the system

- What are actions staff cannot do and issues they live with day-to-day concerning data they define, produce and use?

Evaluate future state and what will support future needs

Identify business needs

- How will this impact the organization's goals?

Assess ramifications and benefits of future data technologies

What is the business case for new technologies

Evaluate data risks

- Data privacy
- Data security

Consider external expert consultation

4 Assess

Regulatory requirements driving health system decisions

- Data privacy & protection laws
- Data security and management (CMS, OCR, etc.)
- Contractual obligations related to privacy and security of data
- Payment card industry data security standard

5 Develop

Policies and standards

- How will you determine what new data to bring into health system?
- How does data enhance business value and health system mission?
- Data standards, definitions, procedures and metrics for maintaining and improving management of risk, quality and usability

6 Monitor

Ensure compliance with data policies standards and processes

Determine overall approach to enforce data policies, standards and processes

- Escalate non-compliance (data stewards to department leaders to data governance council)
- Routine audits by council
- Turn over to internal audit department

Guiding Principles

Integrity
Data Governance participants will practice integrity.

Transparency
It should be clear to all participants and auditors who and when data-related decisions and controls were introduced into process.

Auditability
Data-related decisions, processes and controls subject to data governance will be auditable; they will be accompanied by documentation to support compliance-based and operational auditing requirements.

Accountability
Data governance will define accountability for cross-functional data-related decisions, processes and controls.

Stewardship
Data governance will define accountabilities for stewardship activities that are the responsibilities of individual contributors, as well as accountabilities for groups of data stewards.

Checks and balances
Data governance will define accountabilities for stewardship activities that are the responsibilities of individual contributors, as well as accountabilities for groups of data stewards.

Standardization
Data governance will introduce and support standardization of enterprise data.

Change Management
Data governance will support proactive and reactive change management activities for reference data values and the structure and use of master data and metadata.

In their Healthcare Data Governance Toolkit, 2018, Health Catalyst recommends conducting qualitative and data-driven assessments. "To identify a high-level vision and agenda for data governance, we recommend that you consider two perspectives: a view of your organization's current data "pain points" and usage, and a data-driven view of where better data governance could have the greatest impact on cost and quality."

Accountability of Data Governance

- Manages your data governance activities
- Keeps track of data stakeholder and data stewards
- Coordinates other key disciplines (compliance, privacy, security, architecture, data quality)
- Collects and aligns policies, standards and guidelines from key stakeholder groups
- Facilitates and coordinates data analysis and issue analysis projects
- Collects metrics and success measures and reports on them to data stakeholders
- Provides centralized communications for governance-led and data-related matters
- Maintains governance records

COMPILE A LIST OF APPLICATIONS, DATA REPOSITORIES AND DATASETS ACROSS ORGANIZATIONS

Identify data owners can organize via

- Application/data repository
- Department
- Dataset including master data and reference data
- Big data type
- Business process
- Geography
- Other

Agree with data owners that they are accountable for supporting security and privacy relative to data under their ownership

Obtain buy-in from data owners that they are accountable for the trustworthiness of data under their ownership

- Business Glossary
- Critical Data elements – to drive operating performance, financial reporting or regulatory compliance
- Business Rules
- Data Quality

Ensure that data owners appoint business data stewards to manage data on a day-to-day basis

Most Common Barriers for Data Governance Initiatives:

Organizational
Different groups within an organization must not only understand the importance of data governance, but be able to communicate and coordinate well.

Data quality, MDM and data migration integration
Applications and data must speak to one another and this must be addressed up front and planned for in any integration initiative.

Accountability and ownership of data
People must be held accountable for information assets and supported with technology to ensure the integrity of the assets.

Cost
Data governance initiatives must be implemented in such a way that costs are recouped and business value is proven.

From: "Seven Steps to Data Governance" Information Builders 2011

"Healthcare executives should be aware that technology alone will not create an effective data governance function. To truly enable, embed and continuously improve on key components of data governance, organizations should adopt a capability framework that incorporates people, processes and technology."

DATA GOVERNANCE: Driving Value in Healthcare
KPMG International

Health Information Technology Strategic Plan

ELEMENTS OF A HIT STRATEGIC PLAN

Priorities for the applications portfolio - priority list of applications to be acquired

Applications lists should consider the needs of all major functional areas of the healthcare organization (finance, HR, resource utilization and scheduling, materials management, facilities and project management and office automation).

Include new and replacement systems.

Applications should be ranked in the recommended sequence for implementation and items on the applications priority list should be linked to specific organizational strategies.

Specification of Overall HIT Architecture and Infrastructure

- Degree to which computing is centralized or decentralized throughout the organization.
- The network architecture that specifies how computers and workstations are linked together through communication lines and network servers.
- The manner in which data is stored and distributed throughout the organization, includes database security and control requirements.
- The manner by which individual applications are linked so that they can exchange information.

Statement of resource requirements

HIT plan identifies the resources required to carry out the plan.

- Capital budget should include 5-10-year projections for cost of computer hardware, network and telecommunications equipment and software.
- Operating budget – includes cost for personnel, supplies and materials, consultants, training programs and other reoccurring expenses.

Statement of corporate or institutional goals and objectives (HIT goals/objectives to be aligned with organization strategic goals).

Statement of HIT goals and objectives (be specific and flow from review of strategic priorities and an analysis of deficiencies and gaps in current information processes).

Detailed list of objectives that provide specific targets against which future progress can be measured and systems can be evaluated.

Management and staffing plan

Centralized within IT department or decentralized throughout organization.

- Centralized staffing offers advantages of economies of scale and reduction in the number of technical personnel to be employed.
- Decentralized staffing (throughout organization) brings systems management closer to the user and offers the potential for increased support and user involvement in system development and operation.
- Outsourcing HIT functions allows the healthcare organization to get out of the IT business through contracting with experts in the field. However, the cost of outsourcing may be high and may tend to generate too much distance between users and technical system specialists.

Software development plan

Internal Development vs. External Development

Reasons to use external development (managed service providers) MSP's

- Improve efficiency and reliability of IT operations
- Enhance security and compliance
- Manage all IT infrastructure and services remotely

ELEMENTS OF A HIT STRATEGIC PLAN (CONT.)

To be included

- Include major operational goals and objectives for 3-5 years
- Should align with organizational plan
- Should be specific and flow from review of strategic priorities and an analysis of deficiencies and gaps in current information process
- Set priorities for the applications portfolio

Specify overall HIT architecture and infrastructure

- The degree to which computing is centralized or decentralized throughout the organization
- The network architecture that specifies how computers and workstations are linked together through communication lines and network servers
- The manner in which data are stored and distributed through the organization, including database security and control requirements
- The manner by which individual applications are linked so that they can exchange information

SOFTWARE DEVELOPMENT PLAN

Specify procedures for software Development

- Application service providers (ASPs) a vendor that contracts with a healthcare organization to provide access to and use of applications on a subscription basis on an off-site server
- Managed service providers (MSPs)

Management and staffing plan

- Who is centralized vs. distributed among major user's departments

Statement of resource Requirements

- What is needed to carry out the plan?

End User Computing

- Departmental software packages from vendors
- Watch for data compatibility – use of common codes and data definitions for electronic information exchange across the organization

Integrated Delivery Systems - IDS

- Flow of information across the system
- Corporate policy must provide mechanisms for specialized information systems to meet individual needs

Data warehouses

- Do systems develop data warehouses to serve the needs for facilities in their system?

NHA Data Governance Check List

TO BEGIN THE PROCESS OF IMPLEMENTING DATA GOVERNANCE IN YOUR ORGANIZATION USE THE FOLLOWING CHECKLIST:

Create a Data Governance Council that includes members from a wide range of departments.

Create council from these key stakeholders and ad hoc representatives

- C- suite Executives
- Information Technology
- Privacy
- Security
- Health Information Management
- Clinical Areas Leaders and Front-Line Staff Users
- Quality
- Finance
- Planning
- Human Resources
- Operations
- Legal / Regulatory
- Risk Management
- Education

Develop a Data Governance Council Charter that formalizes the goals, guiding principles and benefits of the Data Governance Council.

Use these goals to create the Charter

- Enable better decision making
- Reduce operational friction
- Protect the needs of data stakeholders
- Train management and staff to adopt common approaches to data issues
- Build standard, repeatable processes
- Ensure transparency processes

Review the current infrastructure of the organizations data.

Use these questions to help review the current infrastructure

- Where is data being collected either electronically or manually?
- Is pertinent historical data being stored somewhere?
- Evaluate all system departments, units, locations for a complete list of current infrastructures?
- Are you accessing external data repositories (ex. NHA NHIS Data Portal)?
- Have you mapped data locations and flow throughout the Health System?

Develop a Health Information Technology Strategic Plan with specific goals and objectives. Ensure that your HIT Plan aligns with your organization plan, is specific and flows from strategic priorities.

Use the following ideas when looking at your strategic plan

- What are your major operational goals and objectives for 3-5 years?
- Does the applications portfolio list consider the needs of all major functional areas of the healthcare organization (finance, HR, resource utilization and scheduling, materials management, facilities and project management, and office automation- (include both new and replacement systems)?
- Are applications ranked in the recommended sequence for implementation?
- Are items on the applications priority list linked to specific organizational strategies?
- Does the capital budget include 5-10-year projections for cost of computer hardware, network and telecommunications equipment, and software?
- Does the operating budget include costs for personnel, supplies and materials, consultants, training programs and other reoccurring expenses?

Identify focus areas related to your strategic goal.

Use these questions to help define your focus areas

- What are areas where the organization's clinical and business operations are being negatively affected due to data limitations?
- What are areas where attention and investment will fuel a competitive advantage or move the organization toward an important strategic goal?

Identify the types of information that are required to support strategic objections and establish priorities for the installation of specific computer applications, the architecture on which the systems function and detailed rules that drive IT functions.

Use these questions to help define your priorities

- What quality metrics determine "good" and "bad" data?
- How have you ensured that the right people have access to needed data for better decision-making?
- Does leadership understand requirements for data exchange, including HIPAA mandates?
- Does your organization have a Data Dictionary This is a list or tool that specified or defines the format of each data element and the coding system associated with that element (ex: date of birth)?
- Do you have policies related to acquisition of computer hardware, software, and network communications?
- Does there need to be a central review and approval of all computer hardware and software purchases?
- Review and approval of all computer hardware and software purchases?

Review policies related to physical and cyber security.

Use the following questions to help review your policies

- Do you have a management policy that specifies individual's system access rights?
- What is your hardware security features/firewall?
- What is your policy regarding physical measures of security such as password access?
- What policies do you have that limit who can take what actions with what information: 1 When they can take that action 2. Under what circumstances that action can be taken and 3. What methods can be employed in that action?
- Do you have data definition standards?
- What are your policies governing the acquisition of hardware, software, and telecommunications network equipment?
- What are your policies on internet data breaches?
- What is your data privacy policy?
- What is your policy related to disaster planning and recovery toolkit?
- Do you maintain documentation of current system components and connections?
- How do you ensure backup of critical data to secure but accessible storage, ideally off-line?
- How do you designate storage options by data type (sensitive, clinical, research, business) to ensure coverage by appropriate security protocols?
- Do you maintain current versions of antivirus and antimalware software?
- Do you maintain current updates of software to ensure currency of security elements?
- Do you enforce policy for regular strong password changes?
- Do you limit access and user rights to system components on need-to-know basis?
- How do you ensure staff have appropriate access for job performance?
- Do you have a policy for removing access from terminated employees?
- What policies do you have that ensure access is on a need-to-know basis?
- What policies do you have that ensure compliance with policies and procedures?
- What procedures do you have in place to manage security incidents? How do you manage your response to those incidents?
- What contingency Plans do you have to prepare for a disaster?
- Have you developed backup and recovery procedures?
- How do you monitor to adjust to environmental or operational changes that affect security?
- How do you enforce business associate contracts and other arrangements – these would be like business associate agreements related to privacy rule but specific to ePHI?

Review policies related to how data are archived and when data is destroyed.

