



# CHALLENGES IN MANAGING DIGITISATION AND INNOVATION IN HOSPITALS

Opportunities and risks for hospital boards

AUTHOR: BRAD DAVIES, DIRECTOR DANDOLOPARTNERS INTERNATIONAL

dandolopartners

---

# Introduction

Operating a hospital has never been more complex or challenging. Hospital boards and executives need to manage critical clinical, regulatory and commercial risks but also deal with the profound effect of information and communication technology (ICT). The 'digitisation' of hospitals offers potential for new insights, efficiencies and improvements related to both management functions and clinical care/patient safety. Digitisation is creating new risks as well as amplifying pre-existing ones.

The notion of hospital digitisation is not new; the term digital hospital was first used more than a decade ago. However, rapid advances in commercial and consumer ICT has changed what's possible and accelerated the pace of that change. Much of the research related to digital hospitals has tended to focus on either the benefits or applications. For example, the 2014 CSIRO report 'A digitally-enabled health system' provides an excellent snapshot of current and future health technology and the potential implications for hospitals.<sup>1</sup>

However, much less has been explored in terms of what hospitals need to have in place in terms of underlying capability to position their organisations for what's coming. This includes appropriate systems, policies, processes, talent and infrastructure.

## This report

This report was commissioned by Cisco and Optus as a contribution to the debate about technology's role in healthcare delivery. The report distils views of a range of stakeholders (hospital executives and board members, government representatives, technology experts) and secondary research. Discussions with stakeholders – and this report – focused on three questions:

- What underlying capability is required to capture benefits from hospital digitisation?
- How well positioned are hospitals to capture new opportunities and manage critical risks?
- What role should the board play – and what questions should they ask – in fulfilling that role?

The report is divided into four sections:

- **Part 1:** Hospitals are at a tipping point
- **Part 2:** The opportunity presented by digital technology and innovation
- **Part 3:** Challenges in capturing value and managing risks from digital and innovation
- **Part 4:** Implications for hospital boards

---

1 CSIRO 2014, *A Digitally Enabled Health System*, <<https://publications.csiro.au/rpr/pub?pid=csiro:EP145606>>

# Executive Summary

The health business model is struggling under the weight of demand and supply side factors. The traditional levers to manage pressures on the health system are likely to be less effective in the future – low-hanging fruit efficiencies have already been picked and government funding is unlikely to rise at the same rate as demand.

Digitisation and innovation are increasingly seen as opportunities to attack fundamental problems and inefficiencies in both clinical and administrative processes, as well as creating the potential for new value. The health sector has a strong track record in adopting specialist clinical technologies and devices, but less so for information and communication technology (ICT) and informatics. Investment in technology of itself is not sufficient – hospitals need to be effective innovators as well.

Hospitals are asking themselves the question: what will it take to capture more benefits from digitisation/innovation than we have in the past? A broad range of issues have prevented hospitals capturing value from innovation and digitisation, including funding/incentives, organisational capability and change management. Beyond these factors three specific challenges were identified as critical if hospitals are to position themselves for digitisation and innovation:

## A) How to move from simply capturing data to making genuinely data-driven decisions and performance improvement

Questions that hospital boards are asking include:

- What new data should boards demand, given the availability of new technologies, tools and techniques?
- Are boards getting *sufficient* data to make decisions, and is it provided in a clear and contextualised form?
- Are data policies stifling innovation, and could they better reflect the hospital's desire to innovate and collaborate?

## B) How to ensure the hospital's digital infrastructure is robust and scalable to meet current and future needs

Questions that hospital boards are asking include:

- Is it fit for purpose and does it anticipate scale and innovation requirements into future years?
- How robust is the hospital's digital infrastructure, including back-up systems and redundancy, and do opportunities exist to optimise existing infrastructure rather than expensive upgrades?
- How to take advantage of new commercial models and move from capex to opex funding models?

## C) How to manage cyber risk without stifling innovation

Questions that hospital boards are asking include:

- Is the level of cyber resilience appropriate, and how does that compare with other hospitals?
- Is the hospital undertaking appropriate external validation (including other hospitals, law enforcement and industry)?

The interpretation of risk is starting to change, particularly when the risk of doing nothing is potentially devastating. Doing nothing – or not doing enough – could leave poor performance undetected, systems inoperable, patient and organisational data exposed and the institution deemed culpable. Facing a perfect storm of financial factors, avoidance or delayed investment in digitisation or innovation will deliver short-term savings, but may cost the hospital in terms of patient outcomes and productivity savings.

# Part 1: Hospitals are at a tipping point

## The health business model is under extreme pressure

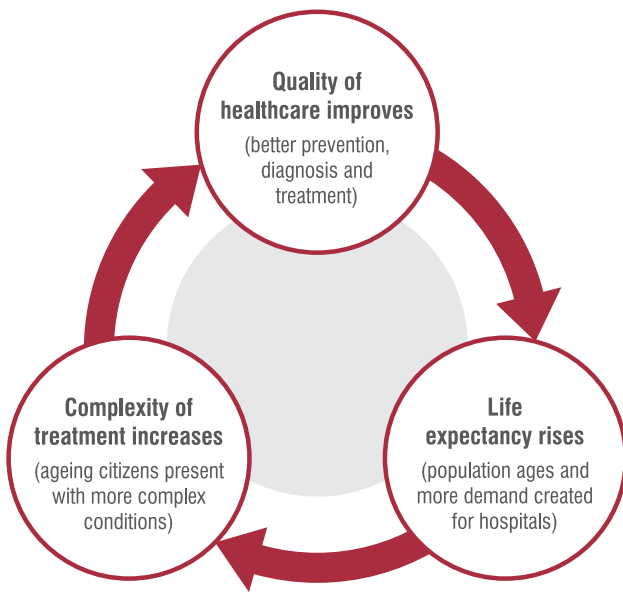
The health business model is struggling under the weight of demand and supply side factors. Health expenditure is already Australia's second-largest area of government spending,<sup>2</sup> having trebled in the past 25 years and expected to double again in the next 40 years.<sup>3</sup> At this rate the Australian Treasury estimates that, by 2043, health expenditure will exceed the entire state and local government tax base, and absorb almost half of all government taxation revenue.<sup>4</sup>

Demand is being driven by lifestyle and demographic factors. Australians' sedentary lifestyle is contributing to higher rates of obesity, diabetes and a general increase in chronic diseases across the age spectrum. The growing and ageing population is also a major factor. Older Australians present with a greater number of health and complex conditions, they are hospitalised more often and stay longer in hospital than younger patients.<sup>5</sup> As a consequence, the Australian Government Institute for Health and Welfare cites chronic disease as Australia's biggest health challenge,<sup>6</sup> manifesting in higher rates of presentation with comorbidities.<sup>7</sup> Department of Health figures show that since 2007 more than 80% of Australians aged over 65 have three or more long-term health conditions.<sup>8</sup> Patients with multiple, serious conditions are more likely to require engagement of multi-disciplinary clinical teams in their treatment. Presentations involving comorbidities also tend to present greater complexity and patient safety risk.

On the supply side, rising costs are linked to more complex and resource-intensive models of care and continuous investment in specialised clinical technologies. The Grattan Institute found that more, improved and new services accounted for around two-thirds of growth in real health spending in the decade to 2013.<sup>9</sup> Contributing to rising cost of treatment is investment in new technologies for treatments and diagnostics. A US study showed new technologies contributed approximately 50% of annual cost increases in US hospitals.<sup>10</sup> In a referral-based system, the availability of new clinical technology tends to increase demand. These technologies are costly, but highly effective, creating an interesting paradox. The more effective the healthcare system becomes the longer people live, and the longer people live the greater the chance patients will present with complex conditions which in turn creates even further strain on the system that prolonged their life.

