



# How a dynamic hospital network is critical to optimal patient care

Healthcare Discussion Paper

A discussion paper  
on the foundational  
role of the ICT  
network in **achieving**  
**HIMSS Electronic**  
**Medical Record**  
**Adoption Model**  
**(EMRAM) Level 7**

## 1. Executive Summary

**Hospitals and healthcare providers are adopting more digital technologies at an increasing rate as a way to be more efficient, improve real-time access to operational and clinical information, and access electronic medical records (EMRs) quickly.**

Ultimately, the goal is improved patient outcomes with greater focus on consistency and certainty in the delivery of care. All of this is at the core of their drive towards digital enablement and operational maturity.

Our National Manager of Healthcare, Martin Burns discusses some of the key issues currently facing the healthcare industry, and the role that advances in networking technologies is playing in helping healthcare organizations in their provision of care within Australia.

### As a HIMSS Analytics Certified Consultant for INFRAM in Australia, we can:

- Provide guidance throughout the INFRAM assessment process.
- Assist to identify the gap and provide both road maps and investment costings to bridge the gap.
- Identify key areas for infrastructure optimization and assist with Board submissions on these areas.
- Develop a vendor neutral strategic road map focused on the key priorities to achieve your EMRAM maturity.

#### Examples of the impact of digital transformation:

##### Positive:

- enhanced patient care and collaboration
- closed loop medication

##### Negative:

- increase in the frequency and variety of cyberattacks

## 2. The impact of digital transformation: positive and negative

Information and communications technology (ICT) has always been an important enabler for hospitals and healthcare providers. ICT is no longer just mission critical for the hospital's business and operational requirements. Now more than ever, it has a direct and profound impact on patient outcomes and the patient experience, both positive and negative.

On the positive side, network technologies such as converged data, voice and video are enhancing patient care and collaboration. These telehealth networks are enabling authorized individuals, physicians and other care providers to access critical clinical information about patients from anywhere, without needing to be in a hospital or medical center. This, in-turn, enables patients to better interact with their care providers, extending care beyond the physical hospital walls into patients' homes and doctors' surgeries.

'Closed loop medication' is another area where digital healthcare technology can play a key preventative role. A report from the Pharmaceutical Society of Australia (PSA) calculates the annual cost of medication-related problems in Australia is nearly \$1.4 billion – equivalent to 15% of total Pharmaceutical Benefits Scheme (PBS) annual expenditure.<sup>1</sup> Globally, the cost of medication errors has been estimated at US\$42billion annually, with discrepancies and errors occurring at transitions of care phase contributing to this figure.<sup>2</sup>

The PSA report reveals that 250,000 Australians are hospitalized each year, with another 400,000 presenting to emergency departments, as a direct result of medication errors, inappropriate use, misadventure and interactions.

**The report states at least half of these instances could have been prevented.**

The report also highlights that up to 90% of people may experience changes to medication during a hospital stay. Without verifiable medication reconciliation at discharge, there's a high probability of drug administering errors appearing on the discharge medication list.

<sup>1</sup> Pharmaceutical Society of Australia Ltd, 'Medicine Safety: Take Care', January 2019

<sup>2</sup> World Health Organisation, Medication Safety in Transitions of Care, September 2019

## How a dynamic hospital network is critical to optimal patient care

Closed loop medication management goes a long way to reduce these errors. It's defined by the Australian Commission on Safety and Quality in Health Care as 'the use of technology in the medication management process, from ordering through to administration. It aims to minimize manual selection, input and transcription, to reduce human effort and some risks of human error'.<sup>3</sup>

The implementation of Electronic Medication Management (EMM) can cover the digitization of everything from prescribing and decision support systems, to dispensing, order and supply solutions, all with the patient's EMR as the central point. This can be taken one step further by integrating the network as part of the process. For example, when the barcode of a new vial of medication is scanned at the bedside and checked against the prescription, the network-connected smart IV drip is also recording the dosage as it's being administered, and automatically updating the patient's EMR. This automatic process removes the risk of incorrect or forgotten manual updates to the EMR.

On the negative side, while digital transformation has resulted in incredible improvements in healthcare, it has also made hospitals and care providers targets of cyberthreats, due to the value of personal data and electronic medical records. EMRs are eight to ten times more valuable on the black market than credit card information. Attackers value this information for

identity theft, fraudulent use of healthcare services, prescription medicines, and government or assistance payments.<sup>4</sup>

The COVID-19 pandemic has spawned an uptick in a variety of cyberattacks against healthcare organizations. Ransomware attacks, phishing exploits, fake domains, disinformation campaigns and supply chain disruptions are threats currently facing the healthcare industry. Telehealth comes with inherent cybersecurity and patient privacy challenges, such as protection of Personal Identifying Information (PII), and protection of medical information, including diagnoses, types of medicines prescribed, medical tests, and lab results. All this data can be accessed in the medical provider's patient portal and potentially be exploited if not protected appropriately.

