the-tech-trend.com

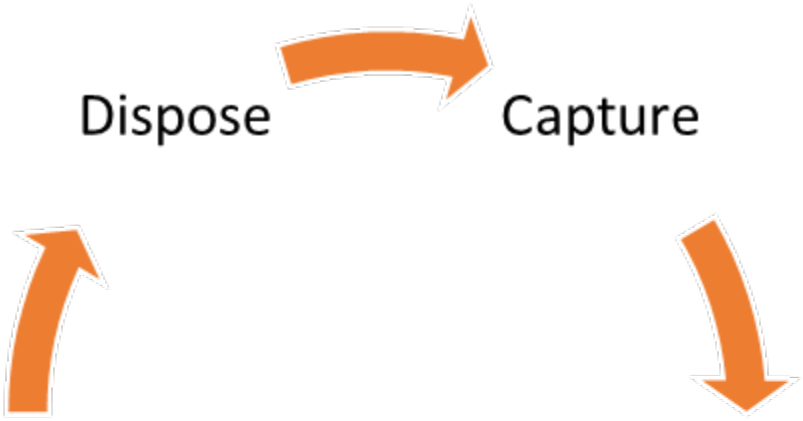
Cybersecurity Governance and Ethics in Healthcare

Arash Habibi Lashkari

16–20 minutes

Data governance in healthcare sets the framework for decision-making and accountability around managing data – from its creation and use to its final archiving or disposal (Gartner, 2024). It's crucial for making data in all forms available, secure, and useful across healthcare organizations.

Data governance also boosts interoperability, making sure data from different sources like EHRs, medical devices, and clinical trials can connect smoothly. By setting standard protocols and formats it helps integrate systems better, enhancing research and patient care. Although well-recognized for its benefits, implementing effective data governance remains a tough challenge for many healthcare organizations (Oachs, 2020).



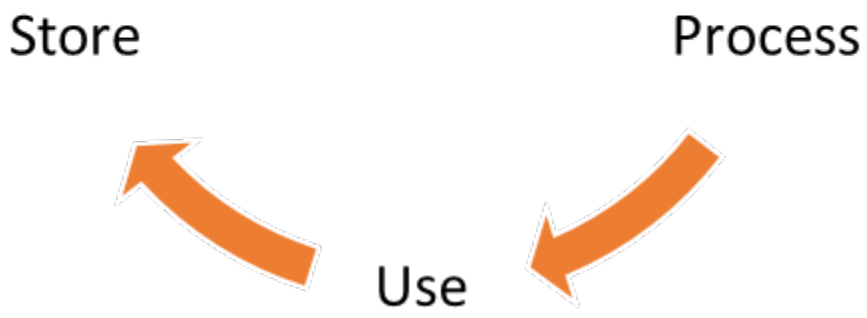


Figure 1: Data Lifecycle in Healthcare

What is a Data Governance Framework?

A data governance framework with respect to the healthcare industry manages the effective handling of data's availability, integrity, usability, and security. This framework requires clear policies, procedures, and systems for how data is collected, used, accessed, and shared. Key roles, responsibilities, and accountability measures must be well-defined (Oachs, 2020).

There are three essential components of every data governance framework: **people, process, and technology**. These elements work together to facilitate a robust structure that effectively manages data and its interactions across an organization. Building on this foundational triad, the Canadian Institute for Health Information (CIHI) has developed a more detailed framework that includes four main areas, each addressing specific health data information capabilities (CIHI, 2020):

- **Strategy and governance**: Directs the overall strategy, accountability, and compliance monitoring of health data programs.
- **Policies and processes**: Addresses the collection, processing, analysis, and sharing of data to uphold data quality, privacy, and

security.

- **Assets and standards**: Establishes necessary data assets and standards to support strategic and operational goals.
- **People and knowledge**: Focuses on engaging and educating the workforce and stakeholders to maintain effective governance.