Figure 1 presents the virtuous cycle in healthcare.

- 
- 2 Department of Treasury 2010, *Intergenerational Report 2010*, Commonwealth of Australia, Canberra, <<http://www.treasury.gov.au/>>
  - 3 Department of Treasury 2015, *Intergenerational Report March 2015*, Commonwealth of Australia, Canberra, <<http://www.treasury.gov.au/>>
  - 4 Department of Treasury 2010, *Intergenerational Report 2010*, Commonwealth of Australia, Canberra, <<http://www.treasury.gov.au/>>
  - 5 Natsem at the University of Canberra 2011, *Length of Hospital Stay by Older Australians: Bed-blocking or Not?*, <<http://www.natsem.canberra.edu.au/storage/WP8%20Final.pdf>>
  - 6 Australian Institute of Health and Welfare 2014, *Australia's Health*, Commonwealth of Australia, Canberra, <<http://www.aihw.gov.au/>>
  - 7 A co-morbidity is a where a patient has two or more conditions
  - 8 Department of Health 2012, *Chronic Disease Prevalence*, Commonwealth of Australia, Canberra. <<http://www.health.gov.au/internet/main/publishing.nsf/Content/chronic-disease>>
  - 9 Daley, J., & McGannon, C 2014, *Budget pressures on Australian governments 2014*, Grattan Institute, <<https://grattan.edu.au/report/budget-pressure-on-australian-governments-2014/>>
  - 10 Callahan, D 2008, *Health Care Costs and Medical Technology*, The Hastings Center, New York. <<http://www.thehastingscenter.org/Publications/BriefingBook/Detail.aspx?id=2178>>



**Figure 1:** The virtuous cycle in healthcare

The traditional levers to manage healthcare pressures are likely to be less effective in the future

**‘Low-hanging fruit’ efficiencies have already been picked.** The focus on Lean and 6 Sigma processes has led to standardisation and automation of processes and workflows, and improved procurement practices have helped to make hospitals more productive and efficient. However, often these processes were micro in nature, may not have had the resourcing to be deployed at scale and didn’t necessarily have the full commitment of clinical leaders within the hospital, or have a major impact on interdepartmental and inter-facility processes. Achieving further productivity savings – at a scale that is worth the effort – will require more fundamental change and involve more implementation complexity. This complexity is not necessarily in the technology, but in the social processes, models of care and clinical relationships between departments that are often siloed and fragmented.

**Government funding is unlikely to rise at the same rate as demand.** There has been a \$423M reduction in Commonwealth Government forward estimate funding in the past three years.<sup>11</sup> Even with the Commonwealth’s recent agreement with states to provide almost \$3B in additional funding to public hospitals between now and 2020, funding is forecast to be lower than both major parties were proposing in 2013.<sup>12</sup> State governments increasingly expect hospitals to deliver efficiency dividends, and are more price-sensitive in terms of what they are prepared to pay for services. This trend also applies to insurers who are seeking to transfer risk and cost to hospitals by refusing to pay for treatment of some conditions and for re-admissions they consider to be a result of poor practices.

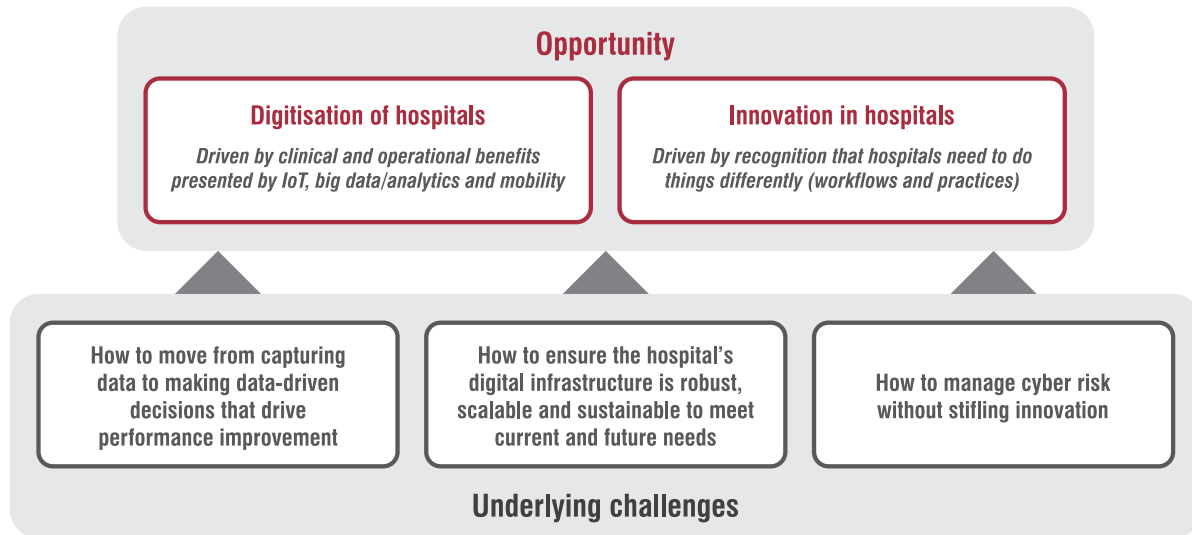
In the face of these issues doing nothing is likely to result in sub-optimal clinical decision-making, unmet patient expectations and a range of other negative consequences.

11 Australian Medical Association 2016, *Public Hospital Report Card 2016*, Australian Medical Association, <<http://www.ama.com.au>>

12 Stephen Duckett, Grattan Institute, quoted in The Mandarin 2016, *Federal Budget 2016 Health Experts React*, <<https://theconversation.com/federal-budget-2016-health-experts-react-58638>>

## Part 2: The opportunity presented by digitisation and innovation

Digitisation and innovation are increasingly seen as opportunities to attack fundamental problems and inefficiencies in both clinical and administrative processes, as well as creating the potential for new value. Hospitals wanting to simultaneously digitise and pursue innovation at scale face a number of underlying challenges related to data, infrastructure and security as shown in Figure 2.



