Diligent

CURING THE DATA DEFICIT

How to Heal Governance Problems in Healthcare

Healthcare Governance in Focus

As with all industries today, data management has a considerable role to play in healthcare. Proper stewardship of that data hinges on good governance practices. However, the industry and its operators – from hospitals to insurers to biotech startups – face an extra imperative.

Healthcare organisations routinely deal with personal and highly sensitive information. Patients and practitioners, quite reasonably, expect that it will be kept secure. Furthermore, the healthcare industry is frequently targeted by cybercriminals, making robust security measures even more critical.

Due to the nature of the data they hold, healthcare organisations in Australia are subject to strict requirements and regulations around record-keeping, security, privacy and governance.

Chief among them is the Privacy Act 1988, which regulates how organisations collect and handle personal information. The legislation around the My Health Record scheme, including the Healthcare Identifiers Act 2010, the My Health Records Act 2012, the My Health Records Rule 2016 and the My Health Records Regulation 2012, lays out security requirements for participating organisations.

Finally, Australia's Notifiable Data Breach scheme places obligations on healthcare providers. Organisations must notify affected individuals and the Office of the Australian Information Commissioner about eligible data breaches. And while most organisations work hard to remain compliant, data vulnerabilities persist.

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

> "From July–December 2019, Australia's health sector accounted for 22% of all data breaches, making it the highest-reporting sector in the country. Yet only a third of Australian healthcare organisations embed cybersecurity awareness and training into their policies and procedures."
>
> Royal Australian College of General Practitioners

The Risks of an Outdated Approach

No matter their size or area of focus, healthcare organisations must maintain a high standard of governance. Attempting to persevere with outdated systems and processes leaves the industry open to dangerous risks.

4 Vulnerabilities of Legacy Processes

- **Slow:** Legacy processes reliant on disparate systems mean that information needs to be tracked down, compiled and reformatted – slowing down boards when they need to act fast.
- **Inaccurate:** Reliance on paper invariably leads to avoidable mistakes. An allegiance to physical board papers and other documentation can cause hard-to-untangle version-control problems.
- **Insecure:** Many healthcare enterprises rely on antiquated devices running outdated software or operating systems. Budgetary and operational constraints often leave them susceptible to attack.
- **Inconsistent:** With multiple board members following multiple processes on multiple boards, there is often a confusing and counterproductive disparity between governance practices.

> "Healthcare providers are facing an unprecedented risk of cyberattacks amid the coronavirus pandemic... the Australian Cyber Security Centre has raised concerns in regard to healthcare providers – including hospitals and aged-care homes – being increasingly targeted by COVID-19-themed ransomware attacks."
>
> Hospital and Healthcare

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

Communication and Collaboration

In larger healthcare organisations, 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 patient information handling, it's essential to have transparent and easily manageable communication. Without clarity and ease of communication, any progress is likely to be slow at best, and non-existent at worst.

Security

As noted previously, 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, US$7.13 million – significantly higher than the global all-industries average (which has fluctuated between US$3.5 and $US4 million in recent years).

File Management and Record-keeping

Healthcare organisations 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.

Record retention is mandated by law, making secure storage a must. Data formats and locations should prevent degradation over time. Simultaneously, 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:

- **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. Over the longer term, a network outage, data theft or other intrusions 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 can drop, and to investors, a data breach may indicate the organisation is inadequately prepared to face cyber risks, 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, 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 organisations will find significant operational gains:

Communication and Collaboration

In light of the healthcare industry's rapid pace of change, organisations should seek technology that offers a centralised, secure method of communication. The solution should also make collaboration and information-sharing as fluid as possible while ensuring all data movements are secure.

A robust governance solution should be able to aid enhanced decision-making. In an industry where boards are consistently presented with new and profoundly consequential strategic options, often involving significant risk, major mission shifts and short windows of opportunity, processes must be in place to enable rapid and secure collaboration.

Security

As remote work becomes more common, as cyber threats become more sophisticated and as workers bring more of their own devices to work, effective security practices are critical.

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

- **Two-factor authentication** to prevent logins 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 unprivileged users.
- **Backup and redundancy** to ensure organisations can restore systems with little to no data loss in the event of a ransomware attack or system failure.