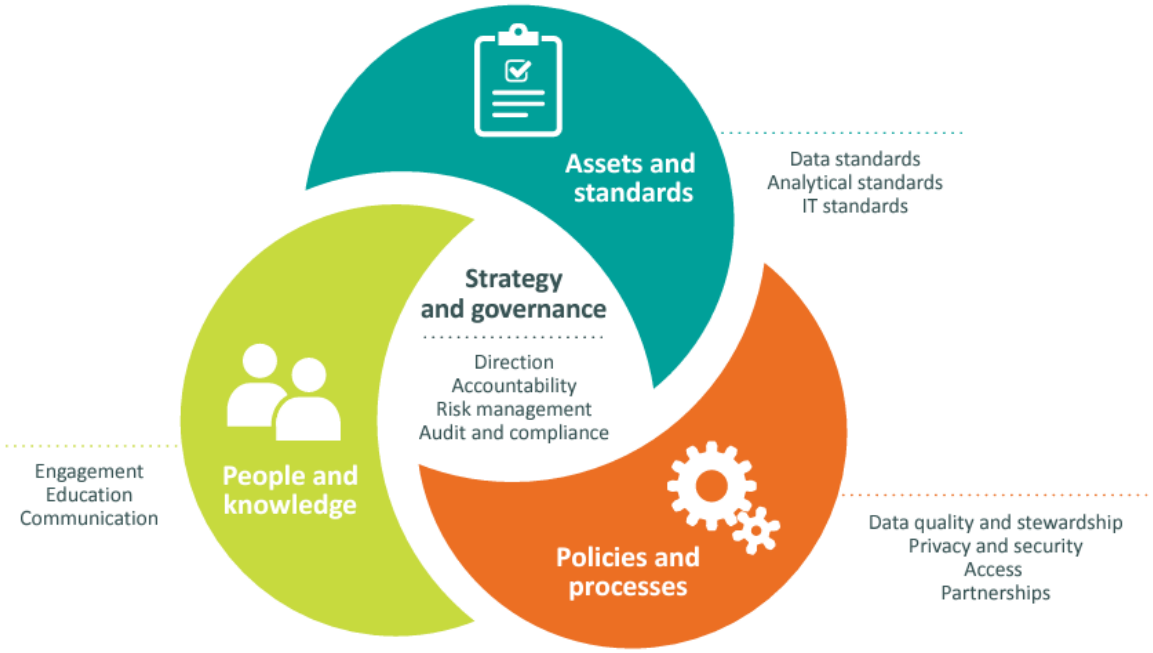


Figure 2: Health Data and Information Governance and Capability Framework (CIHI, 2020).

The Role of Healthcare Data Governance in Big Data Analytics

Healthcare organizations now grapple with massive and diverse medical data sets.

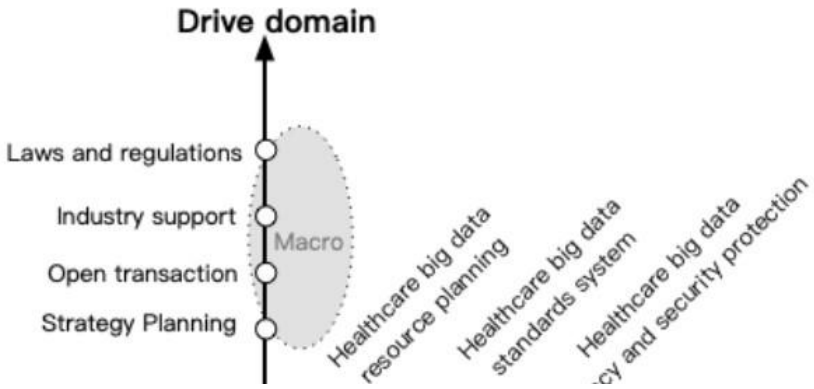
Big data technology steps in to handle these data sets, often incompatible with traditional relational databases, by focusing on their large scale (volume), diversity (variety), and the speed of data processing (velocity). Effective data governance is key to turning these vast, varied, and fast-moving data streams into actionable

insights that drive healthcare decisions. With robust practices in place, organizations can harness big data to enhance patient care and refine critical functions like predictive modeling, survival analysis, and treatment response evaluation.

Managing large-scale datasets, such as genomic sequences, involves cloud computing and technologies like Apache Hadoop for distributed processing of data up to petabytes. This analysis helps healthcare providers develop predictive models for disease progression and resource allocation.

A practical example of effective data governance is seen in China's regional health information networks, which are organized into three domains:

- **Drive domain**: This domain focuses on readiness. Its elements include considerable data strategy planning, laws and regulations, open transactions, and industry support.
- **Capability domain**: This domain addresses the scope of operations. The elements of this domain include healthcare big data organization, collection, storage, process and analysis, and usage.
- **Support domain**: This domain ensures efficiency. Its elements include healthcare, considerable data resource planning, standards systems, and privacy and security protection.