**Figure 2:** Opportunities and challenges presented by digitisation and innovation

### Digitisation is an important lever for hospitals to meet the challenges

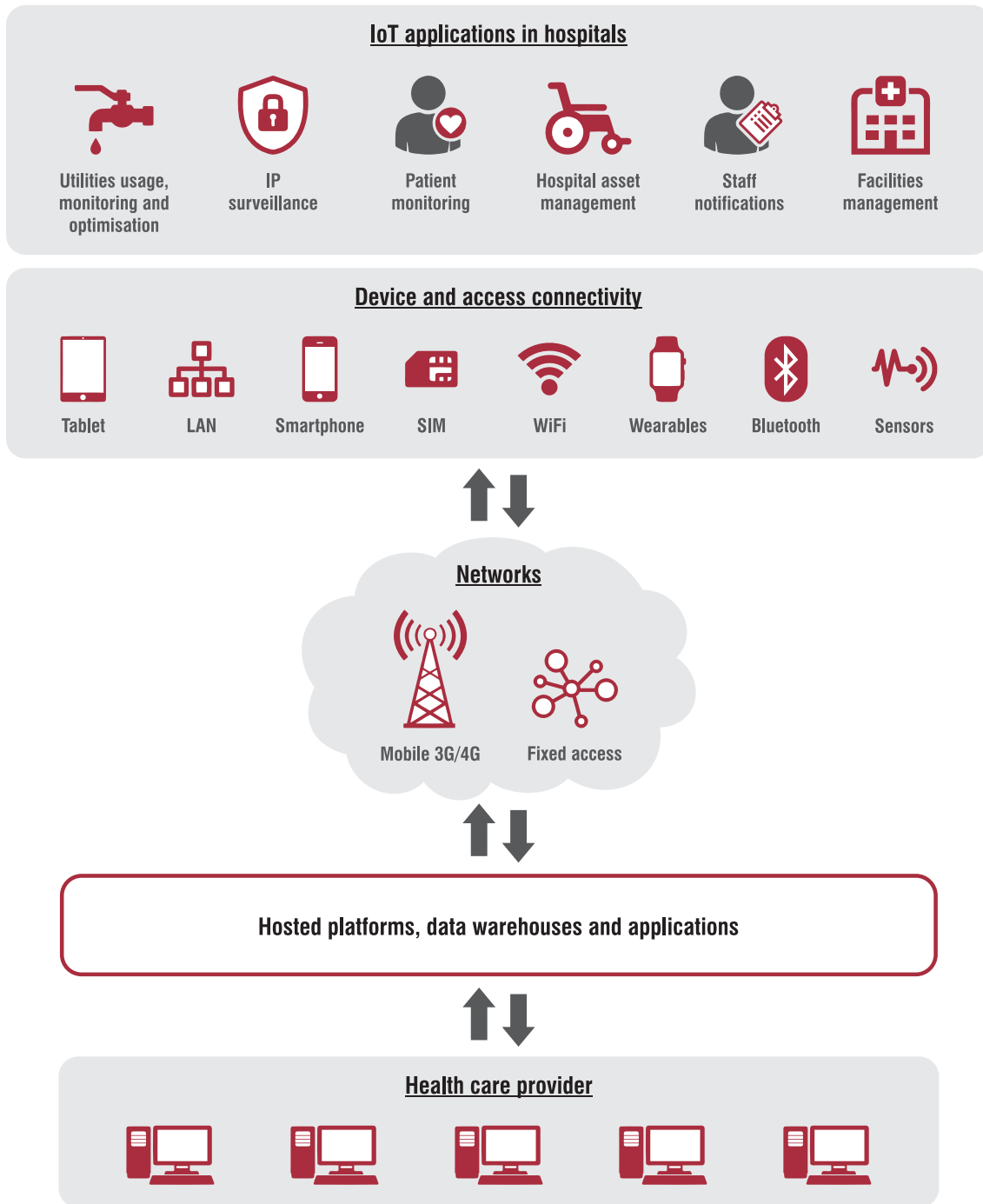
The health sector has a strong track record in adopting specialist clinical technologies and devices, but less so for information and communication technology (ICT) and informatics. There are a number of reasons for this, including the fact that realisation of benefits from these technologies tend to involve cultural and process change from clinicians and others. While the situation is changing, there is a great deal of inertia built into work practices designed to support legacy systems and approaches. There are other reasons, including:

- The high cost of ICT
- A bias among funders to invest in hospital beds over enabling capability including technology
- Patchy digital literacy across the broader healthcare system including among policy makers, funders and hospitals (board, executive, management and clinicians)
- Incompatibilities between supplier software suites, in a market where the plethora of technology solutions are more emerging than mature

Rapid advances in technology are not only creating new opportunities for hospital digitisation, but also the prospect of more rapid and successful implementation. Developments related to the Internet of Things (IoT), big data and analytics, data visualisation, mobility and software create additional functionality but also different commercial models. The IoT is potentially the most disruptive of all technology changes on the horizon. IoT describes the mass connectivity of things and sensors to the Internet, including wearable, embedded, diagnostic and medication devices. At present only 2% of all things that will be connected to the Internet are currently connected.<sup>13</sup> IoT is being referred to as the industrial phase of the Internet, with some commentators suggesting the impact of the IoT

13 Evans D (Cisco) 2011, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*, Cisco IBSG, <<http://cisco.com.au>>

will be more profound than the impact of the Internet itself, fuelling a new era of innovation. In health, the applications of IoT could range from sensors monitoring blood sugar levels and heart rate, to theatre utilisation and power consumption. RFID (radio-frequency identification) technology has been used to track hospital equipment but is increasingly deployed for continuing care and to improve patient safety. Figure 3 depicts potential IoT applications in health and underpinning technology.



**Figure 3:** Sample IoT applications in health and underpinning technology

Wireless patient ID tags will enable clinicians to immediately identify a patient's location, enabling them and their critical information to easily be located in the event of a secondary emergency or urgent check-up.<sup>14</sup> Consumer health tech is a growing market, with 'wearables' forecast to be a \$50B global market in the next two years.<sup>15</sup> Wearables such as fitness tracking devices have largely had 'infotainment' value to date, but as their sophistication and accuracy grows, their healthcare potential will expand. They are also transforming industries; 90% of Weight Watchers' market value has been eroded by the growth in fitness and nutrition apps.

A potentially significant benefit of IoT is increased transparency. More data will be captured about people and processes, creating opportunities for optimisation and better coordination. As an example, dynamic way finding allows a patient's phone to guide them to where their appointment is in the hospital, and simultaneously notify the clinic that they are in the building. For staff it includes the ability to quickly find items of equipment, including whether they are in use or storage, or the ability to assign tasks and notify an individual clinician based on their location and individual skill set. In the more distant future driverless vehicles might be deployed in a non-emergency situation to collect patients, using sensors to provide information about patient condition as it makes its way to the hospital.

The connection of things, of itself, does not necessarily create a platform for change. One of the reasons for the interest in IoT is the parallel advance in mobile technology and big data, analytics and data visualisation. The former is important because it enables sensors and people to establish a continuous connection (e.g. via Bluetooth, 3G, 4G or WiFi). Big data/analytics technology allows the immense tracts of data captured from IoT sensors and other sources to be processed and visualised, creating vital insights into changes to hospital workflows and processes.

## Investment in technology of itself is not sufficient – hospitals need to be effective innovators as well

There is an inextricable link between technology and innovation. The deep interest in innovation by government, industry and institutions is partly driven by the need to capitalise on the current wave of digital disruption. While islands of innovation excellence exist across the Australian health system, it has not typically been seen as core business, adequately resourced or approached systematically. Innovation has not generally been linked to the overall hospital strategy, nor particularly visible to staff and the board.

One of the most difficult decisions for hospitals is how to treat innovation from a structural perspective. Innovation tends to come from the 'edge' of organisations rather than the core. There are a number of reasons for this, including the fact that a hospital often has a complex set of antibodies designed to resist disruption and change. In some cases this is a positive force, particularly when it comes to delivering predictable and consistent workflows. But it can also stifle innovation and change and prevent the promised benefits (including productivity savings) of digitisation from being realised. Some of the most effective hospital innovators, including the Mayo Clinic and MD Anderson, promote the notion that innovation needs to be seen as everyone's role, not just the domain of innovation specialists.