Use the following questions to help review your policies

- Where is your data archived?
- What is your cost for data archiving?
- What security do you have for archived data?
- Have you looked at long-term growth of storage required?
- Are you archiving because it is easier than to design and manage a data disposal policy?
- Have you identified and classified all your organizations data?
- Is your archive in a secure but accessible off-site location in case information resources are damaged or destroyed by a disaster?
- Are you archiving for active use or mandated retention?
- In your record retention schedule have you ensured patient health information is available to meet the needs of continued patient care, legal requirements, research, education, and other legitimate uses of the organization?
- In your record retention schedule have you included guidelines that specify what information is kept, the time range for which it is kept, and the storage medium on which it will be maintained (e.g., paper, microfilm, optical disk, magnetic tape)?
- Do you have destruction policies and procedures that include appropriate methods of destruction for each medium on which information is maintained?
- Do you have policies that prevent data from being stored on devices apart from the main storage locations (i.e., local devices, USB sticks, etc.)?
- Do you have policies that use encryption technologies to render data on devices unreadable should device be stolen or lost?

Data Governance Determines How Data is Valued

DETERMINE VALUE TO THE DEGREE POSSIBLE INCLUDING EVIDENCED-BASED VALUE OBJECTIVES.

Financial

- Cost reductions
- Revenue enhancements
- Productivity gains

Clinical

- HIT's impact on service delivery
- Impact on clinical outcome indicators

Organizational

- Stakeholder satisfaction improvements and risk reduction

"Leaders must promote a data-driven culture. Executives need to endorse data as a critical asset and reinforce it with their behavior. They need to promote the goals and rationale for data governance, transparently share progress and results and facilitate cross-functional participation and feedback. Communication is key to establishing a culture that values data-driven decision making."

HEALTHCARE DATA GOVERNANCE: Health Catalyst. Version 1

PROVIDE DATA BEFORE ESTIMATING THE BUDGET AND RESOURCES REQUIRED TO MEET THE OBJECTIVES AND PRIORITIES ESTABLISHED THROUGH THE PLANNING PROCESS.

Healthcare Data Governance, 2018, Health Catalyst

Identify Focus Areas

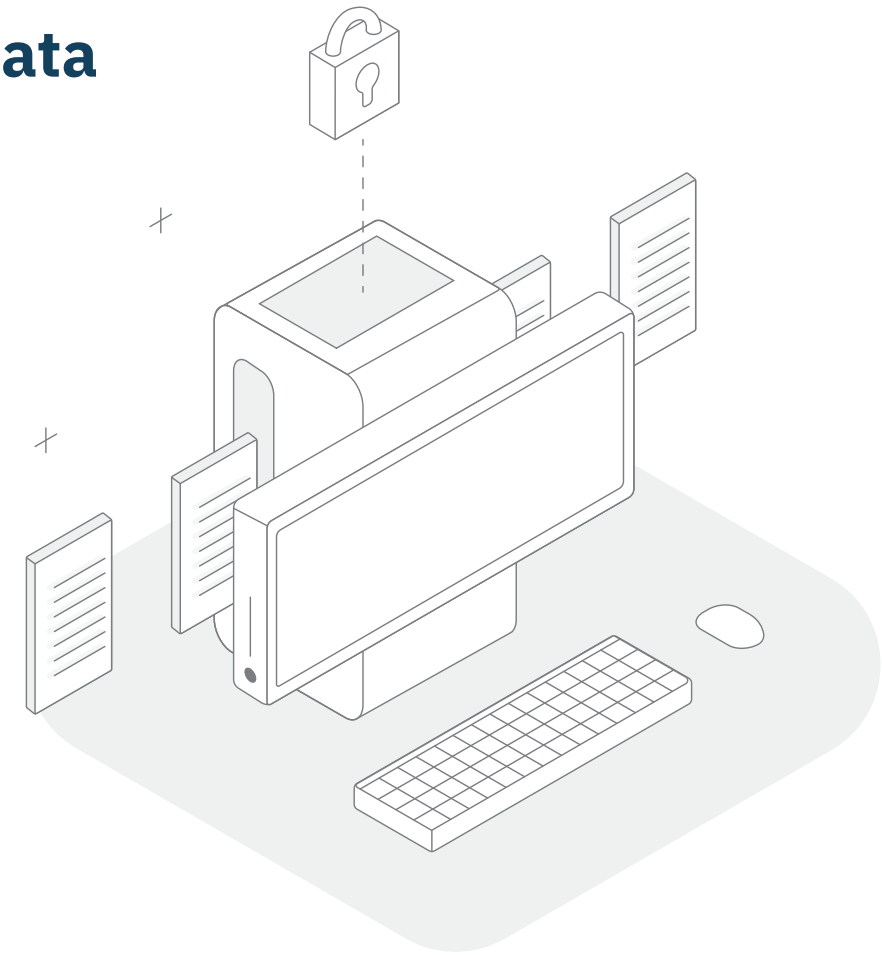
- Areas where the organization's clinical and business operations are being negatively affected due to data limitations. For example, if the organization is incurring penalties for missing quality targets, but has no ability to use data to identify the cause of the quality gaps, you may choose this as a focus of data governance.
- Areas where attention and investment will fuel a competitive advantage or move the organization toward an important strategic goal. If your organization wants to move toward value-based care and risk-sharing contracts, for example, you will need reliable insight into utilization to effectively manage under these new arrangements.

Three essential elements for success (Stacey and Skinner)

Alignment of purpose

- HIT leadership and organizational leadership must agree that they are trying to achieve the same ends.
- Agreement to work jointly to develop goals and tactics to meet those ends by both leaderships
- Agree to share responsibility and accountability for achieving the ends

Data Governance Determines How Data is Created



Leadership

- Manages priorities within Health Information Technology vs. alternative investment options.
- Identify major types of information required to support strategic objectives and establish priorities for installation of specific computer applications, the architecture on which the systems function and the detailed rules that drive IT functions.

Data standards

Leadership should understand requirements for data exchange, including HIPAA mandates, and should develop a policy on data standardization for the organization.

Most computer applications must include ability to share information with other systems within organization.

- Data dictionary – list or tool that specifies or defines the format of each data element and the coding system associated with that element (ex: date of birth)
- Ex: many hospitals mandate all software purchased from vendors must meet industry standards such as HL7

Facilitate the exchange of information among health systems, government and private insurance, medical supply and equipment vendors and other entities.

Hardware and Software Standards

Need policies related to acquisition of computer hardware, software and network communications

Does there need to be a central review and approval of all computer hardware and software purchases?

- Central review and approval help to ensure compatibility and enterprise-wide data standards such as HL7
- Central review and approval of personal computer purchases can ensure that data terminals and workstations use a common operating system, such as Windows
- Central review and purchasing of generalized software provide cost advantages through the acquisition of site licenses for multiple users of common packages (ex: word processing, spreadsheets, database management)
- Central review and approval ensure that hardware and software are of a type that can receive technical support and maintenance from the HIT staff
- Central review and approval can help prevent illegal use of unlicensed software in the organization

Determine data integrity

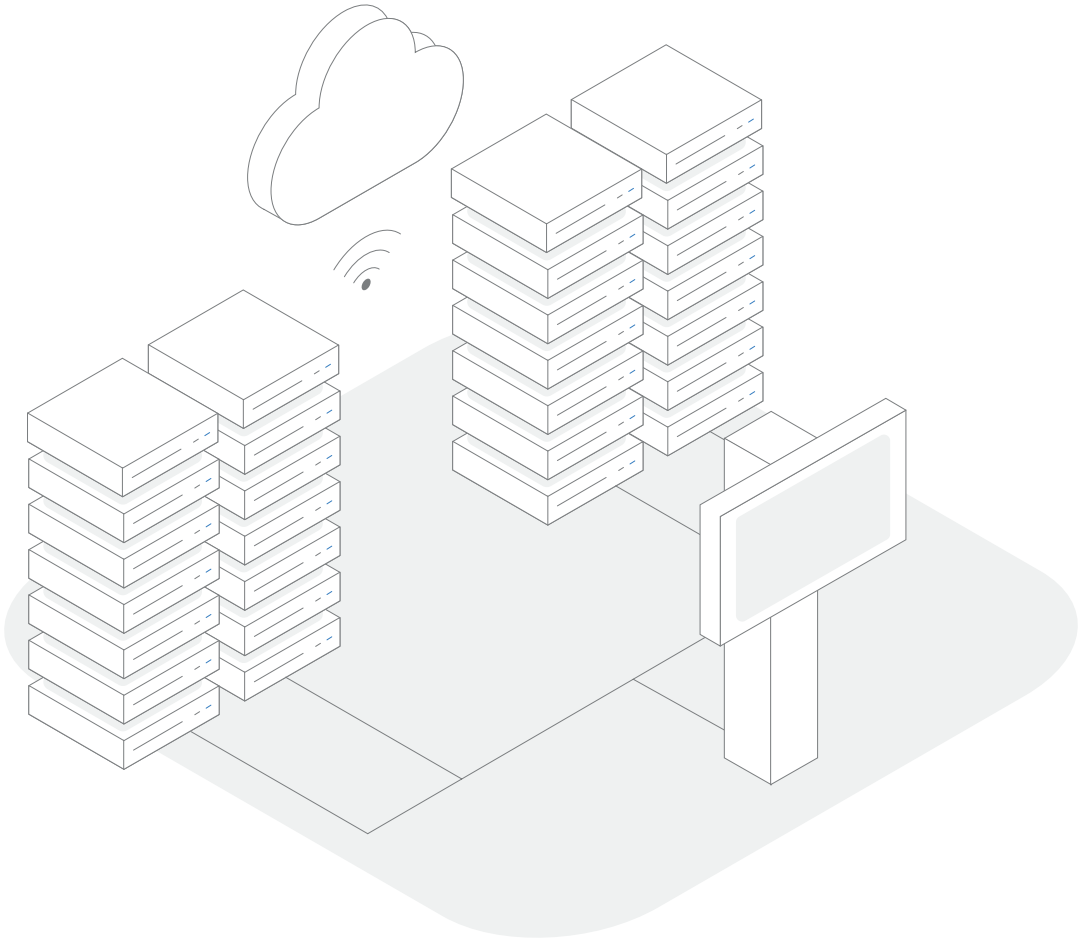
- What defines quality metrics determine "good" and "bad" data.
- Data Profiling Tools - intuitive tools to clean, transform and understand data.
- How have you ensured that the right people have access to needed data for better decision-making?

"Data utilization is a crucial driver within our health care systems to promote sustainable and meaningful quality improvement to advance the health of our patients and communities."

AIMEE BLACK, Director of Quality and Safety

Methodist/Women's Hospital

Data Governance Determines How Data is Stored



"The accumulation of data occurs without proper guidance on how long data should be maintained and also fails to meet basic requirements from various regulations for minimum retention periods."

NEBRASKA METHODIST

HIEs employ a combination of approaches depending on their integration architecture. Some examples include an encrypted virtual private network for interfaced clients, secured sockets layer (a protocol for encrypting information over the Internet) or secured portal with applicable HIPAA safeguards (password complexity, timeouts, and so forth) for portal users.

AIHMA: Ensuring Data Integrity in Health Information Exchange

CONSIDERATIONS FOR DATA STORAGE

Storage Options

- Cost, amount, security, regulatory, processing needs
- Text or non-text version
- Size of images
- How long is it stored?
- How accessible does it need to be?
- Non-volatile storage options
- How much data will need to be stored?
- What levels of physical security are required to adequately secure the stored data?
- In the event of an adverse event, how will the data be secured and maintained? It is important for health systems to understand the protective layers to prevent loss of critical data.
- Is there a level of seperation between primary storage (active use) and secondary storage (archived storage)?

Must develop blueprints for HIT infrastructure

- Hardware configurations (architecture)
- Network communications
- Degree of centralization or decentralization of computing facilities
- Types of software required to support network

Location Options

- On premise hardware-based storage – hard disks in house in arrays of network servers
- Off premise storage – remote data center
- Cloud storage – data stored on internet with external vendor
- Private cloud – IT infrastructure dedicated to a single enterprise (more security and control)
- Public cloud – allows distribution of data of internet servers shared among multiple users.
- Must maintain a secure off-site location – HIPAA

Goal for data utility (efficiency and cost effectiveness is to capture data once and store in a single location (nurse putting in birthdate multiple times)

- Cost (financial and time) putting data in multiple times
- Increased errors
- Different entry formats may cause data to not aggregate correctly

Data Governance Determines How Data is Used

Executive team should evaluate the need for an outside security risk assessment

Privacy and Security

Ensure safe handling done in compliance with regulations and enables the organization to derive maximum value from the information to improve business performance.