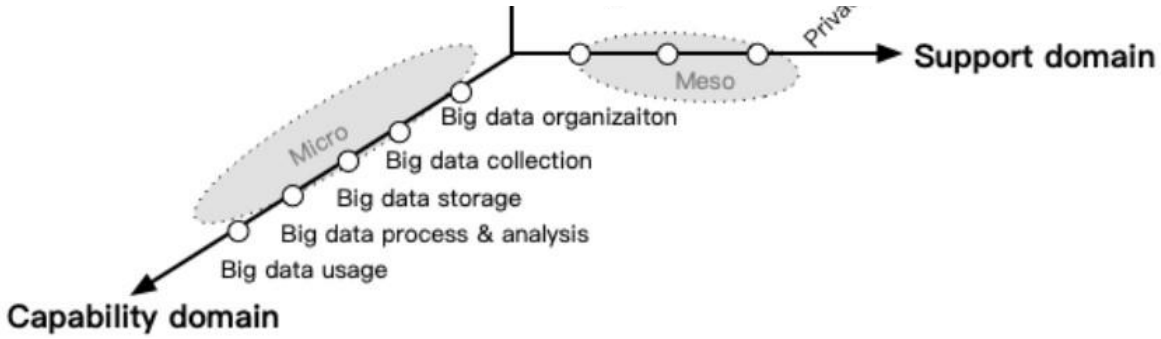


Figure 3: A Framework for Big Data Governance (QLi, 2019).

A Five-Step Guide to Healthcare Data Governance

1. Set Clear Goals

Everything starts with knowing what your organization aims to achieve. Identify the top priorities for the coming year as defined by your executive team. This will be the cornerstone of your data governance strategy.

2. Match Governance to Goals

Tie your data governance efforts directly to these organizational goals. This ensures that every initiative supports and enhances your strategic objectives.

3. Find Your Early Adopters

Look for those who are already inclined to support data governance – those who get it and get it well. These are your early adopters, the ones who see the value in data protection and are aware of its challenges.

4. Focus Your Efforts

Narrow down the opportunities to specific areas that can benefit

most from data governance, such as certain clinical fields or patient groups. This targeted approach helps concentrate your resources effectively.

5. Develop Governance Leaders

As early adopters grow in their roles, encourage them to take on broader responsibilities. They'll move from leading teams to mentoring across the organization, spreading good data governance practices as they go.

Strategic Alignment

Strategic alignment acts as the bridge linking an organization's long-term ambitions with its everyday operations, focusing on how choices made today can help achieve bigger goals tomorrow. This concept is particularly valuable in healthcare when selecting new information systems. The aim is to adopt tools that not only address current challenges but also advance the organization's overall mission.

There are two primary types of strategic alignment: IT-strategy-driven and business-strategy-driven, each focusing on different yet critical activities:

Table 1: Key process of IT-strategy-driven alignment

Key Processes	Activities Involved
1. Identifying technological innovation	Identifying new technologies
2. Clarifying IT strategy	Choosing technology

	Planning for detailed solutions Selecting vendors
3. Shaping business strategy	Articulating strategy
4. Transforming organizational infrastructure and process	Reorganizing organizational infrastructure Reorganizing organizational processes

Table 2: Key process of business-strategy-driven alignment

Key Processes	Activities Involved
1. Clarifying business strategy	Identifying misalignment
2. Modifying IT strategy	Choosing technology Defining functions Collaborating with vendors
3. Transforming organizational infrastructure and process	Arranging IT and business infrastructure

Privacy and Security of Healthcare Data

Protecting patient healthcare data is a top priority for all healthcare personnel and organizations. Privacy in healthcare means patients have the right to control who sees their personal and sensitive health information. Meanwhile, security involves the measures and

tools used to keep patient information safe from unauthorized access, tampering, deletion, or exposure.

When patients doubt the security of their health information, they're less likely to share what's needed for their care. This makes the reliability of healthcare information systems critical.

Implementing strong security measures like access control, pseudonymity, data encryption, authentication, authorization, and blockchain technology is essential to fend off cyber threats. Any breach or misuse of healthcare data can have severe consequences, including financial losses, social and ethical dilemmas, legal issues, and, in extreme cases, can even endanger lives (Pandey, 2019).

