



CURING THE DATA DEFICIT

How to Heal Governance
Problems in Healthcare



Healthcare Governance in Focus

Due to the nature of the data they hold, healthcare organizations in the United States are subject to strict requirements and regulations around record-keeping, security, privacy and governance. These range from the Health Insurance Portability and Accountability Act (HIPAA) to the Health Information Technology for Economic and Clinical Health (HITECH) Act to the Medicare Access and CHIP Reauthorization Act (MACRA), as well as concepts including medical necessity and chain of custody (CoC). Although most organizations are dedicated to remaining compliant, data vulnerabilities persist.

Ultimately, the risks associated with improper data management in the healthcare industry go beyond financial loss and reputational harm, encompassing everything from patient identity theft to hampering leadership decisions and endangering lives. Yet, with the right governance, risk and compliance processes in place, healthcare organizations can thrive.

“A third of all data breaches in the United States now occur in hospitals, while the number of breached personal records in the healthcare industry jumped from 15 million to 40 million just from 2018 to 2019.”

[Tech Republic](#)



The Ramifications of an Outdated Approach

No matter their size or area of focus, healthcare organizations must maintain a high standard of governance. Attempting to persevere with outdated systems and processes leaves the industry open to flaws that can be exploited.

4 Vulnerabilities of Legacy Processes

- **A lack of speed:** Legacy processes reliant on disparate systems mean that information needs to be tracked down, compiled and reformatted.
- **A lack of accuracy:** Reliance on paper invariably leads to avoidable mistakes. An allegiance to paper board books can lead to hard-to-untangle version-control issues.
- **A lack of security:** Many healthcare enterprises rely on antiquated devices running outdated software or operating systems. Budgetary and operational constraints often leave healthcare organizations susceptible to attack.
- **A lack of consistency:** With multiple board members following multiple processes on multiple boards, there is often a confusing and counterproductive disparity between governance practices.

“The risks and costs associated with healthcare data security breaches are too high, and the confidential, personal health data of millions are at risk. This makes data security healthcare’s biggest concern today, and a problem for which innovation and communication are of the utmost importance.”

[University of Illinois at Chicago](#)



Governance Problems in Healthcare

For boards of healthcare organizations, governance problems are most common in these areas:

Communication and Collaboration

In larger healthcare organizations in particular, the sheer numbers involved can make joined-up thinking difficult. Whether that's the volume of data, the number of board members, intricate and finely tuned budgets or the handling of patient information, clear and easily manageable communication is essential. Without clarity and ease of communication, any progress is likely to be at best slow, and at worst nonexistent.

Security

Cybercriminals frequently target healthcare providers. Breaches range from data and intellectual property theft to attacks intending to shut down a provider's or facility's computer systems or networks. Data breaches in the healthcare industry cost, on average, \$7.13 million – significantly higher than the global all-industries average (which has fluctuated between \$3.5 million and \$4 million in recent years).

File Management and Record-Keeping

Healthcare organizations require stable, high-volume storage and robust file management systems. Medical files can be huge, and boards can generate significant quantities of minutes, reports and other information. All must be collected, maintained and stored using consistent formats and taxonomies. At the same time, patient data must be readily accessible to physicians and carers when and as required; protocols that ensure patient records remain confidential are essential.

Risk Mitigation

Healthcare boards must be proactive in their risk-management approach. Boards need to be fully aware of the consequences of a governance failure, which may include:

- **Operational breakdowns:** Cyberattacks can shut down business systems. Shutdowns can present immediate risks to patient welfare and even survival if network-connected devices go offline, or if carers cannot access vital information to make decisions, with significant consequences. Longer term, a network outage, data theft or other intrusion can drastically affect staff rostering, inventory control, delivery and transport management, and other systems.
- **Financial losses:** Healthcare businesses may be unable to process transactions, with immediate impacts on cash flow and overall financial position. Share prices may drop, and investors may see a data breach as an indication that the organization was inadequately prepared to face cyber risks, in turn making it more challenging to attract funding.
- **Reputational damage:** If investors and customers believe facilities are vulnerable, or that management is unaware of or unresponsive to critical risks, then businesses may have difficulty attracting investment and customers.

How a Digital Solution Solves Common Governance Problems

With a digital governance solution, the boards of healthcare organizations will find significant operational gains:

Communication and Collaboration

In light of the rapid pace of change within the healthcare industry, organizations should seek technology that offers a centralized, secure method of communication. The solution should also make collaboration and the sharing of information as fluid as possible, all while ensuring any movement of data is secure.

A strong governance solution should also be able to aid enhanced decision-making. In an industry in which boards are consistently presented with a new set of profoundly consequential strategic options, often involving significant risk, major mission shifts and short windows of opportunity, it's crucial that there are processes in place to empower rapid and secure collaboration.

Security

As remote work becomes more commonplace, as cyberthreats get more sophisticated and as workers bring their own devices to work, effective security practices are a necessity.