Physical security

- Management policy - specifying individuals system access rights
- Hardware security features/firewall
- Physical measures (code/password access)

Data security

Evaluate security risk vs. accessibility

Uses established models that limit who can take what actions with what information

- When they can take that action
- Under what circumstances that action can be taken and
- What methods can be employed in that action

Examples of required data security policies

- Data definition standards
- Policies governing the acquisition of hardware, software and telecommunications network equipment
- Management policy - specifying individuals system access rights
- Hardware security features/firewall
- Physical measures (code/password access)
- Policies on use of internet
- Data breach policy
- Data privacy policy
- Disaster planning and recovery toolkit

Cybersecurity

Protection of internet-connected information systems.

All elements of the system (enterprise and non-enterprise) devices that connect must be considered in designing security protocols to protect enterprise information resources.

Cyberhygiene – adherence to good security practices for internet-connected components. Minimal factors:

- Maintain documentation of current system components and connections
- Ensure backup of critical data to secure but accessible storage, ideally off-line
- Designate storage options by data type (sensitive, clinical, research, business) to ensure coverage by appropriate security protocols
- Maintain current versions of antivirus and antimalware software
- Maintain current updates of software to ensure currency of security elements
- Enforce policy for regular strong password changes
- Limit access and user rights to system components on need to know basis.
- Implement multi-factor authentication

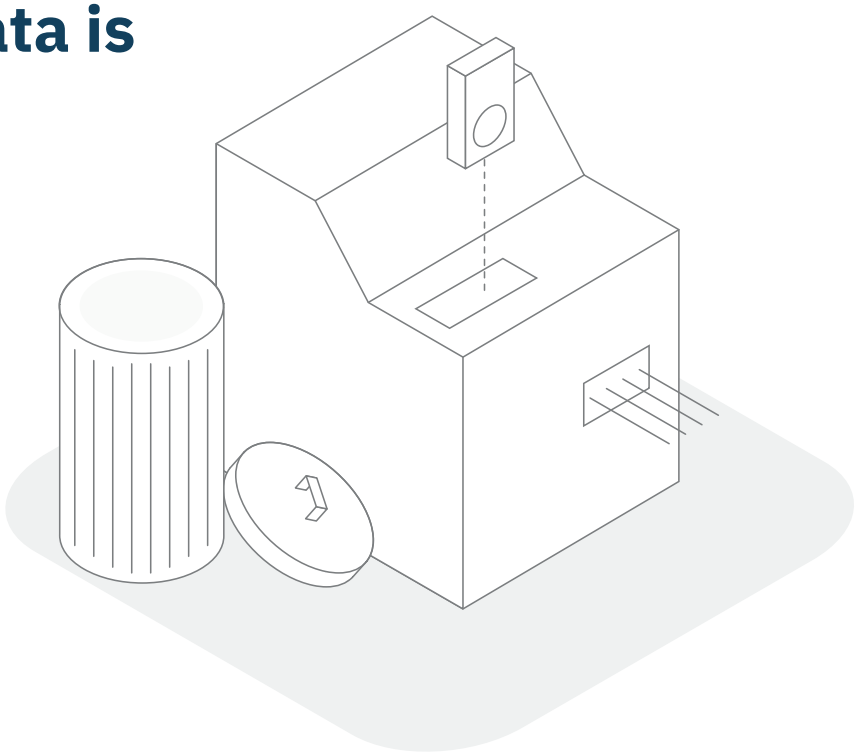
ORGANIZATIONS NEED A PLAN FOR HANDLING DATA IN A CONSISTENT MANNER THROUGHOUT THE ORGANIZATION

CONSIDER AUTOMATION WHERE AVAILABLE

HIPAA security rule requirements

- Security management process – includes risk management and risk analysis
- Assigned responsibility for security
- Workforce Security – ensures access for job performance; removes access from terminated employees
- Management of information access – ensures access on a need-to-know basis
- Security awareness and training – ensures compliance with policies and procedures
- Security incident procedures – reports structure; manages responses
- Contingency Plans – prepares for disaster; develops backup and recovery procedures
- Evaluation – monitors to adjust to environmental or operational changes that affect security
- Business associate contracts and other arrangements – is similar to business associate agreements related to privacy rule but specific to ePHI

Data Governance Determines How Data is Deleted



NEED A DATA DESTRUCTION PLAN VS. UNENDING DATA THAT CAN BE EXPENSIVE AND EXPANSIVE.

AHIMA Retention and Destruction of Health Information 2013 Practice Brief: Sample data destruction form https://library.ahima.org/PB/RetentionDestruction#.YBhyFZeSmUl

"The life cycle of a good record retention program does not end until information has been destroyed. Destruction is an important component to the record retention program because it completes the life cycle of a record. Because of storage capacity, fiscal restraints and legal constraints, most organizations and providers are unable to maintain records indefinitely. There are requirements regarding record destruction that organizations need to be aware of when destroying information."

AHIMA. "Retention and Destruction of Health Information." (Updated October 2013).

According to the International Data Sanitization Consortium (2020), data destruction means obliterating information housed in digital storage media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.

- Prevent data from being stored on devices apart from the main storage locations (i.e., local devices, USB sticks, etc.)
- Use of encryption technologies to render data on devices unreadable should device be stolen or lost

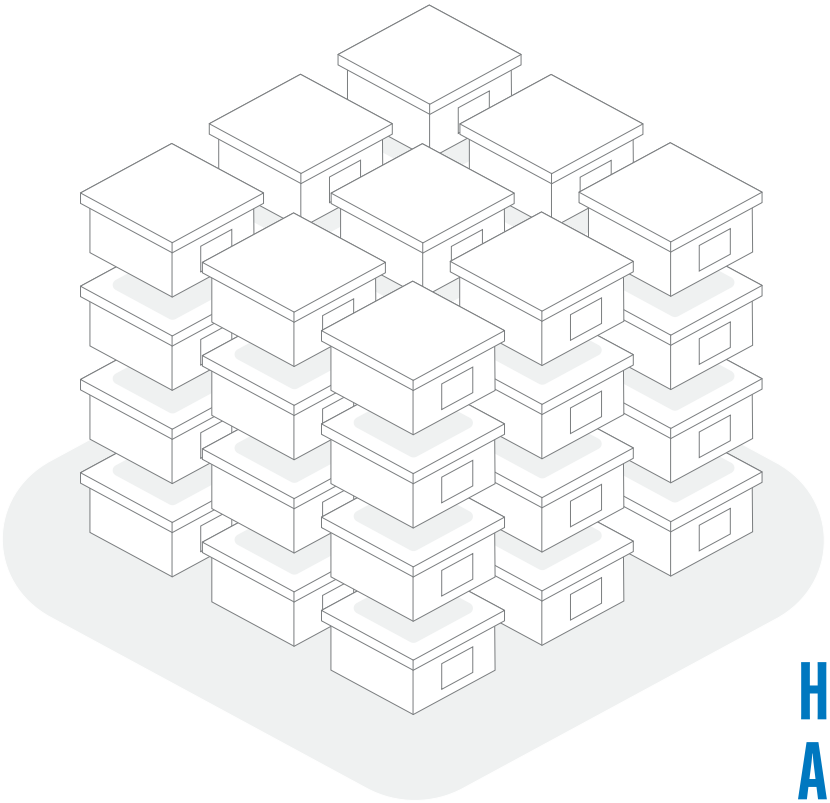
Data privacy guidelines require authentication of destruction for digital media. External companies should provide hospitals with a certificate of destruction and a secure and verifiable chain of custody for auditing and accountability.

UNDER THE HIPAA PRIVACY RULE (45 CFR, PARTS 160 AND 164), WHEN DESTRUCTION SERVICES ARE OUTSOURCED TO A BUSINESS ASSOCIATE THE CONTRACT MUST PROVIDE THAT THE BUSINESS ASSOCIATE WILL ESTABLISH THE PERMITTED AND REQUIRED USES AND DISCLOSURES AND INCLUDE THE FOLLOWING ELEMENTS:

- The method of destruction or disposal
- The time that will elapse between acquisition and destruction or disposal
- Safeguards against breaches
- Indemnification for the organization or provide for loss due to unauthorized disclosure
- Require the business associate to maintain liability insurance in specified amounts at all times

AHIMA. "Retention and Destruction of Health Information." (Updated October 2013)

Data Governance Determines How Data is Archived



HAVE YOU IDENTIFIED AND CLASSIFIED ALL YOUR ORGANIZATION'S DATA?

"The goal for data utility, efficiency and cost-effectiveness is to capture data once and store it in a single location and to have that data available as needed by an application or user. Replicating data for storage in multiple locations is undesirable for many reasons." (Information Technology for Healthcare Managers)

- Expense
- Increased risk for errors
- Data may not aggregate correctly when files are merged across applications
- Legal issues if data cannot be appropriately accessed

Key issues regarding data storage include;

- Data classification
- Media used
- Location (on premise hardware based vs. off premise)
- Cloud storage (public vs. private)
- Cost
- Security
- Long-term growth of storage required

Must maintain a secure but accessible copy of data in an off-site location in case information resources are damaged or destroyed by a disaster – HIPAA Security Rule's Administrative Safeguards (Snell 2015). Resources available at Department of Homeland Security www.ready.gov

Are you archiving for active use or mandated retention?

Accreditation Agency Record Retention Requirements AHIMA Record Retention Recommendations Special Populations
Minors, Behavioral Health, Research Patients, etc.

State record retention for records of historical importance
Healthcare Institutions may choose to keep records or transfer them to the Nebraska State Historical Society (State Archives). The Nebraska State Historical Society is interested in records of historical importance. When records are transferred to the State Historical Society, they become the property of the State Archives.
According to Statute 82-104 The State Historical Society is the custodian of all public records, which includes any institutions that receive money from the Legislature or any County, City or Public Building.

According to Statute 82-105 it says that the State Historical Society shall obtain possession of historical material when it is not in active use and or whenever it is liable to damage. However, the officer or board having care of the department shall consent in writing to the custody of the documents by the society.

According to Statute 82-106 it says that the board shall notify the State Historical Society of any historical material it has in its care.

According to Statute 82-107 any material sent to the State Historical Society the Society may choose to keep for historical reasons at which point it needs to transport and display the material for free use to the public.

ARE YOU ARCHIVING BECAUSE IT IS EASIER THAN TO DESIGN AND MANAGE DATA DISPOSAL POLICY?

Federal record retention requirements
Federal Register

Higher Education Act of 1965 disclosure requirements (20 USC §1232g)

In the absence of specific state requirements, providers should keep health information for at least the period specified by the state's statute of limitations or for a sufficient length of time for compliance with laws and regulations.
If the patient is a minor, the provider should retain health information until the patient reaches the age of majority (as defined by state law) plus the period of the statute of limitations. A longer retention period is prudent, since the statute may not begin until the potential plaintiff learns of the causal relationship between an injury and the care received.

The False Claims Act (31 USC 3729), claims may be brought up to seven years after the incident; however, on occasion, the time has been extended to 10 years.

Record retention policy AHIMA. "Retention and Destruction of Health Information." (Updated October 2013).
At a minimum, record retention schedules must:

- Ensure patient health information is available to meet the needs of continued patient care, legal requirements, research, education and other legitimate uses of the organization
- Include guidelines that specify what information is kept, the time range for which it is kept, and the storage medium on which it will be maintained (e.g., paper, microfilm, optical disk, magnetic tape)
- Include clear destruction policies and procedures that include appropriate methods of destruction for each medium on which information is maintained
- Include Certificate of Destruction to verify and have a record it was successfully and appropriately destroyed

Data Policies by Sunil Soares

ESTABLISH A FRAMEWORK FOR DATA POLICIES

By enterprise data management

- Data Ownership
- Data Architecture
- Data Modeling
- Data Integration
- Data Security & Privacy
- Master Data Management
- Reference Data Management

System of record – inventory of code tables along with a list of canonical or standard values and a mapping across systems.

Stewardship – must assign code tables to data owners or data stewards who will be responsible for adding, modifying and deleting code values.

- Metadata Management

Business glossary – key business terms and definitions, must adopt naming and definition standards, includes a data dictionary with the definitions of column and table names for key data repositories

Data stewardship – assign data stewards to manage business terms and other data artifacts

Business rules – for critical data elements, must be documented and kept up to date

Data lineage and impact analysis – must ingest metadata from key systems, including relational databases, data modeling tools, data integration platforms, reports, analytic models, and Hadoop.

- Data Quality Management
- Information Lifecycle Management

By data domain

- Customer
- Product
- Vendor
- Equipment
- Chart of accounts
- Errors such as customer duplicates and product hierarchies

By critical data element

- Guidelines to identify critical data elements
- Additional privacy elements such as Social Security Number, email, address, phone number and product identifier

By organization

Data issues specific to a given function or department

By business process

- Customer service
- New product introduction

By big data domain

Use of big data such as Facebook, Twitter, equipment sensor data, facial recognition, chat logs, and web cookies.