Security Concerns

Security concerns with healthcare data centers around protecting the confidentiality, integrity, and availability of sensitive patient information:

- **Physical Security**: Protect the physical hardware – servers, storage units, and security devices – is crucial. Unauthorized physical access could lead to data sabotage, theft, or unauthorized alterations. Implementing an effective authentication-based access system can prevent internal misuse.
- **Application Security:** Electronic Health Records (EHR) are accessed through specialized software that handles everything from viewing to modifying patient data. Protect these applications with anti-virus programs, anti-spam tools, and Web Application Firewalls (WAFs).
- **Server Security**: Critical data and applications are housed on

servers that require rigorous protection measures, including firewalls, access control lists, and authentication protocols.

- **Periphery Security**: Secure computing resources at the periphery through intrusion detection systems (IDS), intrusion prevention systems (IPS), and firewalls.
- **Storage and Communication Security**: Data stored on servers or network-attached storage must be defended against unauthorized access. Utilize full disk encryption and secure communication methods, such as VPNs and end-to-end encryption, to protect data during storage and transmission.
- **Ubiquitous Device Security**: Encrypt data on mobile devices and secure communication channels to mitigate the risks of loss, theft, or data breaches.
- **Preserving Confidentiality**: Protect patient confidentiality with encryption algorithms like DES, AES, RSA. Combine encryption with access restrictions for authorized individuals through passwords, biometrics, and one-time passwords (OTPs).
- **Data Integrity**: To protect data from unauthorized changes, use cryptographic methods and protocols such as SHA and MD5.
- **Data Availability**: To combat threats like denial-of-service attacks or system failures, maintain multiple backups and invest in fault-tolerant systems with high availability.

Privacy Concerns: Who Really Owns Patient Data?

Determining who actually owns patient data – whether it's the patients, providers, or tech professionals – is fraught with debate. Traditionally, providers control the data they collect, but patients

are now stepping up to claim their rights to access and manage their own information. Although providers can update records, they cannot delete them; patients, on the other hand, can delete but not alter these entries. Laws like HIPAA and GDPR empower patients with rights to access, correct, and decide who shares their data.

Key Cybersecurity Standards in Healthcare

Authoritative bodies continually develop cybersecurity frameworks to help organizations safeguard their data and comply with industry standards:

- **ISO/IEC 27001**: This standard helps organizations across various sectors develop and refine their Information Security Management Systems, providing guidelines for secure data management (ISO/IEC27001, 2022).
- **SOC 2**: Established by the AICPA, SOC 2 specifies how to handle customer data, focusing on security, availability, processing integrity, confidentiality, and privacy (SOC2, 2021).
- **GDPR**: The EU's General Data Protection Regulation enforces strict rules for personal data handling, emphasizing consent and rapid breach response, especially relevant for healthcare providers (GDPR, 2024).
- **CCPA**: The California Consumer Privacy Act increases consumer control over personal data collected by businesses, including healthcare organizations, mandating access, deletion rights, and protective measures (CCPA, 2018).
- **HIPAA**: US law that protects patient information, setting standards to limit disclosures without consent and ensuring data security

through encryption and access controls (HIPAA, 2023).

- **HITECH Act**: This legislation boosts HIPAA by raising non-compliance penalties and promoting secure electronic health information exchanges (HITECH, 2009).
- **PHIPA**: Governs how healthcare providers in Ontario handle health data, focusing on privacy (PHIPA, 2004).
- **PCI DSS**: Protects payment card data, requiring healthcare providers to secure card information during storage, processing, and transmission to comply with global standards (PCI-DSS, 2024).

IT Governance

At the board level, IT governance steers IT initiatives in alignment with broader business goals, which boosts value and mitigates risks. Deploying IT governance effectively means crafting strategies that better integrate IT into hospital operations.

The modern IT governance landscape features several frameworks that guide organizations in aligning IT operations with strategic objectives, risk management, and regulatory compliance:

- **ISO/IEC 38500**: This standard provides guidelines for the responsible use of IT in organizations, focusing on managing information and communication technology processes and decisions (ISO/IEC, 2024).
- **COBIT**: Created by ISACA, COBIT aligns IT investments with business goals, providing a framework for IT governance, regulatory compliance, and risk management (COBIT, 2019).
- **Global Technology Audit Guide (GTAG)**: GTAG presents

auditing methods to verify if IT governance supports organizational strategies, complementing frameworks like ISO/IEC 38500 and COBIT that detail the processes necessary for a robust IT governance program (GTAG, 2021).