> "Having weak passwords is … an invitation to unauthorised access and cyber compromise. While 80% of people say they are concerned about the security of their personal information, 81% of confirmed data breaches involve weak, default or stolen passwords."
>
> **Amanda Cattermole, CEO**
> Australian Digital Health Agency

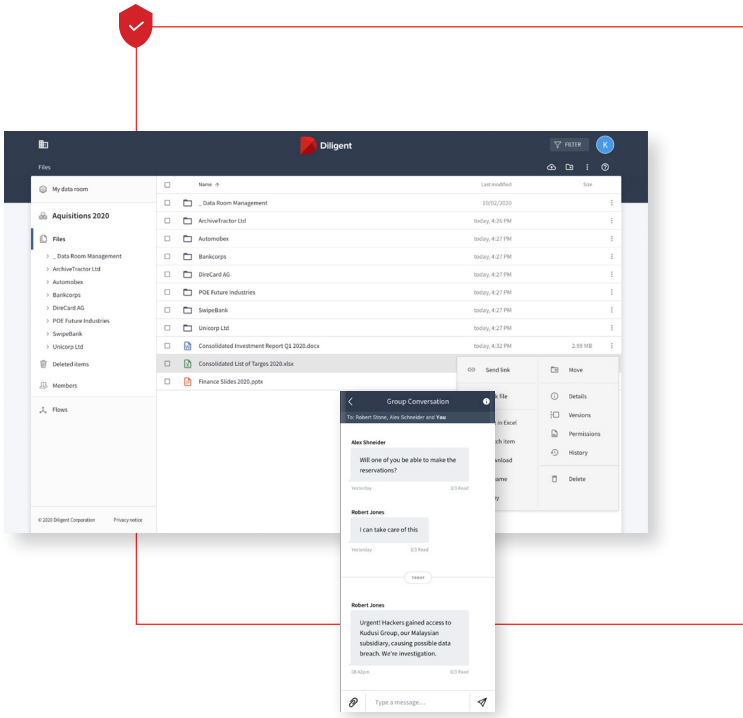
File Management and Record-keeping

A unified file management system should form the backbone of any organisation's data security, recovery and retention system. Access controls ensure that only individuals with the proper privileges can view or download sensitive data, depending on their position, responsibilities and geographical location. 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:** Organisations 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.

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, 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:** In light of the COVID-19 pandemic, boards should facilitate remote-meeting attendance to minimise health risks.
- **Board packs:** Board papers should be available electronically in a secure format with message receipts, tracking and opening confirmation.



Risks

By centralising 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 identifying and cataloguing risks using a curated risk library, a best-in-class risk-management solution helps healthcare boards 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 understand impacts and responses better.
- **Reduce** subjectivity with data-driven risk indicators in assessments and reporting.
- **Align** governance teams across the organisation within a single platform.

What to Look for in a Digital Governance Solution

Digitising board practices brings both organisation and convenience. By bringing governance online, healthcare boards can 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 organisation to adapt to any challenge, crisis or opportunity with agility and strategic acumen.

A good digital platform should include the following:

- A centralised platform for boards that enables secure access to board materials, bulk uploads of important documents, online and offline document sharing, digitised 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 analyse board assessments and performance more efficiently.
- A secure and collaborative minute-taking application that enables governance professionals to take minutes and circulate them for board approval easily.
- A fully secure file-sharing solution that safeguards sensitive information within and outside of the organisation.
- Entity management systems that consolidate subsidiary legal and compliance data into a centralised corporate record for the corporate secretary and general counsel.
- A system for meeting compliance obligations with automation and specified workflows.
- Concierge-level service, especially at critical moments when a rapid response is required, even if after business hours.

The Healthcare Industry's Move Towards Modern Governance

In the healthcare industry, boards should lead from the front, adopt robust governance protocols and set expectations for the rest of the organisation accordingly.

The Diligent platform empowers leaders with the technology, insights and processes to collaborate securely, make data-driven decisions and position their organisations for greater success. Moreover, adopting a unified board management platform allows directors and governance professionals to improve their organisation'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 organisations need in a digital solution.

> "We had to communicate highly sensitive government directives to the Board and collaborating via Diligent was reassuring. It meant we didn't have sensitive data moving around our email network, which kept valuable patient data and system information secure and confidential."
>
> Dauniika Puklowski, Board Secretary
> Homecare Medical

Diligent

a MODERN GOVERNANCE company

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 organisations and nearly 700,000 leaders in over 90 countries. With award-winning customer service across the globe, Diligent serves more than 65% of the ASX, 50% of the Fortune 1000, and 70% of the FTSE 100.

Trusted by over 700,000 leaders and 19,000 organisations across the globe

NHS The Princess Alexandra Hospital NHS Trust

Australian Red Cross

Gwinnett Medical Center

Credit Corporation

GHIT Fund — Global Health Innovative Technology Fund

Liberty Mutual

Highest security standards

- 256-bit encryption
- Remote locking
- Two-factor authentication

Industry-leading support

- 24/7/365 support
- White glove service
- Unlimited user training

Compliance Attestations

- ASAE 18 audits
- ISO-certified
- Third-party security testing

For more information or to request a demo:

Call: **1800 646 207** • Email: **info@diligent.com** • Visit: **diligent.com/au**