The Chief Data Officer Handbook for Data Governance, 2014

Resources

"Data Governance: Driving value in healthcare" KPMG International; 2018 KPMG, LLC.

"Seven Steps to Data Governance"

Information Builders; 2011

"Information Technology for Healthcare Managers" Ninth Edition

Gerald L. Glandon
Detlev H. Smaltz
Donna J. Slovensky

Health Administration Press, Chicago, Illinois 2021

American Health Information Management Association (AHIMA) Information Governance Toolkit 2.0: Building Critical Competencies and Delivering Outcomes Through Excellence in Strategic Information Management

2016 ahima.org/infogov

AHIMA. "Retention and Destruction of Health Information" (Updated October 2013)

Kathy Downing, MA, RHIA, CHP, PMP
Marcy Pye, RHIA

"Healthcare Data Governance: Improving decisions and outcomes... from the boardroom to the bedside" Version 1 (2018)

HealthCatalyst

"The Chief Data Officer Handbook for Data Governance"

Sunil Soares

MC Press Online, LLC 2014

"Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program" 2nd edition

John Ladley

Academic Press 2020

"Non-Invasive Data Governance: The Path of Least Resistance and Greatest Success" 1st edition

Robert S. Seiner

Technics Publications 2014

Data standards, organizations and regulatory bodies

American National Standards Institute

National Information Standards Organization

Organization for the advancement of structured information standards

Public Health Data Standards Consortium

Health Information Technology Advisory Committee (HITAC)

Office of National Coordinator for Health Information Technology (ONCHIT)

ONCHIT HITECH Programs

Office for Civil Rights

Cybersecurity and Infrastructure Security Agency (CISA)

Health Insurance Portability and Accountability Act (HIPAA)

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

Food and Drug Administration Safety and Innovation Act (FDASIA) of 2012

Patient Protection and Affordable Care Act (ACA) of 2010

Medicare Access and CHIP Reauthorization Act (MACRA) of 2015

Healthcare Related Acronyms

ACA
Patient Protection and Affordable Care Act

ACO
Accountable Care Organization

ADE
Adverse Drug Event

ADT
Admission, Discharge, Transfer

AHIMA
American Health Information Management Association

AHRQ
Agency for Healthcare Research and Quality

AI
Artificial Intelligence

AIS/AIMS
Anesthesia Information Systems/Anesthesia Information Management Systems

AMAM
Adoption Model for Analytics Maturity

AMC
Academic Medical Center

AMIA
American Medical Informatics Association

ANSI
American National Standards Institute

APM
Advance Alternative Payment Models

APN
Advanced-Practice Nurse

ARRA
American Recovery and Reinvestment Act

ASP
Application Service Provider

BI
Business Intelligence

C-CDA
Consolidated Clinical Document Architecture

CCHIT
Certification Commission for Health Infrastructure Technology

CCR
Continuity of Care Record

CDC
Centers for Disease Control and Prevention

CDR
Clinical Data Repository

CDS
Clinical Decision Support

CDSS
Clinical Decision Support System

CEHRT
Certified Electronic Health Record Technology

CHIME
College of Healthcare Information Management Executives

CHIP
Children's Health Insurance Program

CMDB
Configuration Management Database

CMS
Centers for Medicare & Medicaid Services

CMV
Controlled Medical Vocabulary

CobiT
Control Objects for Information Technology

CPOE
Computerized Physician/Provider Order Entry

CPT
Current Procedural Terminology

CPU
Central Processing Unit

CVO
Credentials Verification Organization

DBMS
Database Management System

DGO
Data Governance Office

DHS
US Department of Homeland Security

DICOM
Digital Imaging and Communications in Medicine

EDI
Electronic Data Interchange

EBM
Evidence-Based Medicine/Evidence-Based Management

EDW
Enterprise Data Warehouse

EHR
Electronic Health Record

EIS
Executive Information System

eMAR
Electronic Medication Administration Record

EMR
Electronic Medical Record

EMRAM
Electronic Medical Record Adoption Model

ERP
Enterprise Resource Planning

ETL
Extract, Transform, Load

FCC
Federal Communication Commission

FDA
Food and Drug Administration

FDASIA
Food and Drug Administration Safety and Innovation Act

FDDI
Fiber-Distributed Data Interchange

FTE
Full-Time Equivalent

GAN
Global Area Network

GDP
Gross Domestic Product

HCPCS
Healthcare Common Procedure Coding System

HHS
US Department of Health and Human Services

HIE
Health Information Exchange

HIMSS
Healthcare Information and Management Systems Society

HIPAA
Health Insurance Portability and Accountability Act

HIS
Healthcare Information System

HIT
Health Information Technology

HITECH
Health Information Technology for Economic and Clinical Health

HITSP
Health Information Technology Standards Panel

HL7
Health Level Seven

HMO
Health Maintenance Organization

HRIS
Human Resources Information System

ICD
International Classification of Diseases

IDPS
Intrusion Detection and Prevention System

IDS
Integrated Delivery System

IHI
Institute for Healthcare Improvement

IOM
Institute of Medicine

IoT
Internet of Things

IP
Internet Protocol

IRPQ
Incidents, Requests, Problems, Questions

ISDN
Integrated Services Digital Network

ISO
International Organization for Standardization

IT
Information Technology

ITIL
Information Technology Infrastructure Library

KPI
Key Performance Indicator

LAN
Local Area Network

MACRA
Medicare Access and Chip Reauthorization Act

MDM
Master Data Management

MIPS
Merit-Based Incentive Payment System

MPI
Master Patient/Person Index

MSP
Managed Service Provider

NCQA
National Committee for Quality Assurance

NFC
Near Field Communication

NGT
Nominal Group Technique

NHE
National Health Expenditures

NIC
Network Interface Controller/Card

NIST
National Institute of Standards and Technology

NLM
National Library of Medicine

NLP
Natural Language Processing

NoSQL
Nonstructured Query Language

NPI
National Provider Identifier

NPV
Net Present Value

O-EMRAM
Outpatient-Electronic Medical Record Adoption Model

OCR
Office for Civil Rights

OECD
Organization for Economic Co-Operation and Development

OGC
Office of Government Commerce (United Kingdom)

ONC/ONCHIT
Office of National Coordinator for Health Information Technology

OS
Operating System

PACS
Picture Archiving and Communication System

PC
Personal Computer

PCP
Primary Care Provider

PDA
Personal Digital Assistant

PHI
Personal Health Information/Protected Health Information

PHR/ePHR
Personal Health Record/Electronic Personal Health Record

PMI
Project Management Institute

PMO
Portfolio Management Office/Program Management Office/
Project Management Office

PMP
Project Management Professional

PPM
Project Portfolio Management

QPP
Quality Payment Program

QR
Quick Response Code

RAM
Random Access Memory

RBAC
Role-Based Access Control

RCM
Revenue Cycle Management

RFI
Request for Information

RFID
Radio Frequency Identification

RFP
Request for Proposa

RHIO
Regional Health Information Organization

ROI
Return on Investment

ROM
Read Only Memory

SAT
Solutions, Answers and Temporary Fixes

SLA
Service-Level Agreement

SME
Subject Matter Expert

SNOMED-CT
Systematized Nomenclature of Medicine-Clinical Terms

SQL
Structured Query Language

TCO
Total Cost of Ownership

VDT
Video Display Terminal

WAN
Wide Area Network

WHO
World Health Organization

WWW
World Wide Web

Glossary of Data Terms

Account Number
An identifying number for a patient in order to track medical visits. Usually, the account number is automatically assigned by the medical office's computer system.

Accountable Care Organization (ACO)
ACOs are groups of physicians, hospitals and other health care providers that work together to coordinate high quality care for their patients. In some instances, ACO providers contract with payers to accept risk for not meeting goals or to be rewarded for exceeding goals.

Acute Care
A pattern of health care in which a patient is treated for an acute (immediate and severe) episode of illness; for the subsequent treatment of injuries related to an accident or other trauma; or during recovery from surgery. Acute care is usually delivered in a hospital setting by specialized personnel using complex and sophisticated technical equipment and materials. Unlike chronic care, acute care is usually only delivered over a short time span of 30 days or less.

Additional Diagnosis
Any diagnosis, other than the principal diagnosis, that describes a condition for which a patient receives treatment or which the physician considers of sufficient significance to warrant inclusion for investigative medical studies.

Administrative Information System
An information system designed to assist in the performance of administrative support activities in a healthcare organization, such as payroll, accounting, account receivable, accounts payable, facility management, intranets and human resources management.

Admission
Admitting a client to hospital as an inpatient.

Admitting Diagnosis Code
Is a code indicating a patient's diagnosis at admission.

ADT
An ADT system sends automatic notifications or alerts from hospitals to primary care practices and/or care managers when a patient has an admission, discharge or transfer. Its intent is to improve the timely flow of information needed when a patient is transitioning to care in another setting or in the community.

Algorithm
A step-by-step procedure for performing a task. Computer algorithms consist of logical and mathematical operations.

All Patient Diagnosis Related Groups (APDRG)
An enhancement of the original DRGs, designed to apply to a population broader than that of Medicare beneficiaries, who are predominantly older individuals. The APDRG set includes groupings for pediatric and maternity cases, as well as services for HIV-related conditions and other special cases. Example 3M APRDRG Grouper

Ambulatory Care
Health services delivered on an outpatient basis. If the patient makes the trip to the doctor's office or surgical center without an overnight stay, it is considered ambulatory care.

Analog Signal
The representation of data by varying the amplitude, frequency, or phase of a waveform. See also digital signal.

Analytics
The science of logical analysis; analysis of large data sets by use of mathematics, statistics, and computer software.

Ancillary Care
Additional health care services performed, such as lab work and x-rays.

Application Service Provider (ASP)
An organization that contracts with a healthcare facility to provide access to online application.

Applications Program
A program that performs specific tasks for the computer user, such as payroll, order entry and inventory control.

Appointment
An event in a PHC outpatient clinic. A scheduled booking for a client to attend a clinic. Once the client arrives, an event occurs e.g., procedure or consultation, and is attached to the appointment. If the client is a no-show or must be cancelled, the appointment will still appear to users but will display the relevant status e.g. no-show, cancelled.

Arithmetic Logic Unit (ALU)
A computer component that performs the computational and comparison functions. The ALU's speed is a primary consideration for applications involving image processing and other clinical applications.

Artificial Intelligence (AI)
A discipline that attempts to simulate human problem-solving techniques in a computer environment. See also expert system.

Assessment
Diagnostic procedures, history, physical services and tests for the purpose of determining whether or not an eligible insured is an appropriate candidate for specified healthcare services.

Asynchronous transfer mode
A networking technology that segments data into small fixed-length cells, directs the cells to the appropriate destination and reassembles the data.

Bandwidth
A measure of the data-carrying capacity of a transmission medium. The higher the bandwidth, the larger the volume of data that can be moved across networks.

Bar Code
A printed sequence of vertical bars and spaces that represent numbers and other symbols. The code can be read and translated automatically by specially designed computer input devices.

Bar-Code Scanner
An input device that allows computer users to scan a bar code and transfer its contents to a computer.

Behavioral Health Care
Treatment of mental health and/or substance abuse disorders.

Benefits Realization
Determining, during the postimplementation phase of a project, whether goals for health information technology (HIT) investment were achieved.

Bit
A binary digit (0 or 1) that is part of a data byte. In most computer systems, eight bits make up one byte.

Blockchain
A distributed transactional database comprising linked records stored across multiple computers. All participants view, exchange and store information with a central authority.

Bridge
An interface that connects two or more networks that use similar protocols.

Browser
A software application that enables users to view and interact with information on the World Wide Web.

Bus
(1) The physical network topology in which all workstations are connected to a line directly. (2) Within a computer, the signal path that links the central processing unit with primary memory and with input and output devices.

Byte
The smallest addressable piece of information in a computer's memory, typically consisting of eight bits, used to signify a letter, number or symbol.

Cache Memory
Primarily, short-term storage of data to facility high-speed processing. Although most cache data are deleted with the computer is powered down, some data-access tracking and application-specific information may be retained. Some cache memory must be deleted by command.

Case Mix
The distribution of patients into categories reflecting differences in severity of illness or resource consumption.

Case Mix Index
A measure of relative severity of medical conditions of a hospital's patients.

