Balancing Innovation and Cybersecurity in Healthcare.

Roundtable 3 Summary Report

INNOVATING health

creating a new conversation

INNOVATING health series

hisa
AUSTRALIA'S DIGITAL HEALTH COMMUNITY

accenture

About the Series

HISA is delivering a new thought leadership series - ***Innovating Health. Creating a New Conversation.***

Through a series of roundtable events and other activities, we aim to lift and support the digital health innovation agenda in healthcare. To create a new conversation, we seek to bring together health leaders with industry experts, challenge current thinking with new and different perspectives, harness our collective knowledge and ideas, and ultimately share topics and discussion with others to stimulate sector change. The series is in collaboration with and supported by Accenture.

Never has there been a time of such pressure on the healthcare system. The need to transform is vital.

Conjointly, the conditions and promise of innovative change are tangible through the development and application of new digital technologies, rapidly changing business models, Government policy reforms, the rise of health consumerism, and service led reform.

"Many of the ways we go about improving health and care were designed in a different mindset for a different set of circumstances.

Given the radical and complex nature of our transformational challenge, these 'tried and tested' methods increasingly won't deliver what we need to deliver for patients."

Helen Bevan and Steve Fairman NHS UK

Event 3 – Balancing Innovation and Cybersecurity in Healthcare Melbourne 27 July 2016

Overview

Whilst we embrace digital programs and solutions to innovate and support health system change, we must be aware of the ever increasing and inherent risks to health operations and the protection of health related data.

This roundtable explored the question: ***how do we balance innovation against risk?***

We welcomed an international guest - **Theresa Meadows,** Senior Vice President and CIO at Cook Children's Health Care System in Dallas Texas, and Co-Chair of US Department of Health and Human Services Healthcare Industry Cybersecurity Taskforce (Taskforce). Theresa provided perspectives on the question of significance and the current state of cybersecurity in healthcare.

Additionally, **Professor Trish Williams,** Chair and Professor of Digital Health Systems at Flinders University, aided Theresa and led the discussion focused on innovation and the digital change agenda within healthcare, which is the theme of this series. Finally, we were also fortunate to have **Simon Eid**, Country Manager ANZ for Splunk, who provided specific insights and industry trends in cybersecurity, analytics and the protection of data across industries including healthcare.

Cybersecurity in healthcare is becoming an increasingly important topic to all stakeholders in health involved in data collection and use. This includes, but is not limited to healthcare service providers, medical device manufacturers, health insurers, pharmaceutical companies, healthcare professionals, and individual patients. Risks posed include legal and reputational risks of loss of confidentially held data, operational risks for organisations whose networks can be effectively shut-down, and identity fraud risks with people obtaining health-related data. In the US, 45% of all hospitals and health service providers faced some cybersecurity threat last year. On the black market an individual medical record sells for $50 USD whereas credit card details sell for just $1 USD. A significant amount of these cybersecurity attacks are automated and originate from all parts of the world. "Ransomware is about making money" and health is an increasingly attractive area as we go more digital.

The roundtable discussion sought to provide an international update on cybersecurity in healthcare, in particular what the Taskforce in the US is aiming to accomplish, and to pose the question of how do we innovate and reform whilst dealing with increasing and more sophisticated cyber threats? The discussion focused on a number of key themes on governance, risk appetite, protecting and sharing information, organisational preparedness, using security as part of innovation, and thinking differently about data in healthcare.

A number of take-away points from the discussion were captured.

Take-Away Points:

1. Increasing focus on the protection of data

Until recently healthcare organisations talked mainly in terms of privacy and consent in regards to the collection and use of data. The conversation is now shifting significantly to the protection of data as cyber threats increase and the risks become better understood. That is, protection of data that is entrusted to organisations and health providers in terms of patients' safety and well-being. In some instances, there are examples of medical information being misrepresented or changed which increases the risk of wrong information being presented for clinical decision making and points of care. **The emphasis is shifting to ensuring patient safety** in treatment, not just in management of their medical records. This discussion needs to emanate up to governance forums.

"Today is less about privacy, and more about safety"
Theresa Meadows

2. Need to share more openly to innovate and respond

Theresa outlined the need to share more openly if we are going to innovate and respond to these threats in healthcare. Generally, when faced with cyber threats or the threat of attacks, our general inclination is to lock things down and not share. This does not enable the health sector to advance on addressing these threats but also in advancing our efforts in a connected health system which is an ultimate goal of digital connectedness. How can we use security expertise, knowledge and experience in response efforts, and views on best practice to address outcomes rather than just close things down is a key factor in supporting change?

We do not need more rules stopping innovation. The US Taskforce is seeking to identify and list threats and guidelines to address as a key output which can be shared and built upon. If we can eliminate common threats and have guidelines for addressing other types of threats, then this would provide a framework for business continuity and service reform which is steadily occurring within the health sector. The goal is not to have new policy or regulations but guidelines on 1) good back-up processes, 2) being able to respond, 3) real-time information sharing, etc. The US Taskforce is due to release its report and guidelines in mid-2017.