Boosting Cybersecurity Awareness and Adherence

Cybersecurity awareness training aims to educate staff on best practices and motivate them to protect sensitive information. This training reduces cyberattacks that stem from human-related vulnerabilities, such as human error and phishing scams.

Healthcare professionals, including IT staff, doctors, and nurses, receive training to spot potential cyber threats like social engineering and phishing. This training gives them the tools they need to manage information security and understand data protection in their day-to-day work. Training programs should be customized for different roles.

The effectiveness of a cybersecurity awareness program heavily depends on the delivery of its content. Here are some engaging delivery methods:

- Utilize leaflets, posters, and newsletters.
- Security experts can lead lectures, seminars, and workshops to raise awareness.
- Include e-mail broadcasts, online discussions, blogs, animations, and multimedia.
- Interactive online games that integrate graphics, play, and educational content to provide immersive learning experiences.
- Use educational videos for self-paced learning without the need for

a live trainer.

- Send simulated phishing emails to test and train staff on recognizing and reacting to phishing attempts. Remedial training is provided if they fall for a simulation, with follow-up tests to measure improvement.

Wrapping Up

This article explored the crucial aspects of cybersecurity governance and ethics in healthcare, focusing on the data lifecycle, governance frameworks, and the transformative role of big data analytics. By tackling interoperability challenges, strengthening privacy, and aligning IT strategies, healthcare organizations can use data governance to boost patient care and secure data more effectively in our digital age.

References:

Alder, S. (2024, Feb 20). What is Healthcare Regulatory Compliance? Retrieved from The HIPAA Journal: https://www.hipaajournal.com/healthcare-regulatory-compliance/

CCPA. (2018). California Consumer Privacy Act (CCPA). CALIFORNIA: STATE OF CALIFORNIA DEPARTMENT OF JUSTICE. Retrieved from https://www.oag.ca.gov/privacy/ccpa

CIHI. (2020). Canadian Institute for Health Information. CIHI's Health Data and Information Governance and Capability Framework. Ottawa, ON: Canadian Institute for Health Information (CIHI).

COBIT. (2019). Control Objectives for Information and Related Technologies (COBIT) ISACA's Framework. Retrieved from Information Systems Audit and Control Association (ISACA):

https://www.isaca.org/resources/cobit

Gartner. (2024). Data Governance. Retrieved April 2, 2024, from Data Governance: https://www.gartner.com/en/information-technology/glossary/data-governance

GDRP. (2024). General Data Protection Regulation (GDPR). Retrieved April 2, 2024, from GENERAL DATA PROTECTION REGULATION (GDPR): https://gdpr-info.eu/

GTAG. (2021, Sep 10). GTAG: Auditing IT Governance. Retrieved from Global Technology Audit Guide (GTAG): https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-auditing-it-governance/

ISO/IEC. (2024). Information technology – Governance of IT for the organization (ISO/IEC 38500:2024). Retrieved from https://www.iso.org/standard/81684.html

ISO/IEC27001. (2022). Information security, cybersecurity and privacy protection. Retrieved from ISO: https://www.iso.org/standard/27001

Oachs, P. a. (2020). Health Information Management: Concepts, Principles, and Practice (6 ed.). (A. W. Pamela K. Oachs, Ed.) American Health Information Management Association (AHIMA) Press. Retrieved from https://books.google.ca/books?id=msNnwwEACAAJ

Pandey, A. K. (2019). Security and Privacy of Electronic Healthcare Records: Concepts, paradigms and solutions. In S. T. Sudeep Tanwar, Security and Privacy of Electronic Healthcare Records Concepts, paradigms and solutions (pp. 17-39). London, United Kingdom: The Institution of Engineering and Technology.

PCI-DSS. (2024). Payment Card Industry Data Security Standard (PCI DSS) v4.0. Retrieved from https://www.pcisecuritystandards.org/

QLi, Q. a. (2019). A Framework for Big Data Governance to Advance RHINs: A Case Study of China. IEEE Access, 50330-50338. doi:10.1109/ACCESS.2019.2910838