Centers for Medicare and Medicaid Services (CMS)
The CMS is an organizational unit within HHS and is responsible for administering the Medicare, Medicaid and Children's Health Insurance Programs, as well as the Health Insurance Marketplace.

Chronic Care
Long term care of individuals with long standing, persistent diseases or conditions. It includes care specific to the problem as well as other measures to encourage self-care, to promote health and to prevent loss of function.

Claim
Information submitted by a provider or covered person to establish that medical services were provided to a covered person, from which processing for payment to the provider or covered person is made.

Claims Data
Medical claims data is information found in medical billing claims forms filed on behalf of a group or population. This information is gathered from the medical bills or claims submitted by medical providers to government and private health insurers. The information obtained from medical claims can be used to evaluate the delivery and cost of healthcare as part of evidence-based public health programs. Medical claims data is sometimes called health claims data.

Claim Control Number
A number assigned to a claim that is used to process the claim.

Claim Scrubbing
The process of cleaning claims to make sure they contain all the necessary data elements so that they will be accepted by insurance companies. Usually performed by a clearinghouse.

Clean Claim
An insurance claim that is completed with all the necessary information for the insurance company to process it.

Clearinghouse
An online interface which receives claims from providers, scrubs them to make sure they are clean claims and sends them in batches to insurance companies.

Client (or server) computing (or architecture)
A configuration in which users interact with their machines (called clients) and one or more other machines (called servers) that store data and do much of the computing.

Client Identity
A set of information (typically including name, date of birth, gender and client identifier) that uniquely identifies a client.

Clinical Data Repository
A database that consists of information from various sources of care and from various departments and facilities. The database may represent a longitudinal description of an individual's care.

Clinical Decision Support System
An application that accesses structured databases of clinical information to aid a clinician provider in defining probable diagnoses or in selecting appropriate diagnostic tests or treatment options.

Clinical Information System
A computer system designed for collecting, storing, amending and retrieving information relevant to healthcare delivery.

Clinical Quality Measure (CQM)
A CQM is a tool that helps measure and track the quality of health care services provided to ensure effective, safe, efficient, patient-centered, equitable and timely care. Aspects of patient care measured include patient and family engagement, patient safety, care coordination, population/public health, efficient use of health care resources and clinical process/effectiveness.

Closed system
A completely self-contained system that is not influenced by external events. See also cybernetic system, open system, system.

Cloud Computing
A remote access to data storage and processing functions via the internet without use of or concern for the physical location in which the actual processing or storage systems are housed.

Cloud Storage
An off-premise, distributed storage model; data are stored on the internet, generally through a contractual fee-for-service arrangement.

Computerized Physician (or Provider)
Order Entry (CPOE). A process of electronically entering instructions or orders regarding the diagnosis and treatment of patients.

Configuration Management Database (CMDB)
A knowledge store of solutions, answers and temporary fixes; a knowledge store for system configuration settings that first-level technicians can use to potentially expedite the resolution of an end user's incident.

Connectivity
The capability of information systems to exchange information and data across components and devices.

Controlled Medical Vocabulary (CMV)
A nomenclatures and classification systems of medical terms used to create a standard information infrastructure for capturing, storing, exchanging, searching and analyzing clinical data.

Critical Access Hospital (CAH)
Designation given by CMS to certain rural hospitals that meet specified criteria related to availability of emergency services, bed size, average length of stay and location from any other hospital. The designation entitles the hospitals to certain levels or types of payment and exempts them from Medicare Prospective Payment System requirements.

Current Procedural Terminology (CPT)
The CPT is a series of alpha-numeric codes used to document medical treatment on claims for payment. It is the HIPAA standard code set for medical, surgical and diagnostic services and is maintained by the American Medical Association.

Cyberhygiene
Adherence to good security practices for internet-connected system components.

Cybernetic System
A self-regulating system that contains the following automatic control components: sensor, monitor, standards and control unit. See also closed system, open system, system.

Cybersecurity
A protection of internet-connected information systems from unauthorized access.

Data
Raw facts and figures collected by the organization from clinical encounters, empirical observations or research. Data in and of themselves often have little value and take on meaning only after they are sorted, tabulated and processed into a usable format (information).

Data Breach
Any unauthorized access to information.

Database
A series of records, containing data fields, stored together in such a way that the contents are easily accessed, managed and updated.

Data Dictionary
A file that contains the name, definition, and structure of all the data fields and elements in a database.

Data Field
One piece of information stored.

Database Management System (DBMS)
A software that enables the creation and accessing of data stored in a database.

Data Governance
A process for ensuring that data are maintained according to business and clinical needs, securely protected to meet privacy and regulatory requirements and properly destroyed at the terminal point of their life cycle.

Data Record
A group of individual fields, corresponding to a real-world entity, that are stored together in a database. Demographic and clinical information captured during a patient encounter is one example.

Data Redundancy
is a situation in which the same data item appears in several files of a healthcare organization's computer system.

Data Stewardship
Data stewardship encompasses the responsibilities and accountabilities associated with managing, collecting, viewing, storing, sharing, disclosing or otherwise making use of personal health information. Principles of data stewardship apply to all the personnel, systems and processes engaging in health information storage and exchange within and across organizations.

Data User Agreement (DUA)
In health care, a DUA is a legal document executed between a requestor and holder of data containing protected health information and/or personally identifiable information. Its purpose is to ensure that the requestor adheres to legal requirements associated with privacy and security of the information shared.

Data Warehouse
A collection and organization of data from disparate sources into an integrated, subject-oriented repository to facilitate decision-making.

Decision Support System
A system designed to support the decision-making process of an individual or organization through data retrieval, modeling and reporting. See also clinical decision support system.

Demographics
The patient's information required for filing a claim, such as age, sex, address and family information. An insurance company may deny a claim if it contains inaccurate demographics.

Deterministic System
A system in which the component parts function according to completely predictable or definable relationships with no randomness present.

Diagnosis Related Groups (DRG)
A term used to describe how inpatient claims are paid, based on a formula determined by both diagnosis and procedure codes.

Digital Signal
The representation of data as a series of on/off pulses (ls and 0s). See also analog signal.

Distributed Processing
A computer network topology in which the workload is spread out across a network of computers that can be located in different organizational units or geographical locations.

Discharge
The release (to home, to another hospital or institution) or death of a person who was admitted to a hospital on an inpatient or day surgery basis. It is also referred to as an encounter with the health care system or hospital event.

Documentation
A written information that provides a description and overview of a computer program or system and detailed instructions on its use.

Down-Selection
Reducing a list of potential vendors to a small number of finalists based on criteria for retention before extensive vetting.

Dumb Terminal
A device that can provide input to and display output from a central computer but cannot perform any independent processing.

E-Health Application
A healthcare software delivered through the internet and related technologies.

Electronic Data Interchange (EDI)
Refers to the computer-to-computer exchange of business documents in a standard electronic format between business partners.

Electronic Health Record (EHR)
An EHR is an electronic version of a patient's medical history maintained by a provider over time. It includes key administrative clinical data relevant to a patient's care, such as demographics, past medical history, progress notes, problems, medications, vital signs, laboratory data and radiology reports. Its purpose is to automate access to information to streamline a clinician's workflow and support other care-related activities through various interfaces. This term is often used interchangeably with EMR – Electronic Medical Record.

Electronic Medication Administration Record (eMAR)
An application that tracks medications dispensed to patients and automatically documents them in the electronic health record. Medications may be scanned into the system using barcodes or other electronically readable tags.

Electronic Networking
A data exchange between organizations and business partners to facilitate transactions such as billing and insurance or transfer of patients across the continuum of care.

Encounter
A member visit to the medical group with the intent of seeing a health care provider. There may be a variety of services performed at an encounter, i.e., a brief office visit, EKG, lab test and an immunization.

Encryption
The scrambling of an electronic transmission by using mathematical formulas or algorithms, to protect the confidentiality and security of communications.

Enterprise Resource Planning (ERP)
System A bundled application that integrates operational information derived from finance, human resources, materials management and other function-based areas into a robust database used to achieve business management objectives.

Episode of Care
All treatment rendered in a specified time frame for a specific disease.

Ethernet
The trade name for a logical network topology used to control how devices on the network send and receive messages. The goal is to prevent "collisions" between two devices attempting to send messages simultaneously.

Events
A term which refers to any medical service a patient receives and can include, but is not limited to hospitalizations, outpatient procedures of diagnostic tests, physical therapy, etc.

Evidence-Based Medicine and Evidence-Based Management (EBM)
A movement to explicitly use the most current, best scientific evidence available for managerial or medical decision-making.

Executive Information System (EIS)
An organized data storage, retrieval and reporting system that is designed to provide senior management with information for decision-making.

Expert System
A decision support system that can approximate a human decision-maker's reasoning processes. It can assist in reaching a decision, diagnosing a problem or suggesting a course of action.

Extranet
A private computer network an organization shares with customers and strategic partners using internet software and transmission standards.

Fee-for-Service (FFS)
In health care, this is a payment model where services performed are unbundled and separately reimbursed.

Fiber-Distributed Data Interchange (FDDI)
A network consisting of two identical fiber-optic rings connected to local area networks and other computers.

Fiber-Optic Medium
A communication-transmission medium that uses light pulses sent through a glass cable at high transmission rates with no electromagnetic interference.

File (or Server) Architecture
The physical and logical configuration of the data storage components of a networked system.

File Transfer Protocol (FTP)
This term refers to a standard network protocol used for the transfer of computer files between a client and server on a computer network. The protocol is built on a client-server model architecture and uses separate control and data connections between the client and the server.

Firewall
A hardware and software that restricts traffic to and from a private network from the general public internet network.

Flat File
This term usually refers to a file that consists of a series of fixed-length records that include some sort of record type code.

Front-End Processor
The processor with which application users interact directly. In a client/server network, the front-end processor would correspond to the client.

Gateway
The interface between two networks, that use dissimilar protocols to communicate.

Global Area Network (GAN)
The use of wireless technology to extend a computing network beyond the geographic limits of a hard-wired network.

Governance
The way organizational leaders manage the conflict of interest that occurs when operational authority of an entity or unit is delegated to nonowners and used to define decision rights and accountabilities.

Graphical User Interface (GUI)
A particular interface between the human user and the computer to manage the functioning of the software and hardware that employs icons (graphical symbols on the monitor screen) to represent available operating system commands.

Grid Computing
A distributed computing model whereby multiple internet connected computers emulate a supercomputer.

Groupware
A collaborative software that enables sharing of information via an interactive network.

H4 Technology
Information Technology Company that is responsible for building NHIS View and reorganization of NHIS systems.

Hardware
The physical components of a computer system.

Health Information Exchange (HIE)
An HIE allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically to improve the speed, quality, safety and cost of health care. There are three key forms: direct exchange of information between providers, query-based exchange so providers can find or request information about a patient from another provider and consumer-mediated exchange so patients can aggregate and control the use of their health information among providers.

Health Information System (HIS)
This term refers to any system that captures, stores, manages or transmits information related to the health of individuals or the activities of organizations that work within the health sector.

Health Information Technology (HIT)
This term refers to health information management across computerized systems and the secure exchange of health information between consumers, providers, payers and quality monitors.

Health Information Technology for Economic and Clinical Health (HITECH) Act
A component of the American Recovery and Reinvestment Act that specifically promotes widespread dissemination and adoption of EHRs through provider incentives.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Public Law 104-191 provides, among other things, data privacy and security provisions for safeguarding medical information.

Health Level Seven (HL7)
A standard for data formatting that helps to facilitate the exchange of data among disparate systems within and across software vendors.

Healthcare Common Procedure Coding System (HCPCS)
A set of health care procedure codes based on the American Medical Association's Current Procedural Terminology (CPT) with two levels, the first being the CPT codes. The second level of codes is used to bill for other medical and health services, including those rendered by non-physician practitioners and a wide range of other providers.

Healthcare Cost and Utilization Project (HCUP)
A federal study undertaken by the Agency for Healthcare Research and Quality to create a national database for research into the efficacy and costs of U.S. health care.

Healthcare Effectiveness Data and Information Set (HEDIS)
A tool used by more than 90 percent of America's health plans to measure performance on important dimensions of care and service. Entrusted to the NCQA, the measurement development process has expanded in size and scope to include measures for physicians, preferred provider organizations, and other entities.

Help Desk
Also called Service Desk, provides in-person, telephone or email access to trained personnel who can assist IT users in the resolution of equipment malfunctions and incidents or to answer technology-related questions.