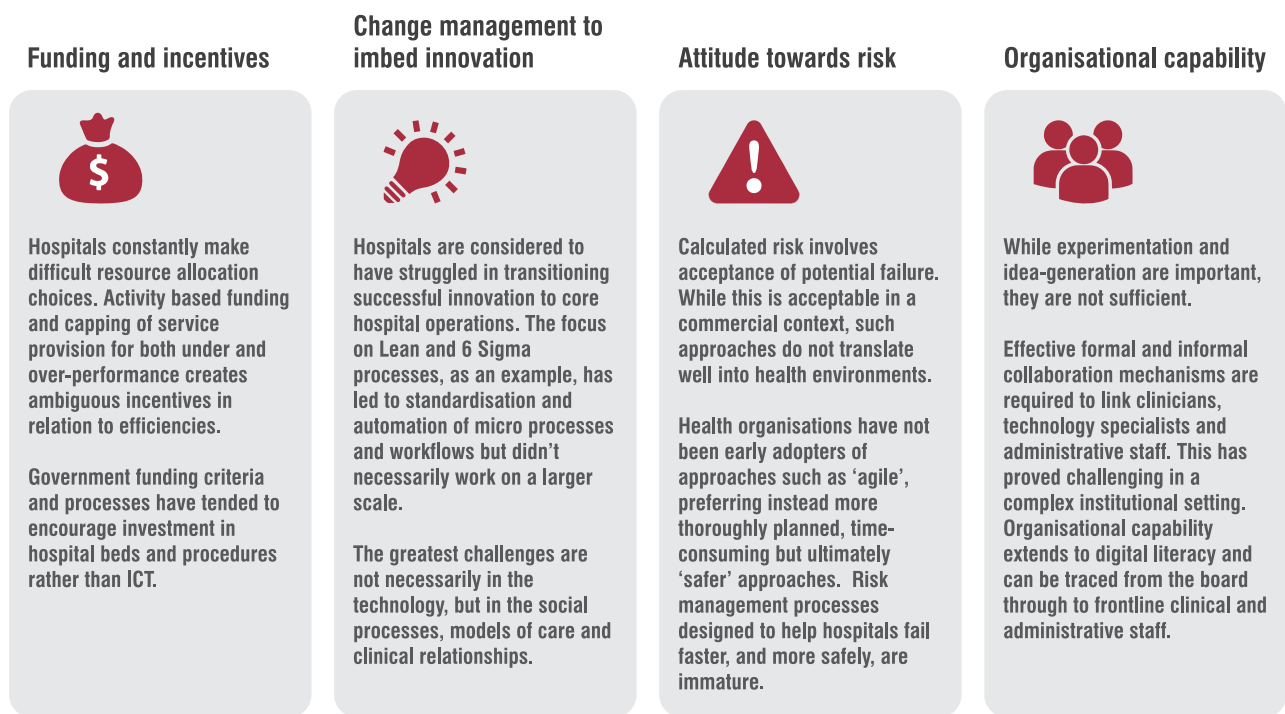
Another difficult decision for hospitals is when to adopt technology. Adopting immature technologies can be risky and expensive, and hospitals are particularly conscious of the risks associated with adopting 'orphaned technology' in a period of such immense technology disruption. But there is also risk in not adopting technology as it becomes available, including the potential for hospitals to forgo improved business processes, reduced clinical error rates and productivity savings. The notion of risk for both innovation and technology require careful balancing.

---

14 CSIRO 2014, *A Digitally Enabled Health System*, <<https://publications.csiro.au/rpr/pub?pid=csiro:EP145606>>  
15 Onworld 2014, *Mobile Sensing Wearables, a Market Dynamics Report*, <<http://onworld.com/wearables/>>

# Part 3: Challenges in capturing value and managing risks from digitisation and innovation

Hospitals are asking themselves the question: what will it take to capture more benefits from digitisation/innovation than we have in the past? While there is no simple answer, getting the underpinning capability in place is critical. A broad range of issues have prevented hospitals capturing value from innovation and digitisation, depicted in Figure 4.



**Figure 4:** Capturing value from innovation and digitisation

Three specific challenges were identified as critical if hospitals are to position themselves for digitisation and innovation:

- How to move from simply capturing data to making genuinely data-driven decisions and performance improvement
- How to ensure the hospital's digital infrastructure is robust, scalable and sustainable to meet current and future needs
- How to manage cyber risk without stifling innovation

## Challenge 1: How to move from capturing data to making data-driven decisions that drive performance improvement

### Profile of a data-driven hospital

A data-driven hospital has the ability to predict – not just monitor – its performance and make more informed decisions about interventions. Hospitals making real-time use of data have the capacity to predict patient volumes, monitor readmissions, prevent unnecessary admissions (for chronic conditions in particular), avoid medication errors and further personalise treatment. Digitisation also has the ability to improve process coordination and patient flow, with downstream impact on both operational efficiency and patient experience. A data-driven hospital would have the capacity to interact with other healthcare providers and support patients being treated in the most appropriate setting, be that the home, acute facility or aged care facility.

Radiology and pathology reports would be automatically reconciled with records of treatment, highlighting incidences outside standard procedures. A similar approach could be used to help clinicians match seemingly disparate symptoms over time in order to deliver more accurate diagnoses for chronic conditions such as diabetes.<sup>16</sup> Data would be accessible in real time to members of multi-disciplinary clinical teams treating patients with comorbidities, and available to different members of the increasingly integrated healthcare system, ensuring information risks associated with transitioning patients between home or sub-acute and acute settings are appropriately managed. A data-driven hospital would improve transparency around bed utilisation and management, and get the ‘hygiene’ factors right, including data accuracy, governance and security.