"If you don't share data and information you cannot innovate"
Theresa Meadows

3. You need a response plan and need to be proactive

Healthcare has traditionally been a laggard in technology change compared to other sectors, such as banking and financial sectors. For example, the medical device companies are still quite behind in their product development in terms of digital data relay and secure systems to protect information. This is mainly due to fact the process for design and testing of medical devices is too slow and does not keep up with the pace of change.

This said, we are quickly digitising healthcare services and consumers are demanding more. Health organisations and service providers need to have a plan to respond to security threats / attacks and be proactive in enabling new business models while being as secure as reasonably possible. Professor Trish Williams commented on security being a friend and enabler – rather than someone that says no.

With ransomware attacks becoming more common and, increasingly, automated, we need real-time and, potentially, automated responses to threats. It needs to be accepted as part of business that security enables better information sharing whilst protecting patient data and wellbeing.

"The thing about ransomware - always know what your back up plan is"

Cybersecurity Industry expert

4. Think differently about data and, therefore, security

Simon Eid presented the need to track and intervene in real-time and the possibilities of current and emerging technologies that can assist in addressing cybersecurity threats. Simon highlighted the need for real-time tracking and actively monitoring system and network data to identify attempts and threats. He encouraged the participants to think about the fact that current strategies on isolating networks are flawed and that "rule based systems are dead". Alternative approaches proposed included opening up raw data, analysing it on the fly, applying machine learning and behavioral analytics to encourage innovation, enabling real-time monitoring of cyber threats, and gaining answers to questions at a faster rate.

Our issue here is that we have a lot of information, but there is still an inability to share. Healthcare needs to work out ways of sharing data while adhering to data governance and operational principles.

"Data is absolutely key to healthcare change but we need to share"

Simon Eid, Splunk

5. Governance and Risk Appetite

How mature are the discussions of risk appetite within health Boards and across Senior Executive in regards to the digital agenda? The consensus from attendees was that "we accept risk but we don't often talk about them."

The digital agenda and impacts on health systems and organisations are still being understood. The pace of technology change, rapidly evolving consumer expectations and behaviour along with emerging business models pose new and interesting questions for accountable executives and senior decision makers. As we go more and more digital there are increasing examples of operational services being severely affected or closed down due to cyber-attacks.

To balance innovation approaches in health against increasing cybersecurity threats are challenging. However, we need to highlight these discussions and remove the "it won't happen to me" mentality. Digital changes in healthcare are now part of the norm and so must be the questions on how we manage and protect data. Theresa Meadows observed that US Healthcare institutions have started to change their mindset over the last 6-9 months but there is still a long way to go.

"Not if it occurs, but when it occurs"

James Horton, Datanomics

Conclusion - HISA Reflection on the Event

The level of discussion and sharing at our third Innovating Health Roundtable was great to see and we thank the attendees for their participation. We also thank Theresa Meadows, Professor Trish Meadows and Simon Eid for their knowledge, expertise and sharing their thoughts.

Our key take-away as participants and observers at the event were:

- The need to focus on patient safety rather than just privacy.
- The need to share data to innovate in healthcare. This continues to be a challenge.
- The need to have a plan to respond to cybersecurity threats. No more "Not Me" mentality.
- Start seeing security as an enabler for innovation, data exchange and protection of data.
- Advancements in machine learning, natural language processing, and behavioral analytics are innovations that need to be utilised. We need to be thinking differently. Rule based systems are dead.
- Not if but when these threats occur.

We look forward to our next event in the series in Canberra – **Blending of Health and Human Services.**

Innovating Health – Health Leaders in attendance:

- Theresa Meadows, Co-Chair of US Department of Health and Human Services Healthcare Industry Cybersecurity Taskforce
- Professor Trish Williams, Chair and Professor Digital Health Systems Flinders University
- Simon Eid, Country Manager ANZ Splunk
- Dr John Zelcer, Board Member Epworth Healthcare
- Russell Withers, CIO Western Health
- Mei Ling Doery, Clinician
- Simon Goodritch, Portable
- David Rowlands, Managing Director, Rowlands Healthcare
- Ryan Turan, Founder ArtOfCyberwar
- Assoc Prof Jason Potts, School of Economics, Marketing and Finance RMIT
- Shane Smith, Executive Director, Corporate Services, Wesley Mission
- Steve Nicoll, Public Sector Lead ANZ, Amazon Web Services
- James Horton, CEO Datanomics
- Lee-Ann Breger, Program Manager, Health Market Quality Program, Capital Market CRC
- Zoltan Kolkai, Executive Director Eastern Health
- Christine Kilpatrick, CEO Royal Melbourne Children's Hospital
- Dr Vishaal Kishore, Chief Strategy Officer, LaunchVic
- Dr Pradeep Phillip, CEO LaunchVic
- Pablo Borras, Client Executive Accenture Australia
- Dr John Lambert, Chief Clinical Information Officer, eHealth NSW
- Ian Manovel, Principal Innovation Accenture Australia
- Adam McLeod, CEO Melbourne East General Practice Network
- Sofia Chancey, Managing Director Healthcare VIC Accenture Australia
- Dr Mark Santamaria, Emergency Physician, Alfred Health
- Peter Summers, ICT Manager, Alfred Health
- Dr Louise Schaper, CEO HISA
- Greg Moran, HISA Host

Innovating Health Series website resources and commentary –

http://innovatinghealth.org.au/roundtables/cybersecurity/