Hospital Day
A term to describe any 24-hour period commencing at 12:00 a.m. or 12:00 p.m., whichever is used by a hospital to determine a hospital day, during which a patient receives services at the hospital.

Host
A computer to which other, smaller computers in a network are connected and with which it can communicate.

Hub
A hardware device with multiple user ports to which computers and input/output devices can be attached.

ICD-10
The 10th revision of the International Statistical Classification of Diseases and Related Health Problems (ICD), a medical classification list by the World Health Organization (WHO). It contains codes for diseases, signs and symptoms, abnormal findings, complaints, social circumstances and external causes of injury or diseases.

Incident Management
The processes designed to restore normal operations following a disruption of service.

Information
Data or facts that have been processed and analyzed in a formal, intelligent way so that the results are directly useful to clinicians and managers.

Information Technology
This term refers to the application of computers to store, study, retrieve, transmit and manipulate data, or information, often in the context of a business or other enterprise.

Information Technology Infrastructure Library (ITIL)
Framework of how HIT department processes should be interlinked to gain optimum proactive HIT service management.

Inpatient
A patient admitted to a hospital, who is receiving services under the direction of a physician for at least 24 hours.

Input
Data fed into a computer system, either manually (such as through a keyboard or bar-code device) or automatically (such as in a bedside patient monitoring system).

Integrated Services Digital Network (ISDN)
Network that uses a telephone company branch exchange to allow separate microcomputer workstations, terminals and other network nodes to communicate with a central computer and with each other.

Integrated System
Set of information systems or networks that can share common data files and can communicate with one another.

Internet of Things (IoT)
Entirety of devices and objects with unique identifiers that transmit data over the internet without an intermediary person or device. Examples include wearable medical sensors and home environment management systems.

Internet Protocol (IP)
Addressing scheme that identifies each machine on the internet and is made up of four sets of numbers separated by dots.

Interoperability
Ability of health information systems to effectively transmit and share medical information across organizations.

Intranet
Private computer network contained within an organization that uses internet software and transmission standards.

Legacy System
Computer application designed to meet specific operational needs. Usually developed independent of a broad organizational information management or information technology plan and often is not compatible with newer integrated systems.

Life Cycle
The sequence of specification, design, implementation, and maintenance of computer programs. For models of computer hardware, the life cycle is the sequence in market status development, announcement, availability and obsolescence.

Local Area Network (LAN)
A computer network enabling communication among computers and peripherals in an organization or group of organizations over a limited area. The network consists of the computers, peripherals, and communication connections, either hardwired or wireless.

Magnetic Storage
The online or offline data storage in which each data character is stored as a O or 1 in magnetic form. Magnetic storage includes magnetic disks and tapes.

Mainframe
A large computer system that normally has very large main memories, specialized support for high-speed processing, many ports for online terminals and communication links and extensive auxiliary memory storage.

Master Patient (or Person) Index (MPI)
is a relational database containing all of the identification numbers that have been assigned to a patient anywhere in a healthcare system. The MPI assigns a global identification number as an umbrella for all of a patient's numbers, thus permitting queries that can find all appropriate data for a particular patient regardless of where that person was treated in the system.

Meaningful Use (MU)
Refers to the use of certified EHR technology to improve quality, safety and efficiency; reduce health disparities; engage patients and family; improve care coordination as well as population and public health; and maintain privacy and security of patient health information. MU sets specific objectives that eligible hospitals and eligible professionals must achieve to qualify for federal incentive programs and to receive EHR Incentive payments.

Medical Device Integration
Involves incorporating data from medical devices into the electronic health record without manual intervention.

Medical Tourism
Involves traveling across country, borders for healthcare, including elective and needed surgical procedures to achieve better quality, lower cost or more timely services.

Medical Record Number (MRN)
A unique number that identifies a patient. May also be referred to as a chart or account number.

mHealth application
A health- and healthcare-related information, tools and other resources that can be accessed on mobile devices.

Microcomputer
A relatively small computer system in which the microprocessor, main memory, disk drives, CD-ROM and interface cards and connectors are installed in a small case or box. See also microprocessor.

Microprocessor
A CPU contained on a single semiconductor chip.

Middleware
The system architecture in which applications are connected to and distributed by networked systems.

Minicomputer
A computer with capabilities somewhere between those of a microcomputer and of a mainframe computer. See also mainframe, microcomputer.

Modem (Modulator/Demodulator)
A data-communication device that modulates signals from output devices for transmission on a data link and demodulates signals destined for input devices coming from the transmission link.

MS-DRG Grouper
Software program managed by CMS that is designed to assign the DRG classification.

Multiplexing
The process of combining two or more signals into a single signal, transmitting it and then sorting out the original signals. The devices that combine or sort out signals are called multiplexers.

Multisourcing
Involves outsourcing information system functions and tasks to a number of different vendors. See also outsourcing.

National Provider Identifier (NPI)
Given to each provider or medical facility/office that bills for services.

Nebraska DHHS State Mandates
Data reporting mandates that require hospitals to submit data for different conditions or injuries (see below). NHA submits that data to DHHS on a monthly and yearly basis for the hospitals.

- External Cause of Injury (Neb. Rev. Stat. 71-2078 to 71-2082; NAC 186-3)
- Head, Brain & Spinal Injury (Neb. Rev. Stat. 81-653 to 81-661; NAC 186-2)
- Ambulatory Surgical Center (Neb. Rev. Stat. 81-6,111 to 81-6,119; NAC 186-6)
- Communicable Diseases (Neb. Rev. Stat. 71-532; NAC 173-1)
- Parkinson Disease Registry (Neb. Rev. Stat. 81-697 to 81-6,110; NAC 186-4)
- Cancer Registry Early Case Capture (Neb. Rev. Stat. 81-642 to 81-650; NAC 186-1)
- Contagious, Infectious, or Poisoning (Neb. Rev. Stat. 71-503)

Network
A collection of computer and peripheral devices interconnected by communication paths. See also local area network, wide area network, global area network.

Network Computer
A low-cost personal computer that has minimal equipment and is designed to be managed and maintained by a central computing function.

Network Configuration
The established connections between the components of a network; the physical and logical topologies.

Network Controller
A mini- or microcomputer that directs the communication traffic between the host and the terminals and peripheral devices.

Network Interface Card (NIC)
A plug-in board used in microcomputers and workstations to allow them to communicate with a host computer and other nodes in a local area network.

NHA Care Compare
Website managed by NHA that provides information on hospital pricing and quality, provides links to individual hospitals here in Nebraska and answers commonly asked questions about bills for health care services. The web site may be accessed at www.nhacarecompare.com.

NHA Market Analysis Subscription
Web portal that contains inpatient and outpatient market area analytics and charts. Has a module that allows subscribers to pull custom data and place individual filters.

NHA Pricing Guide
Report or online service created by NHA that compares CPT codes charges across Nebraska hospitals.

Open System
A system whose components are exposed to everyone and can thus be modified or improved.

Operating System
A set of integrated subroutines and programs that control the operation of a computer and manage its resources.

Operational Management System
A non-patient care information system, such as financial, purchasing, or office automation applications.

Optical Disk
A disk in which data are written and read by a laser. Optical disk types include a number of variations of CDs and DVDs.

Outpatient Care
Care given a person who is not bedridden. Also called ambulatory care. Many surgeries and treatments are now provided on an outpatient basis, while previously they had been considered reason for inpatient hospitalization.

Output
Any data or information that a computer sends to a peripheral device or other network.

Outsourcing
Delegation of responsibility for specific organizational tasks or functions to an external entity on a contract basis. Examples include software development and accounts receivable collection.

Parallel Processing
The use of multiple CPUs linked together generally for the purpose of more efficiently completing complex tasks.

Patient Portal
A mechanism by which patients can access a component of the enterprise information system; generally intended to increase patient engagement in the care experience and in the enterprise itself.

Patient Protection and Affordable Care Act (ACA)
2010 legislation extended HIPAA rules by requiring a unique health plan identifier and by setting standards and rules for financial transactions.

Peer Network
A decentralized computing environment in which each computer on the network has either data or some hardware resource that it can make available to the other users on the network.

Peripheral Devices
A general term used to refer to input, output and secondary storage devices on a computer.

Personal Health Information (PHI)
Any health information, in any medium, that can be identified as related to an individual.

Picture Archiving and Communication System (PACS)
A device that provides online storage and retrieval of medical images for transmission to user workstations.

Population Health / Population-Based Needs Care
Looks at the health care needs of a specific population and making health care decisions for the population as a whole rather than for individuals. Health care practitioners using similar treatment recommendations or guidelines for populations with a specific disease, injury or illness.

Portfolio
A collection of programs and projects undertaken by an organization.

Portfolio Management
The process of selecting and managing the organization's programs and projects, including valuing existing and proposed projects against strategic business and clinical objectives for investment decisions.

Portfolio Management Office (PMO)
A central organization dedicated to improving the practice and outcomes of projects via holistic management of all projects. This includes the professional management and oversight of an organization's entire collection of projects. The terms PMO, project management office, and program management office; are used interchangeably.

Primary Storage
Internal memory where data to be processed are stored for access by the CPU-or in the broader sense, repositories for frequently accessed transactional data.

Principal Diagnosis
The medical condition that is ultimately determined to have caused a patient's admission to the hospital. The principal diagnosis is used to assign every patient to a diagnosis-related group. This diagnosis may differ from the admitting and major diagnoses.

Probabilistic Algorithm
A decision support system that employs statistical probabilities rather than relying solely on knowledge collected from expert human beings.

Procedure
An action taken to fix a health problem or to learn more about it. For example, surgery, tests and putting in an IV (intravenous line) are procedures.

Program
Is (1) an ordered set of instructions that a computer executes to obtain a desired result, or (2) a group of related, often interdependent projects being conducted in an organization.

Programming Language
A software system that has a specific format, or syntax, used for writing computer programs.

Protected Health Information (PHI)
Under US law, this term refers to any information about the health status, provision of health care or payment for health care that is created or collected by a covered entity, is transmitted by or maintained in electronic media or other form or medium and can be linked to a specific individual.

Provider
Any healthcare professional licensed to prescribe or write an order, including physicians, midwives, nurse practitioners, clinical pharmacists and dentists.

Quadruple Aim
A national initiative to improve health outcomes, lower costs of healthcare, improve physician satisfaction and provide better patient experiences.

Quality Assurance (QA)
As it relates to health care, this term means maintaining a high quality of care by constantly measuring the effectiveness of the providers and organizations providing it.

Radio Frequency Identification (RFID)
An automatic identification method that relies on storing and remotely retrieving data using devices called transponders or RFID tags. The RFID tag can be applied to a product, an animal, or a person for the purpose of identification using radio waves.

Random Access Memory (RAM)
Storage that permits direct access to the data stored at a particular address on a computer's hard drive. Data stored in RAM are deleted when the computer is powered off.

Ransomware
A form of malware, or malicious software, that invades a host computer to encrypt the victim's files. The attacker demands a ransom to restore access to the files.

Read-Only Memory (ROM)
Storage that contains permanent instructions or data that cannot be altered by ordinary programming.

Real Time
Describes a computer or process that captures data, performs an operation or delivers results in a time frame that humans perceive as instantaneous.

Registers
High-speed CPU memory; employed during processing activity.

Relational Database
A type of database that stores data in individual files or tables, with data items arranged in rows and columns. Two or more tables can be linked for the purposes of ad hoc queries if at least one data item (the "key") is common in each of the tables.

Revenue Cycle Management
A process encompassing the business and clinical activities associated with generating and receiving revenue through patient care.

Router
A device located at a gateway that manages the data flow between networks-See also gateway.

Secondary Storage
Occurs on various devices and media designed to maintain small or large quantities of data, generally for archival purposes or infrequent access.

Secure File Transfer Protocol (SFTP)
A network protocol for accessing, transferring and managing files on remote systems. SFTP allows businesses to securely transfer billing data, funds and data recovery files. SFTP uses SSH to transfer files and requires that the client be authenticated by the server. Commands and data are encrypted in order to prevent passwords and other sensitive information from being exposed to the network in plain text. This is also called SSH File Transfer Protocol.

Service Continuity Management
The process for restoring HIT services as quickly as possible after a service interruption.

Service-Level Agreement (SLA)
A contract between an HIT department and specific customers that describes the services to be provided or the deliverable, along with other details.

Software
Programs that control the operation of a computer, including applications, operating systems, programming languages, development tools and language translators.