On the technology side, organizations should have key security measures enabled, including:

- **Two-factor authentication** to prevent log-ins from bad actors.
- **Secure online content management** to keep documents and data out of reach.
- **Secure messaging apps and platforms** to keep sensitive communications private.
- **Encryption** to lock down data and make it inaccessible to unauthorized users.
- **Backup and redundancy** to ensure that systems can be restored with little to no data loss in the event of a ransomware attack or system failure.

File Management and Record-Keeping

A unified file management system is the backbone of any organization's data security, recovery and retention system. In terms of operational governance, critical capabilities include:

- **Collaboration and file sharing:** Secure access to document pools or libraries ensures that versions and changes can be tracked by users as required.
- **Secure downloads and messaging:** Organizations must have visibility into who has downloaded information, when they've downloaded it and to what type of device. Similarly, they must be able to track messages, including confirmation of receipt and opening, and visibility of replies and forwards.
- **Granular access control:** Access control must be capable of distinguishing various degrees of access to files and data repositories.



“63% of confirmed data breaches involved taking advantage of passwords that were the default, weak or stolen. Healthcare employees should not only use strong passwords, but ensure they are changed regularly.”

[Health Informatics, University of Chicago](#)

Data management and record-keeping are just as crucial for boards of directors. Essential record-keeping functions for the board include:

- **Minutes:** Secretaries should circulate meeting notes and draft minutes securely, manage and integrate amendments, send final drafts for approval, and then store and recirculate as required.
- **Voting:** Software to enable remote-access voting should be secure, with confirmation to the voter as well as vote tallying and communication of outcomes.
- **Remote meeting attendance:** Especially in light of the COVID-19 pandemic, boards should facilitate remote meeting attendance to minimize health risks.
- **Board packs:** Board papers should be available electronically in a secure format with message receipts, tracking and confirmation of opening.

Risks

By centralizing and simplifying core risk management activities into a single, integrated platform, a healthcare enterprise can effect change in the right areas at the right time. From real-time risk reporting to automated risk assessments to the identification and cataloguing of risks using a curated risk library, a best-in-class risk management solution helps healthcare boards to focus on what matters most.

The solution should allow boards to:

- Improve risk-based decision-making – going from reactive to predictive action
- Identify and deal with fast-moving or emerging risk quickly and effectively
- Simplify risk reporting to better understand impacts and responses
- Reduce subjectivity with data-driven risk indicators in assessments and reporting
- Achieve alignment across governance teams within a single platform



What to Look for in a Digital Governance Solution

Digitizing board practices brings both organization and convenience. By bringing governance online, healthcare boards are able to increase efficiency, mitigate cyber risk, improve their decision-making and action a more impactful response in a crisis.

From board meeting preparation and boardroom record-taking to proper board communication practices and around-the-clock support, a gold standard governance solution will empower an organization to adapt to any challenge, crisis or opportunity with agility and strategic acumen. The right digital platform should include the following:

- **A centralized platform** for boards that allows for secure access to board materials, bulk uploads of important documents, online and offline document sharing, digitized voting and eSignature integration
- **A streamlined messaging system** that conveys information quickly, easily and without risk, allowing for collaboration and sharing in a secure environment
- **Board evaluation tools** that help administrators and directors manage and analyze board assessments and performance more efficiently
- **A secure and collaborative minute-taking application** that enables governance professionals to easily take minutes and circulate them for board approval
- **A fully secure file-sharing solution** that safeguards sensitive information inside and outside of the organization
- **Entity management systems** that consolidate subsidiary legal and compliance information into a centralized corporate record for the corporate secretary and general counsel
- **A system for meeting compliance obligations** with automation and clearly specified workflows



The Healthcare Industry's Move Toward Modern Governance

In the healthcare industry, boards should lead from the front, adopting robust governance protocols and setting expectations for the rest of the organization accordingly.

The Diligent platform empowers leaders with the technology, insights and processes to collaborate securely, make data-driven decisions and position their organizations for greater success. Moreover, adopting a unified board management platform allows directors and governance professionals to improve their organization's risk management, streamline processes, enhance communication and reduce time spent on administrative tasks.

Diligent's platform digitally transforms how boards and executive teams work while still protecting all confidential and sensitive data, information and workflows. From a dedicated and secure messaging system to secure collaboration capabilities to online and offline document sharing, Diligent's modern governance solutions have everything organizations need in a digital solution.



“You have so many key factors when it comes to cybersecurity. Diligent puts our board at ease. They know that we’re taking these measures to be secure, to keep our information private and to really protect our patients.”

Judith Coleman
Office Manager, GBMC Healthcare

About Diligent

Diligent is the pioneer in modern governance. Our trusted, cloud-based applications streamline the day-to-day work of board management and committees, support secure collaboration, manage subsidiary and entity data, and deliver insights that empower company leaders to make better decisions in today's complex landscape. With the largest global network of corporate directors and executives, Diligent is relied on by more than 19,000 organizations and nearly 700,000 leaders in over 90 countries. With award-winning customer service across the globe, Diligent serves more than 50% of the Fortune 1000, 70% of the FTSE 100 and 65% of the ASX.

Learn more and explore our solutions at [Diligent.com](https://www.diligent.com)