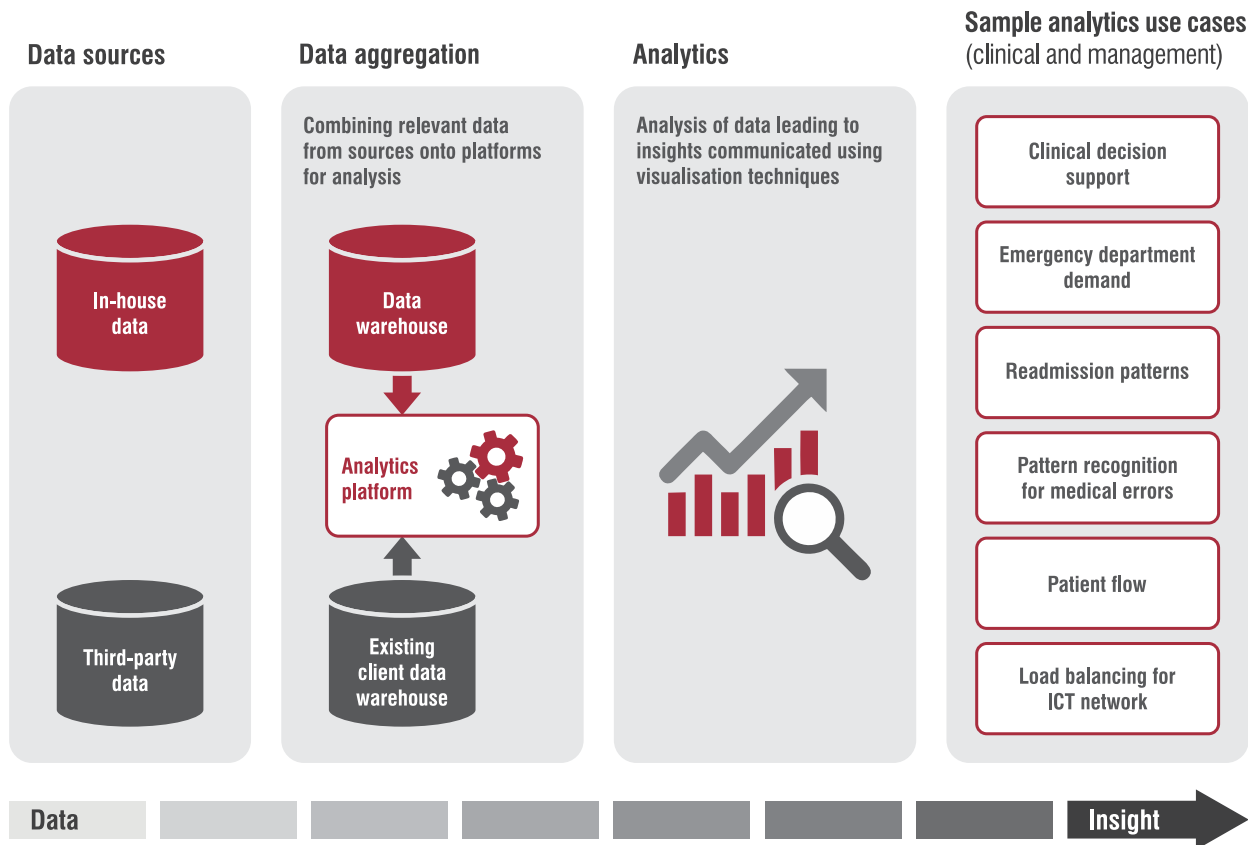


Figure 5: The data value chain

### Case study – Using data to forecast the impact of ‘winter’ in Queensland hospitals

Anticipating and planning for seasonal demand presents challenges for many hospitals. Queensland Health<sup>17</sup> recognised that better forecasting seasonal demand could improve both efficiency and patient outcomes. The Department collected historical data from hospitals to forecast the impact of ‘winter’ on operations. It established that winter was not a significant health event for some hospitals, but a major issue for others. The data allowed hospitals to make more informed resourcing/rostering decisions, reduce patients’ waiting times and avoid the costs of rostering clinicians unnecessarily.

<sup>16</sup> CSIRO 2014, *A Digitally Enabled Health System*, <<https://publications.csiro.au/rpr/pub?pid=csiro:EP145606>>  
<sup>17</sup> This work was undertaken by the Clinical Excellence Division, Health Improvement Unit of the Queensland Health

## **Barriers to progress**

Hospitals have experienced significant challenges in exploiting the full value of data to drive improvement in hospital performance.

Reasons include:

- a) Poor systems for capture/coding of data – particularly data in image and handwritten and audio formats.
- b) Data resources have been skewed to meeting conditions of funding requirements rather than hospital performance.
- c) Processed data isn't always accessible/meaningful to the people who can use it to make decisions.

## Developments that could influence how hospitals may respond in the future

### *Data is becoming cheaper and easier to process*

Advances in tools and expertise related to big data, analytics and visualisation creates significant possibilities. Big data analysis was, until recently, the exclusive domain of specialist researchers supported by super-computing infrastructure. As the price of computing and storage power has decreased, and the power of tools has increased, big data capability is now accessible to start-ups and medium-sized companies. These advances are forecast to gain pace as billions of new sensors are connected to the IoT. Integration issues between datasets have been among the limiting factors in creating sophisticated analytics capability, but are being resolved. For example heuristic matching takes a rule-based approach to match records from different datasets and has been applied successfully to health. The manual matching of ambulance and hospital system data in one Australian state was estimated to take six weeks of full-time effort by an employee, but reduced to four seconds using heuristic-matching technology.<sup>18</sup>

### *The capacity to effectively deal with data is seen as a competitive advantage*

Data has been described as 'the new oil'. Unlike oil, the value of data comes not from its scarcity, but from its abundance. The value of data increases as new sources are tapped and these sources can be correlated with existing datasets. In a hospital context this value manifests in everything from clinical decision-making to new patient workflows and better resource planning. The capacity to exploit data will de-risk hospitals and provide them with a competitive advantage in the quest for productivity and improved outcomes. The challenge for hospitals is doing so when experts in health informatics, clinical coding and analytics are scarce and global demand for data scientists is projected to exceed supply by more than 50% by 2018.

## **Case study – A marketplace for anonymised data**

The California Health Information Exchange (Cal INDEX) is a data exchange that links the medical records of nearly nine million patients served by a range of different health providers. As well as providing an integrated electronic health record service, Cal INDEX provides participating hospitals and researchers with access to anonymised records, which they can draw on for a range of applications. For example, clinicians mine the data to assess the relative success of different interventions to inform treatment strategies, while administrators use the data to benchmark hospital performance and identify potential areas for improvement.

### *Failing to analyse available data may no longer be a legitimate defence*

As understanding of data's value increases, and the capacity to undertake sophisticated analysis improves, hospitals will be under increased pressure to be more data-driven, not just more transparent. This pressure is likely to come from regulators, funders and patients who increasingly expect that available technology (e.g. big data and analytics) will be fully exploited, particularly in areas of high risk such as medication errors. The legal ramifications of this trend are also potentially significant when you consider that a hospital may be deemed accountable for what they should have known – or could have known – not what they did know.

### *Innovation objectives – not just information security – are being represented in decisions about data governance*

A hospital's policy for sharing data is increasingly important and complicated. On one hand hospitals need to maintain adequate information security, which tends to result in restrictive policies and highly privileged access. On the other hand the hospital's desire to promote innovation creates pressure for more open access to all but the most sensitive, individualised data. Hospitals committed to using data as a platform for innovation are broadening rather than restricting data access in what McKinsey described as a 'sharing, with protections' philosophy.

### **Implications/questions for boards**

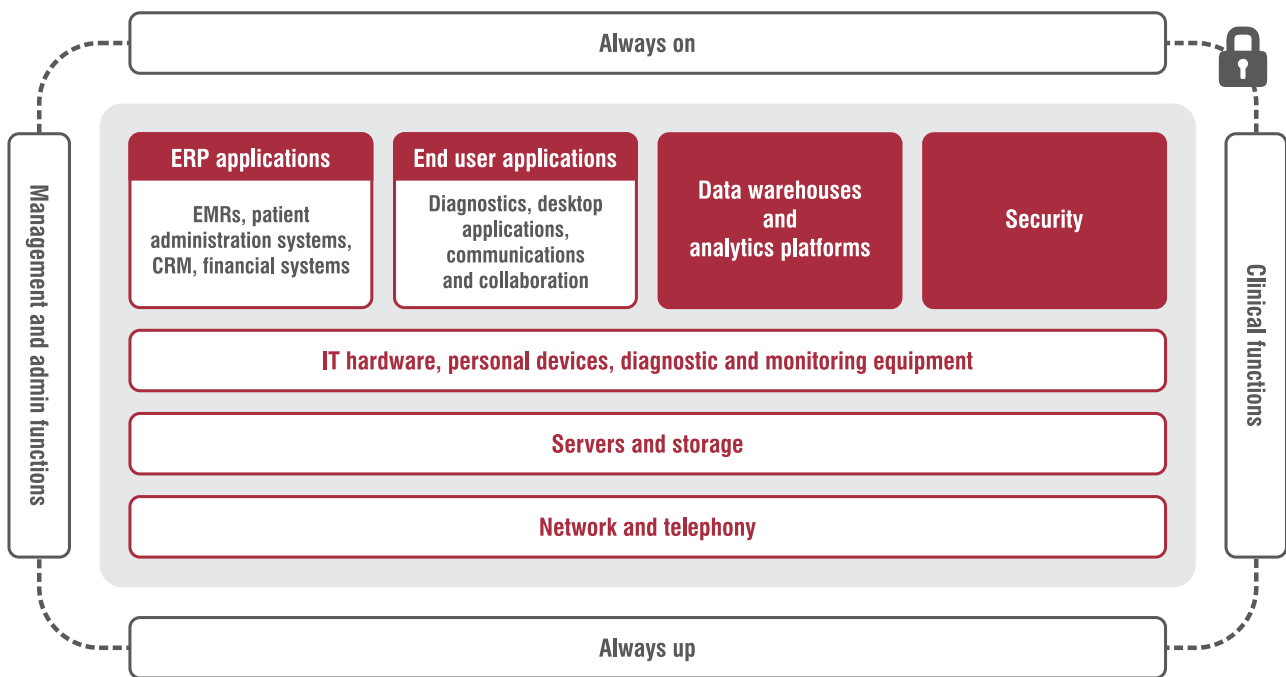
Changing technology and governance in relation to data raise the following questions:

- a) Does the board have a clear and shared understanding of what data is most important in assessing clinical and operational performance, including an understanding of how others are using data?
- b) What new data should boards demand, given the availability of new technologies, tools and techniques?
- c) Are boards being provided with sufficient data to make decisions, and is it provided in a clear and contextualised form?
- d) Are data policies stifling innovation, and could they better reflect the hospital's desire to innovate and collaborate?
- e) Does the hospital have sufficient human capacity, expertise and IT literacy as well as ICT hardware/software to comprehend the wisdom within hospital and external data?