Strategic decision support system
The system that extracts data from clinical and management information systems and external data sources to enable analyses that support planning, managerial control and outcomes assessment.

Swing Beds
Acute care hospital beds that also can be used for a different level of care.

Synching station
A device wired to a computer that allows data to be exchanged between a personal digital assistant and a personal computer so that current data are available on both.

Syndromic Surveillance
Syndromic surveillance is the collection and analysis of health data about a clinical syndrome that has a major impact on the health of the population. Currently collected by DHHS from participating hospitals. Collects clinical data from hospitals, that includes chart information and clinical notes but not billing information.

System
A network of components or elements joined together to accomplish a specific purpose or objective. Every system must include input, a conversion process and output. See also closed system, cybernetic system, open system.

Systems Analysis
The process of collecting, organizing and evaluating facts about information system requirements and processes and the environment in which the system will operate.

Taxonomy Code
Medical billing specialists utilize this unique code set for identifying a healthcare provider's specialty field.

Telecommunications
The transmission of information over distances through wired, optical or radio media.

Telehealth
The telehealth visit type is used when the client does not attend in person nor is seen in person off-site. All contact is verbal or written.

Telemedicine
Also referred to as telehealth and e-health, this is a rapidly developing application of clinical medicine that employs communications and information technologies to assist delivery of care (consulting, medical procedures or examinations).

Terminal
A device consisting of a monitor and keyboard that allows a computer user to perform processing on a host computer directly. See also dumb terminal.

Terminal-Host System
A centralized computer network configuration in which dumb terminals are connected to a large central host computer (typically a mainframe) and all the computing takes place on the host computer. See also host, mainframe, terminal.

Thin Client
A system architecture in which most processing is performed on a server remote from the end user or client.

Three-Tier Architecture
A configuration in which the user interface resides with the client, the relational databases reside on one server and the application programs reside on a second server. Three-tier system offers faster information processing and distribution than does a two-tier system.

Throughput
The total time span from collection of the first data element to the preparation of the final report in a given system.

Total Cost of Ownership
A financial measure that incorporates both startup (one-time) and recurring costs associated with technology purchases, such as training costs, costs associated with failure or outage and recovery from security breaches and other hidden costs.

Transaction Processing Systems
Application programs that form the bulk of the day-to-day activities of an organization, such as financial, clinical, admissions, and business office systems.

Transmission Control Protocol/Internet Protocol (TCP/IP)
A collection of data communication protocols used to connect a computer to the internet. TCP/IP is the standard for all internet communication.

21st Century Cures Act
A law, enacted in 2016, intended to accelerate medical product development and bring innovations to market faster.

Two-Tier Client (or Server) Architecture
A system in which all back-end functions (database management, printing, communication, and applications program execution) are performed on a single server.

UB-04
The standardized claim form for use by inpatient hospital billing.

Voice Over Internet Protocol (VOIP)
The delivery of voice communication and multimedia sessions via the internet.

Web Browser
Software that enables a user to view and interact with information stored on the web.

Wide area network (WAN)
Involves a computer system connectivity over a large geographic region using telecommunication networks.

Workstation
(1) a microcomputer connected to a larger host computer in which some independent processing is performed. (2) a high-end microcomputer with a large amount of primary storage, a fast processor, a high-quality sound card, high-resolution graphics, a CD-RW drive and in many cases a DVD drive or (3) any computing device that allows users to input, process or retrieve data or information necessary to perform their job duties.

835
Term used to describe code set that provides claim payment information after 837 is submitted.

837
Term used to describe the code set for submitting medical claims electronically.

Samples

SAMPLE POLICY

PURPOSE: The purpose of this Standard is to detail the method for managing FACILITY data and Information Assets.

SCOPE:

In order to effectively manage information security risks and to secure FACILITY's data, there must be a vocabulary that can be used to describe the data and to quantify the amount of protection required. This policy defines the major categories into which all FACILITY data can be divided into and the roles and responsibilities of maintaining them. It covers all FACILITY data and Information assets owned, leased, or otherwise provided to FACILITY, regardless of location. Also covered by the Standard are hardcopies of FACILITY data, such as printouts, notes, etc.

This document supports section 3 of the Information Security Policy

POLICY:

A. Data Classification

Data owned by FACILITY must be continually evaluated and classified according to the Data Classification Model within this document. This model will be used to determine the appropriate data restrictions for data stored, processed, or transmitted within or on behalf of FACILITY. Such restrictions include but not limited to authorized access and modifications.

Data Classifications apply to FACILITY owned data independent of where it resides, and in no way supersedes any state or federal government classifications. Data that is not categorized from the categories below will default to the highest applicable data classification.

Inventory Tracking

In addition, it is recommended that data classifications be applied to assets which are tracked in an Information Technology asset management database. Such items include and are not limited to:

- Applications
- Databases
- Documents
- Medical devices
- Storage devices
- Credit card processing systems that are either remote hosted or on premises.

See the FACILITY Information Technology Asset Management Standard

B. Roles and Responsibilities

The various department heads of the FACILITY are considered Data Trustees that own a multitude of types of documents, applications, and data. Each department head must classify their data according to Section C and the Data Classification Model. Information Security may assist with the classification process and coordinate with the business units to achieve consistency across the FACILITY. Data

Trustees may appoint directors and/or managers to help define, implement, and enforce data management policies and procedures within their specific business domains.

Term: Data Trustee

> Definition: Individuals defined as institutional officers, (i.e. Vice Presidents, Vice Provosts, Deans, Chancellors, etc.) who are appointed by the President and have the authority, accountability, and ownership over budgets, rules, policies, standards, guidelines, and procedures regarding their business data and the access and usage of that data within their delegations of authority.

C. Classification Levels

Public Data

Public data is information that may be disclosed to any person regardless of their affiliation with FACILITY. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the FACILITY community and no steps need be taken to prevent its distribution.

Examples of Public data include: press releases, course catalogs, and applications for hire, request forms, and other general information that is openly shared. The type of information a department would choose to post on its website is a good example of Public data.

Sensitive Data

Sensitive (confidential) data is information that, if made available to unauthorized parties, may adversely affect individuals or the business of FACILITY. This classification also includes data that the FACILITY is required to keep confidential, under a confidentiality agreement with a third party, such as a vendor. This classification extends to intellectual property such as policies, procedures, forms, design layouts, configuration standards, physician contracts, performance reporting. Sensitive data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

Any unauthorized disclosure or loss of Sensitive data must be reported to the head of the FACILITY Compliance department.

Minimum security controls of this data classification include:

- Authorized access definitions
- Authorized modification definitions
- Record retention and disposal definitions
- Backup and restore definitions
- File storage restrictions

FACILITY's obligations will depend on the particular data and the relevant contract or laws.

Examples of Sensitive data include:

- Information covered by contractual obligations
- Data used for research and performances reporting that has de-identified PHI
- Personally identifiable information entrusted to our care that is not Restricted data or covered under federal, state or local regulations.
- FACILITY ID Number, when stored with other identifiable information such as name or e-mail address
- Information covered by the Gramm-Leach-Bliley Act (GLB), which requires protection of certain financial records.
- Information that is the subject of a confidentiality agreement.
- FACILITY intellectual property rights, such as policies, procedures, financial forms, physical and logical design documents.
- Recordings of Zoom meetings.

Restricted Data
Restricted data includes any information that FACILITY has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. Where unauthorized disclosure or loss of this data (a data breach) would result in potential civil penalties for the organization and its board members, require FACILITY to notify State and Federal authorities, affected individual(s), and local news outlets which would negatively impact FACILITY's reputation.

Security controls of this data classification includes:

- Authorized access definitions
- Authorized modification definitions
- Authorized disclosures
- Access monitoring
- Encryption protection
- Third party data use/sharing agreements (i.e. Business Associate Agreements, connectivity agreements VPN's)
- Record retention and disposal definitions
- Backup and restore definitions
- File storage restrictions
- Periodic risk assessments

Any unauthorized disclosure or loss of Restrictive data must be reported to the head of the FACILITY Compliance department.

Examples of Restrictive data include:

- Information used to communicate to individuals that authenticate and authorize access to electronic resources, such as passwords, keys, and other electronic tokens.
- "Criminal Background Data" that might be collected as part of an application form or a background check
- Student data.
- Individual employment information, including salary, benefits and performance appraisals for current, former, and prospective employees. Legally privileged information.
- Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA), which sets standards for protection of medical records and patient data.

- Financial account numbers covered the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored. See the Credit Card Processing Policy.
- Legal/court documents that are not public knowledge.
- U.S. Government Classified Data
- Restricted Use data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of Restricted Use data must be reported to FACILITY Compliance.

	Restricted Data (high level of sensitivity)	Sensitive Data (moderate level of sensitivity)	Public Data (low level of sensitivity)
Legal Requirements	Protection of data is required by law, regulation and/or statute	Protection of data is required by contractual obligation	Protection of data is at the discretion of the owner
Access	Only authorized individuals with approved access, signed confidentiality agreements, and a business need to know	Only authorized individuals with approved access, signed confidentiality agreements, and a business need to know	FACILITY affiliates and general public with a need to know

Examples	• Protected Health Information (PHI)[1]
	• Personally Identifiable Information (PII)[2]
	• Employee information[3]
	• Financial information[4]Student Data[5]
	• Information covered by regulatory requirements
	• Credit Card holder information
		• Internal use only :
		  ○ Financial forms
		  ○ Communications
		• Information covered by confidentiality agreements that is not specifically classified as “Restricted”
		• Contracts
		• Internal Employee Directory
		• Physical design detail or building blueprints
		• FERPA Directory Information[6]
		• Intellectual Property
		• Recordings of Zoom meetings
			• FACILITY company history
			• Business contact data
			• Company directory

[1]Protected Health Information (PHI) is all individually identifiable information that relates to the health or health care of an individual and is protected under federal or state law.

[2]Personally Identifiable Information (PII) is any data about an individual that could, potentially identify that person, such as a name, fingerprints or biometric data, email address, street address, telephone number or social security number, and is protected under federal or state law.

[3]Includes employment applications, personnel files, benefits information, salary, birth date, and personal contact information.

[4]Includes Primary Account Numbers, taxpayer identification numbers, privileged contract information, etc.

[5]Includes non-directory information as defined by FERPA - social security number, student ID's, Race, ethnicity, and/or nationality, Gender, Transcripts: grades, financial information Includes student's name, address and telephone listing, date and place of birth, field of study, previous schools attended, academic class, enrollment status, dates of attendance, academic awards and degrees, photographs, e-mail address, graduation date, advisor, achievements in campus organizations, class rosters, class schedules.

D. Data Retention

Documentation

a) The CIO shall be responsible for maintaining all information security policies, Standards and procedures. This documentation shall be made available for all FACILITY workforce members and Users.

b) The CIO shall be responsible for ensuring that any action, activity or designation required under information security policies, Standards and procedures is maintained in paper and/or electronic form. All such documentation shall be maintained as specifically required.

Documentation Retention

a) All information security documentation, and all revisions of information security documentation, shall be retained for six (6) years from the date of its implementation.

b) No information security documentation shall be destroyed before consultation with the CIO and/or Outside Legal Counsel.

For more specific implementation guidance, please see the Record Retention Schedule.

REFERENCES:

FACILITY Information Technology Information Security Policy
FACILITY Information Technology Asset Management Standard
FACILITY Credit Processing Policy
FACILITY Record Retention Schedule
FACILITY Information Technology Removable Media Standard
FACILITY Information Technology Secure Clear Desk Clear Screen Standard
Use of De-Identified Data Policy

FACILITY CONTROLS

FACILITY Controls ISO: 27002:2013 - 8.2.1

RELATED REGULATIONS:
HIPAA 164.308(a)(ii)(B)
164.530(c)(1)

PCI-DSS 3.2

APPLICABILITY: This document is part of FACILITY's security program and has the security classification of “Sensitive”. The information contained within can only be shared within the organization and cannot be modified without the proper authorization by the individuals listed in the attached signature page. Other Policies, Standards and Procedures may apply to the topics covered in this Standard, and as such the applicable documentation should be reviewed and applied as needed.

ENFORCEMENT: Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

POLICY STATEMENT
To correct identification, demographic, payer and clinical information errors in compliance with the appropriate governing body regulations and internal policies.