## **Challenge 2: How to ensure the hospital's digital infrastructure is safe, secure, reliable, scalable and sustainable**

### **Profile of a scalable and future-proofed hospital**

Digital infrastructure broadly refers to networks, servers and storage, device integration, security and unified communications that sit within a hospital's technology environment (see Figure 6). The underlying digital infrastructure needs to support the organisation's current and future business objectives, and be 'always on, and always up'. Robust digital infrastructure is smart enough to predict and remedy potential issues, and when a system fails a back-up is available and does not disrupt business continuity or compromise patient safety. Future-proofed hospital infrastructure will need to support the rapid uptake of bandwidth-rich clinical applications (Telehealth, digital imaging and remote monitoring), increasingly powerful Electronic Medical Record (EMR) systems and a broad range of smart services (from sensor-enabled energy, waste and building management to smart parking and lighting). The infrastructure also needs to be capable of evolving, dynamically responding to rapidly changing diagnostic and treatment technologies. An under-emphasised component of digital infrastructure relates to the tools that enable staff to access and use clinical and management data housed in databases and repositories.



**Figure 6:** The hospital's digital infrastructure

### **Barriers to progress**

There is growing concern that hospital infrastructure is barely able to support current demand, let alone be capable of scaling to meet future requirements. This risk is heightened as hospitals' core clinical and operational systems are increasingly reliant on a high-functioning network. Reasons cited for current challenges include:

- a) High-profile ICT failures which have had a chilling effect on investment in ICT generally, including infrastructure.
- b) 'Back office' ICT has not necessarily been seen as a clinical priority in the way that clinical technology has been.
- c) Digital infrastructure has not been seen as a strategic asset worth the significant investment.
- d) It's been easier to avoid – or delay – investment in infrastructure than other priorities.

### **Developments that could influence how hospitals respond in the future**

*The pace of hospital digitisation is pushing infrastructure to breaking point – and failure will be catastrophic*

Requirements for voice, video, mobility, storage, computing power and security have been driven by demand for health analytics, information systems, patient services, business management tools (including collaboration tools) and a growing list of 'smart' services such as smart lighting, smart energy and smart parking. As hospitals have committed to digitisation of their services, cracks have begun to appear in legacy infrastructure that is not necessarily scalable, robust or future-proofed. As an example, networks are often tested when new software applications are deployed, creating risks for both the network but also the user experience for the new application. Infrastructure is also being tested by on-demand and cloud-based services, where service availability is subject to the stability and dimensioning of the network. WiFi and mobile phone black-spots take on much greater significance than 'inconvenience', given they could result in the complete suspension of services.

### *Commercial models are changing, creating opportunities and risks*

New technologies have created new commercial models for the procurement of infrastructure services. The rise of ‘as a service’ commercial models was initially dismissed as merely an accounting change (i.e. from capex to opex). However, the rapid uptake of cloud services (Australia was one of the world’s earliest adopters of cloud services) has been driven by the desire to take cost and complexity out of the management of ICT. The need for consumption-based service agreements with suppliers is a major challenge. Hospitals are often funded for new processes on a capex basis, meaning that the initial systems implementation is funded but not the ongoing maintenance and upgrade path.

### *Hospitals are treating digital infrastructure as an innovation enabler*

The network and other aspects of hospital infrastructure have generally been viewed as a cost centre and unavoidable expense. However, organisations are increasingly recognising the critical role of infrastructure in providing information that is contextual to the patient and staff needs, has the ability to connect people to each other, support collaboration and makes access to information both easier and more secure. All these capabilities enable new and more effective models of care and operational models – the absolute core business of the hospital. Organisations are increasingly looking at what their infrastructure might support beyond critical business requirements. The Australian Centre for Health Innovation at the Alfred Hospital in Melbourne is an example of a facility that is absolutely dependent on a high-quality digital infrastructure, and an example of a ‘living lab’. The emergence of living labs in hospitals – particularly in Europe – provides some insights into how the hospital’s infrastructure backbone can be applied to innovation. San Raffaele Hospital in Milan operates a City of the Future Living Lab to trial a range of digital health services in a practical, real world setting. Hospitals are increasingly realising that investments in infrastructure, big data, storage and security can be leveraged for innovation benefits.

#### **Case study – When even the lights are connected**

The Danish Outdoor Lighting Lab (DOLL) is currently trialling a range of lighting applications with relevance to hospitals. DOLL has proven that the intensity and colour of light can be varied to create different effects. Blue light, for example, is proven to reduce stress in psychiatric patients and patients in recovery rooms benefit from lighting that becomes stronger as the patient recovers. Lighting becomes one more application that needs to be supported by the hospital’s WiFi network.

### **Implications/questions for boards**

The growing importance of digital infrastructure raises the following questions:

- a) Are we investing in the tools and technologies that will allow clinicians and management to extract value from major investments in data systems?
- b) Is it fit for purpose and does it anticipate scale and innovation requirements into future years, including new smart services presented by IoT?
- c) Is governance of IT cognisant of potential failures in the design, implementation and use of digital technologies?
- d) How robust is the hospital’s digital infrastructure, including back-up systems and redundancy, and do opportunities exist to optimise existing infrastructure rather than expensive upgrades?
- e) How do we accommodate and benefit from new commercial models given the move away from one-off capital expenditure to annuity payments for services?

## Challenge 3: How to manage cyber risk without stifling innovation

### Profile of a secure hospital

The prospect of cyber attack and disruption is a constant and growing threat. The theft of health records is the primary threat to hospitals. Estimates suggest that someone's health record is worth up to 10 times the price of an individual's credit card information on the black market,<sup>19</sup> but potential risks extend far beyond the theft of health records.

Cyber resilience goes beyond the hospital's own systems – it involves monitoring the supply chain to the hospital and ensuring that a weakness in a supplier's systems and data integrity cannot be used to backdoor into the hospital systems. In one high-profile case,<sup>20</sup> Lockheed-Martin's secure defence work was compromised by a weakness in a supplier responsible for secure encryption keys (RSA). Theoretically any number of hospital partners and suppliers could inadvertently create a hole in the hospital network.

The desired end state is that a hospital's infrastructure and systems – and organisations that are integrated into hospital processes and workflows – are resilient to cyber attacks. When an attack is detected, damage is avoided or minimised and costs for remediation are contained. Another desired outcome is that cyber security measures do not unduly impede the hospital's capacity to innovate, share data and function effectively.

### **Barriers to progress**

- a) Cyber security was not seen as a priority and treated as an operational IT function.
- b) The 'closed-door' approach to cyber by organisations has hidden the problem from view.
- c) Cyber resilience is costly and complex.

### Changes that might influence how hospitals respond in the future

#### *Hospitals are a bigger target for cyber attack*

The Identity Theft Resource Center in the US reported that healthcare accounted for 43% of all breaches in its 2014 Data Breach Category Summary. This is consistent with a separate KPMG survey of more than 200 US-based healthcare executives that concluded healthcare organisations were at the high end of the risk spectrum for cyber attacks. Approximately 80% of surveyed healthcare executives reported their IT environment had been compromised by cyber attacks, primarily from typical financial fraud and medical insurance fraud. In 2015 the US Government warned that medical devices were vulnerable to hacking. In one particular case, officials said an infusion pump could be modified to deliver a fatal dose of medication. Given the forecast explosion in connected medical devices as part of IoT, this warning takes on greater significance particularly given these sensors are unlikely to be patched to full security.

19 Humer, C & Finkle, J 2014, *Your medical record is worth more to hackers than your credit card*, Reuters, <<http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924>>

20 Watts, S 2011, *No excuses for Lockheed Martin Cyber Attack*, Computerworld, <<http://www.computerweekly.com/opinion/No-excuses-for-Lockheed-Martin-cyber-attack>>

Beyond hospitals, cyber security breaches are rising in Australia generally. Australia had a 109 per cent increase in cyber attacks in the past 12 months – almost triple the 38.5 per cent global average.<sup>21</sup> Another malicious threat to hospitals is ransomware,<sup>22</sup> where the attacker gains access to a hospital's system and encrypts data before demanding a ransom. One challenge for hospitals is that staff have the potential to create windows into the secure network. A high proportion of breaches are attributed to human factors such as transmitting data over unsecured networks and applications. This requires vigilance on two fronts: a) to ensure staff are educated about the dangers of going outside of secure networks and 2) to implement an identity management strategy that ensures the hospital can validate users' identity before they join the network. The use of biometrics, as an example, is one such form of identity validation and has the added advantage of reducing the reliance on user passwords which are more hackable.

### **Case study – Digital technology is walking through the door**

Clinicians have access to powerful consumer technologies, and use them in their workplaces to supplement and/or workaround hospital systems. An example of a workaround would be the use of camera phones by clinicians to photograph medical symptoms and transmit them to colleagues via public networks. This practice would be innovative and pragmatic, but also highly insecure and illegal. A study by Intel<sup>23</sup> asked frontline staff how commonly 'workarounds' were used in their organisation, including personal devices/apps and social media that may be out of compliance with policy. Approximately 21% said it happened every day, 30% sometimes and 21% rarely. Only 9% said it never happened (the balance said they didn't know).

### *The way hospitals are thinking about the return on investment from cyber security is changing*

Cyber criminals and hackers are not the only ones who understand the value of online fraud. Hospitals understand the cost of cyber security lapses. A recent study put the average cost of an Australian data breach (per event) at A\$2.82m.<sup>24</sup> McKinsey<sup>25</sup> found that the majority of costs related to an attack resulted from an inadequate response to a breach, rather than the breach itself.

The other 'hidden' cost of cyber is its effect as a brake on innovation. Cyber security is now more likely to be seen as a 'growth' enabler, not just a threat. Cyber security has been compared to the brakes on a Formula One vehicle. The brakes do not propel the car, but braking performance is a major contributor to fast lap times. Hospitals face the same choice: slow down the 'vehicle' so that braking performance doesn't matter as much, or invest in the performance of its cyber environment.

### *Understanding of how to deal with cyber threats has matured – including greater collaboration on security*

One of the challenges for hospitals is identifying what represents an adequate level of cyber resilience. Even the most resilient environments detect threats in their environment; the challenge is how to deal with it. The traditional approach to cyber security in hospitals was characterised as perimeter-based defence. The focus has changed to defending the organisation from the inside by embedding security into the cellular structure of the organisation itself, in the same way that lymphocytes can recognise and respond to an infection within the human body. Institutions are also adopting a more collaborative approach to security. Hospitals will increasingly need to work closely with law enforcement agencies, government, vendors and other hospitals to gather intelligence and reinforce their operations. This spirit of openness extends to the workforce, with some organisations using innovative techniques including gamification to better inform staff of their cyber security obligations and risks.

- 
- 21 Accountants Daily, *Australia number one for cyber security breaches*, <<http://www.accountantsdaily.com.au/latest-news/17-news/8626-australia-suffers-world-s-highest-cyber-security-breaches>>
- 22 Zetter, K 2016, *Why hospitals are the perfect targets for ransomware*, WIRED magazine, <<https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/>>
- 23 Intel Corporation, 2013, *Workarounds in Healthcare, a Risky Trend*, <<http://www.intel.com/content/www/us/en/healthcare-it/workarounds-in-healthcare-risky-trend.html>>
- 24 IBM 2015, 'Ponemon Institute's 2015 Global Cost of Data Breach Study', <<http://www.-03.ibm.com>>
- 25 McKinsey & Co 2014, *The rising strategic risks of cyberattacks*, McKinsey Quarterly <<http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rising-strategic-risks-of-cyberattacks>>

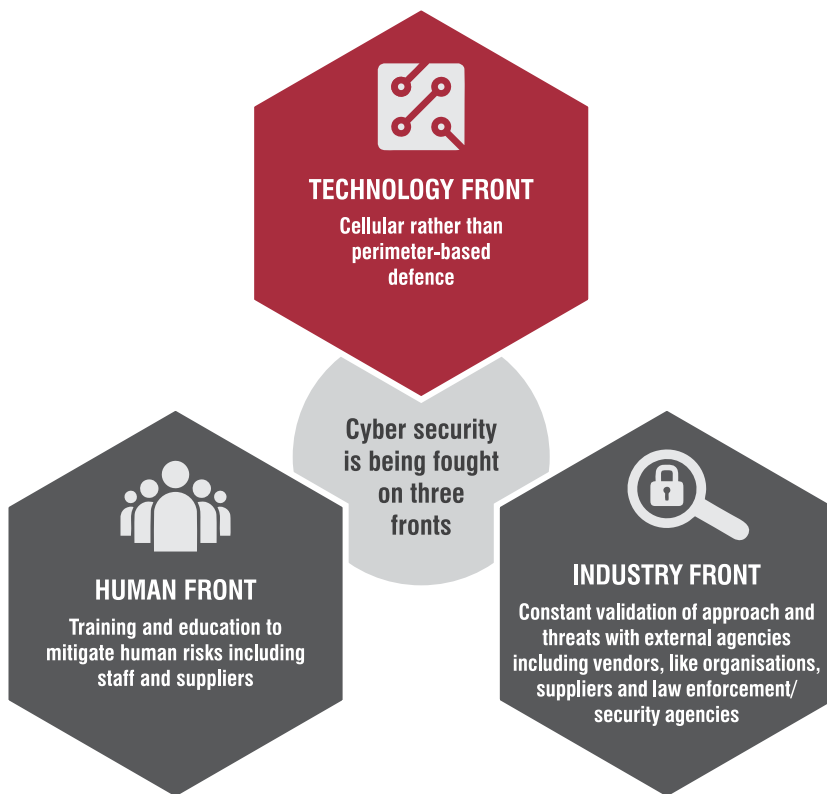


Figure 7: The three fronts of cyber security

### Implications/questions for boards

The increased threat of cyber security raises the following questions for boards:

- Who is responsible for cyber security, and is there any ambiguity about roles and responsibilities?
- Is the level of cyber resilience appropriate, and how does that compare with other hospitals?
- Is the hospital undertaking appropriate external validation, and learning what it can from others (including other hospitals, law enforcement and industry)?
- Is there a clear policy in place for managing integration of new virtual and physical infrastructure, and interactions with external parties?
- Do we know where the hospital's most sensitive data is located, who can access it and how it is controlled?