PURPOSE
This policy addresses the identification and correction of patient, guarantor, coverage, and patient contact demographic information and clinical documentation errors. Such errors may be entered and disseminated via registration, scheduling, and billing activities, interfaced to all Electronic Health Record (EHR) service areas, other systems, and entity or accessed via the patient web portal.
Issues resulting in care issues or clinical documentation errors must be communicated to the Health Information Management (HIM) team and immediately addressed according to the Chart Correction policy and procedures.

PROCEDURE
The process for responding to identified occurrences includes completely identifying the nature and the cause of the error; correcting the information and performing service recovery in the required timeframe.
Root cause analysis, staff re-education and potential corrective actions will be performed and documented. These steps are to be performed in compliance with the appropriate governing body regulations and internal policies.

Identification:
When an error is identified the person identifying the error will report the issue according to their department policy. The designated individual(s) flag the patient or accounts as below and then conduct a preliminary investigation. If there is an imminent patient safety issue the HIM team should be notified immediately. Once errors are identified they must be communicated to the internal error documentation system as soon as possible and no later than 24 hours after identification.

Flagging:
The EHR portal will be assessed and if the patient(s) involved are active and another patient's information is visible due to the error, the account must be disabled until the error correction process is completed. Once erroneous information has been removed from the account the EHR portal account can be re-enabled.

Upon notification the designated individual(s) will immediately place a hold on the patient and/or guarantor accounts according to departmental policy.

Notification:
The Privacy Incident Reporting form will be completed and communicated to HIM by designated individual according to departmental policy.

Error Diagnosis:
The designated individuals charged with investigating the error will determine which of the following errors exist. This investigation may require contacting the patient(s) or person(s) reporting the error. Items to be investigated may include but are not limited to the following:

- Incorrect Patient

- Patient Demographic Type-Over
- Guarantor Demographic Type-Over
- Incorrect Guarantor Attached
- Incorrect Patient Contact
- Additional Patients involved
- Erroneous default hospital account
- Incorrect coverage attached or billed
- Statements attached to the wrong guarantor
- Future appointments

Error Correction:
After completion of the Privacy Incident Reporting Form, the HIM team will correct the errors and document their actions. Any additional errors found should be added to the form and communicated to the HIM team immediately if significant. HIM member will follow their documented process to correct errors.

Completion and Documentation
The HIM team is responsible for reviewing the Privacy Incident form and documenting that each section has been completed. The HIM Lead, HIM Document Services has oversight to monitor each form for completeness and follow up with areas/items remaining incomplete. Once the Privacy Incident form is completed it will be moved to the completed folder within the documentation folder and maintained for future reference if needed.
This documentation must be retained for a minimum of 6 years

Release:
Each area will remove the flagging or holds once the information has been corrected. Once PDFs are removed, the EHR patient account will be re-enabled.

Time Frame:
Errors reported to the HIM team must be completely resolved within 5 days. Exceptions will require notification to the HIM team with reasons for the delay. The reasons for an exception to the 5 day time frame will be documented on the Privacy Incident form.

Education/Coaching and Corrective action:
The HIM team will maintain a spreadsheet to track the users responsible for the error. Once the Privacy Incident form has been completed representatives from the HIM team will complete the coaching form outlining the error and the correct process. The spreadsheet and all coaching forms will be maintained within the documentation folder.

EMPLOYEE EDUCAITON/FOLLOW UP

The manager of the employee responsible for the error will receive an email copy of the Education Form.
Managers will be expected to follow up with the identified employee and coordinate follow up step with the Privacy Office and HR. Follow steps include re-education, training, coaching and corrective action when appropriate.

DESTRUCTION OF CONFIDENTIAL INFORMATION

Purpose:
To establish guidelines for the proper destruction of confidential information

Policy:
1. It is the policy [Entity] and its affiliated entities to ensure the privacy and security of confidential information in the maintenance, retention and eventual destruction/disposal of such media. All destruction/disposal of confidential information media will be done in accordance with federal and state law and pursuant to Record Retention policy. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
2. Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If a preservation notice is received the record retention schedule shall be suspended for these records until the preservation notice terminates.
3. Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of the information is complete.
4. Private and confidential information shall be destroyed/disposed of using a method that ensures the information cannot be reconstructed or read. For purposes of this policy, confidential information means individually-identifiable health information (protected health information) and proprietary information, including contracts, business plans and practices, financial information, employee records and meeting minutes.
5. Individuals who know or suspect that confidentiality has been breached by another person or persons have a responsibility to report the breach to the respective supervisor or to the Human Resources Department. Employees should not confront the individual under suspicion or initiate investigations on their own, as such actions could compromise any ensuing investigation. All individuals are to cooperate fully with those performing an investigation pursuant to this policy.

Procedure:
1. If destruction/disposal services are contracted, the contract must provide that the contactor (business associate) will establish the permitted and required uses and disclosures of information as set forth in the federal and state law (in accordance with Contract Management Policy) and include the following elements:
    a. Specify the method of destruction/disposal
    b. Specify the time that will elapse between acquisition and destruction of data/media
    c. Establish safeguards against breaches in confidentiality
    d. Indemnify the organization from loss due to unauthorized disclosure
    e. Require that the contractor (business associate) maintain liability insurance in specified amounts at all times the contract is in effect
    f. Provide proof of destruction/disposal
2. Confidential information shall be disposed of according to the table below:

Medium	Destruction Procedure(s)
Paper	All paper should be disposed of in the desk-side recycling bins, the recycling carts or shredded in a shredding machine. All paper is considered confidential in the recycling process. Food waste and toiletry products are excluded and should not be placed in the recycling bins.
Audiotapes/Videotapes	Tape over the information or forward the audio/videotape to Environmental Services in a sealed package for destruction.
CD ROMs/ DVDs	Cut in two and dispose of in trash. *Large volumes of CDs may be forwarded to Environment Services.

1

Medium	Destruction Procedure(s)
Cell Phones	Cell phones which are no longer in use shall be returned to Information Services. Information Services shall dispose of the equipment.
Computerized Data/Hard Disk Drives (NOTE: This includes hard drives in any devices, including copy machines or devices with non-removable hard drives)	This section includes tablet devices (such as iPads, Samsung Tablets, etc.) as well as laptops with non-removable hard drives (such as MacBooks or Surface computers). Requestor will enter a Service Request containing the following information: 1. Request to decommission a data/hard disk storage device 2. A statement that records are being destroyed in the normal course of business pursuant to Record Retention Policy 3. Name of the department representative authorizing data destruction 4. Phone number of representative authorizing destruction 5. Requestor will then arrange secure delivery of devices to PC Support. 6. PC Support will receive and will securely store the devices until physically destroyed. 7. Final destruction and salvage takes place in IT. 8. Questions regarding this process can be directed to PC Support NOTE: In the circumstances where a copier is being traded out, PC Support will ensure that the hard drive is secured by following their internal procedures. NOTE 2: PC Support may, at its discretion, use data wiping tools to enable reuse of certain hard drives. PC Support will follow NIST Special Publication 800-88 Guidelines for Media Sanitization which authorizes using the DOD certified standard 5022.22, 3X for wiping
Cassette Tapes/Magnetic Media	Forward to Environmental Services in a sealed container for destruction.
Computer Diskettes/Floppy	Forward to Environmental Services in a sealed container for destruction.
Laser Disks	Forward to Environmental Services in a sealed container for destruction.
Microfilm/Microfiche	Forward to Environmental Services in a sealed container for destruction.
Photographs	Photographs should be shredded or cut in multiple pieces. Photographs should not be placed in recycling containers.
Radiology Films	Refer to Radiology Dept. Policy
Printer Ribbons	Forward to Environmental Services in a sealed container for destruction.
Other	Follow federal/state requirements; contact Environmental Services or Privacy Officer for further information.

Destruction of Paper

1. Handling and Security Procedures

   a. Departmental management and Environmental Services should jointly develop a plan for the security, transport and storage of confidential materials from customer departments to the secured locked containers. The placement of the secured locked containers will be jointly developed between departmental management, Recycling Coordinator and Environmental Services
   b. Locked containers should not be tampered with by unauthorized [Entity] employees
   c. Environmental Services will be responsible for issuing and logging the keys for unlocking these containers
2. Documentation of Secure Disposal
   a. The Certificate of Destruction for all recycled confidential material will be kept on file in the Recycling Coordinator's office

Data Governance Charter

PURPOSE

Data Governance is a key driver of an organization's approach to data management. The Data Governance Committee (DGC) will oversee the people, processes, and information technology required to create consistent and proper handling of data and understanding of information across the organization. Information is treated as an organizational asset and is readily available to support evidence-based decision-making and informed action to improve clinical, operational, financial, and patient experience outcomes.

SCOPE

The DGC provides a leadership role in the sequencing and prioritization of the organization's information and data management goals, standards, practices, and processes to ensure alignment with the strategies of the organization. The DGC will provide recommendations on how to improve data quality, ensure a balance between data access and data security, prioritize data acquisition efforts, and raise the level of data literacy across the health center.

RESPONSIBILITIES

As a strategic, cross-functional decision-making entity, the DGC will be responsible for the following:

- ***Vision and Direction:*** Set the vision and direction for the future of Data Governance.
- ***Oversight and Decision-Making:*** Act as a centralized hub, to make decisions and provide oversight on key data initiatives
- ***Strategic Alignment:*** Champion and align the Data Governance Strategy with organization strategy
- ***Data-Driven Culture:*** Instill and promote an organizational climate that embraces the use of data in achieving organizational goals and making positive change through
- ***Oversight and Decision-Making:*** Act as a centralized hub, to make decisions and provide oversight in relation to key data governance components, such as policies, and processes, data protection, data privacy

GOALS

The high-level goals of the DGC are to improve data quality, increase data literacy, and maximize data use in achieving organizational goals.

People

- Coach the organization on the value and implications of good data and information assets and the importance of an organizational climate that embraces the use of data in achieving enterprise strategy.
- Coach senior leaders on the importance of sponsoring analytics efforts, advocating for a structured approach to analytics, and allocating resources for analytics efforts.
- Define, agree, and communicate the roles and responsibilities of data stewards and Clinical and Business Analysts. Define responsibilities at each level and identify the appropriate staff in each area to incorporate into Data Governance committee and team structures.
- Ensure that relevant stakeholders are kept fully informed of the changes introduced by the Data Governance framework and encourage them to champion the changes in their areas of influence.
- Drive organizational and behavioral change as it relates to the use of data

Process

- Establish and execute a Data Strategy and set priorities for associated data governance activities.
- Develop a Cost-Benefit Analysis to identify and track the realization of benefit opportunities arising from the provision and use of better quality information.
- Provide data stakeholders with guidance, standards, and consultation to enable stakeholders to develop common and accepted data definitions for all shared data.
- Establish data quality policies, processes and quality measures.
- Work with Clinical and Business Analysts, data stewards, and technical staff to implement data cleansing plans and participate in the root cause analyses of data quality issues.

Technology

- Seek out program, process, and technological improvements/innovations that will:
  - Foster improved data quality and reporting
  - Balance access to information with the need for security of data
  - Improve the reliability, accuracy, and confidence in information
  - Enable visualization of data that help frontline staff to interpret and act on results

DATA GOVERNANCE COMMITTEE MEMBERSHIP

Representation on the DGC needs to include the administrative, clinical, operations, and financial sides of the organization, covering key data categories such as EHR data, patient experience data, and financial data as well as incorporate key organizational enabling functions like Information Technology (IT), Quality Improvement (QI), and Human Resources (HR).

The proposed membership of the DGC is as follows:

- CTO
- CMO
- IT Leadership
- CHCO
- COO
- CNO
- CFO
- CAO

ATTENDANCE AND PARTICIPATION

To aid the successful implementation of the DGC, the following outlines expectations for attendance and active participation:

- ***New Membership Selection:*** The DGC will select new DGC members.
- ***Ad Hoc Attendees:*** Ad hoc attendees may be requested to provide specialist input as required.
- ***Quorum:*** Quorum for the DGC is considered when, at a minimum, 50% of the DGC members. The program manager will ensure that the list of attendees is robustly maintained.

FREQUENCY AND NATURE OF MEETINGS

To aid the successful implementation of the DGC, the following outline the frequency

- ***Monthly Meetings:*** The DGC will meet initially every month for one hour, and on a nad-hoc basis, as required.
- ***Periodic Review:*** Periodically, the DGC will review the frequency and duration of meetings in-line with the organization's needs

Nebraska Hospital Association

3255 Salt Creek Circle, Suite 100 • Lincoln, NE 68504-4778
Ph: 402-742-8140 • Fax: 402-742-8191
Laura J. Redoutey, FACHE, President
nebraskahospitals.org