## Part 4: Implications for hospital boards

Despite the inherent benefits offered by digitisation and innovation, there is an underlying anxiety about hospitals' capacity to resource a large-scale digitisation effort and make the changes to workflows and practices needed to deliver a return on that investment. Hospitals are particularly focused on the costs and risks associated with investing in ICT at the cutting edge.

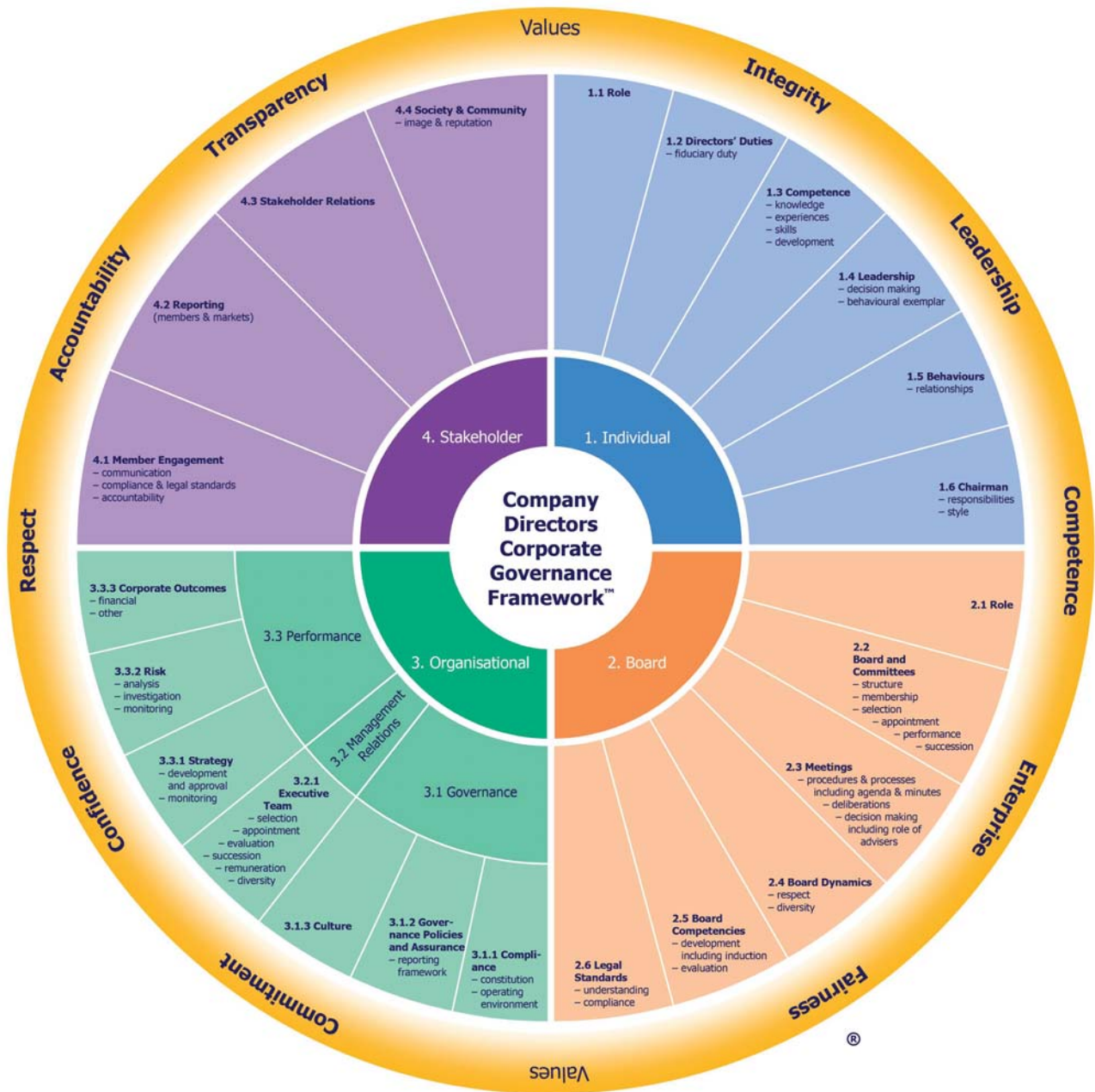
The interpretation of risk is starting to change, particularly when the risk of doing nothing is potentially devastating. Doing nothing – or not doing enough – could leave poor performance undetected, major systems inoperable, patient and organisational data exposed and the institution deemed culpable. Facing a perfect storm of financial factors, avoidance or delayed investment in digitisation or innovation will deliver initial savings, but may ultimately cost the hospital much more in terms of patient outcomes and productivity savings. Deciding where the 'line' is for optimal return on investment on both digital technology and innovation is a major board decision given the size and ongoing nature of investment required.

This report potentially brings a number of board issues and accountabilities into sharper focus. Table 1 describes the potential implications of this study for hospital board members, and executives more broadly.

**Table 1:** Potential actions for boards

Board accountability	Potential actions that could be explored
<b>1. Leadership and culture</b>	<ul style="list-style-type: none"> <li>▪ Demanding better and clearer data sends a powerful signal about what's valued</li> </ul>
<b>2. Setting strategy/direction</b>	<ul style="list-style-type: none"> <li>▪ Need to clarify whether innovation is about experimentation or change (at scale)</li> <li>▪ Set KPIs that relate to data that could be collected, not what is collected</li> <li>▪ Need to establish whether ICT is a genuine 'competitive advantage' or a utility</li> </ul>
<b>3. Clinical risk management</b>	<ul style="list-style-type: none"> <li>▪ Identify clinical data that regulators, funders and patients are likely to require in future and position organisation to meet those demands</li> </ul>
<b>4. Non-clinical risk management</b>	<ul style="list-style-type: none"> <li>▪ Imperative for big data and cyber security policies</li> <li>▪ Hospitals' capability related to data, infrastructure and security need to be assessed against the hospital's strategic objectives (i.e. is it up to the task)</li> <li>▪ Engagement with specialist external parties on cyber security</li> <li>▪ Discourse with management needs to be about balancing risk of being early adopters of technology versus lost opportunity for not investing/doing nothing</li> <li>▪ Consideration of the move from capital to operational expenditure funding for ICT</li> <li>▪ Consider more formalised risk processes for innovation to ensure safer/faster failure</li> </ul>
<b>5. Talent management</b>	<ul style="list-style-type: none"> <li>▪ Skill gap analysis for specialist informatics, analytics and cyber skills</li> <li>▪ Investment in professional learning to increase appreciation of role of data</li> <li>▪ Need for strategic partnerships with specialist organisations</li> </ul>
<b>6. Operation of the board</b>	<ul style="list-style-type: none"> <li>▪ Status of data systems/capability, digital infrastructure and cyber resilience reported regularly to risk and audit sub-committee (not just breaches and failures)</li> <li>▪ Expectation of basic (but growing) digital literacy for all board members</li> <li>▪ Consideration of specialist expertise in cyber security</li> </ul>

It is important to understand these potential implications in the context of board responsibilities. Figure 8 depicts the Australian Institute for Company Directors' (AICD) board governance framework. Using the framework as a guide indicates that the vast majority of implications in Table 1 relate to organisational matters rather than individual, board operations and stakeholder issues.



Note: This is the registered trade mark of the Australian Institute of Company Directors

Figure 8: AICD board governance framework

DANDOLO.COM.AU

---

CONTACT DETAILS

Brad Davies

Level 1, 155 Queen Street, Melbourne, Victoria 3000

E: [braddavies@dandolo.com.au](mailto:braddavies@dandolo.com.au)

M: 0412 256 004