In 2020, we saw the first reported patient death as a direct consequence of a ransomware attack. This took place in Germany, where a patient died after being re-routed to a hospital in the city of Wuppertal, more than 30 km away from her initial intended destination, the Düsseldorf University Hospital. The hospital at Düsseldorf was in the middle of dealing with a ransomware attack at the time and couldn't accept any emergency cases.<sup>5</sup>

**So how do you enable hospitals to be digitally connected, flexible and functional, yet secure at the same time?**



<sup>3</sup> Bainbridge, M., & Askew, D. (2017). Barcoding and other scanning technologies to improve medication safety in hospitals. Australian Commission on Safety and Quality in Health Care

<sup>4</sup> NTT Ltd. '2020 Global Threat Intelligence Report', p 58

<sup>5</sup> Catalin Cimpanu, 'First death reported following a ransomware attack on a German hospital', ZDNet, 17 September 2020

### 3. Introducing NTT Ltd.'s Digital Enterprise Capability Maturity Model for Healthcare

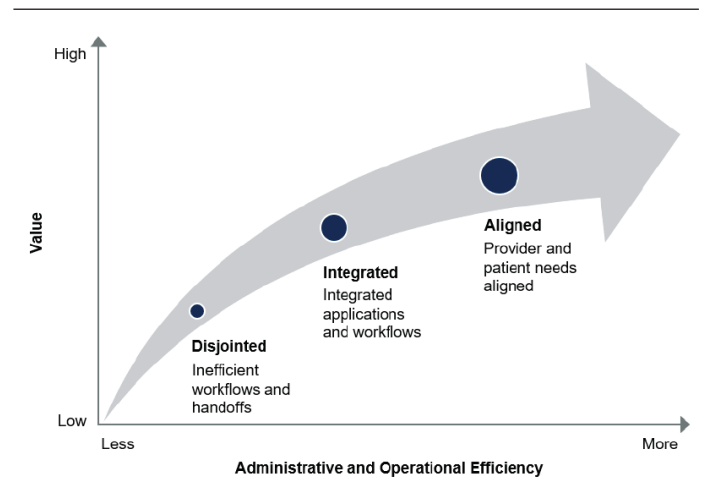
The Healthcare Information and Management Systems Society (HIMSS) Electronic Medical Record Adoption Model (EMRAM) is an eight-stage model that allows a hospital to assess their acute hospital maturity. It is used for inpatients only for hospitals to track their organization's progress in adopting electronic patient record technology against their digital plan or other healthcare providers from around Europe and the world (there's a separate model for outpatients).

Gartner Inc. has a lifecycle model<sup>6</sup> that identifies the inefficiency in workflows and handoffs that are caused by disjointed operations and delayed insights, which results in less effective consumer care.

In 2019, Johnson & Johnson found that inefficient operations limiting throughput and **creating unnecessary variations in care accounted for up to 30% of costs.**<sup>7</sup>

Both of these international models focus on the process. However, the areas that EMRAM and Gartner's models don't address are the required support to enable the achievement of different levels. As a hospital moves up the EMRAM scale it becomes more dependent on digital technologies and therefore needs to consider technology more holistically.

To address the above gap in technology considerations, our Digital Enterprise Capability Maturity Model allows health services to take a holistic view and gain an understanding of the total investment and capability required including the ICT requirements.



Gartner, Inc. Lifecycle of efficient administrative and operational processes



<sup>6</sup> Gartner Inc., Healthcare Innovation Trends: Reinventing Hospital Operations and Administration, Oct 2019

<sup>7</sup> Johnson & Johnson Medical Devices Companies, Health System Leaders Shift Top Focus from Costs to Patient Outcomes, September 2019 services.global.ntt

Achieving the appropriate maturity can no longer be an afterthought. Networks need to be dynamic in nature, self-healing to reduce any downtime and self-configuring to allow changes, both to the security and the flexibility required of a modern hospital.

From a networking perspective with the objective of progressing hospitals to a 'dynamic' state of readiness, NTT Ltd. is leading the field assisting a number of Australian hospitals to achieve EMRAM Level 7. Some of the benefits of this level of maturity enable smart IV drips and connected MRI machines to deliver updated data in real-time across the network and to the patient's EMR instead of relying on paper charts at the end of the bed. Another example is to use the dynamic network to increase the capabilities of remote care and patient monitoring by aggregating and analysing data from bedside devices with a combination of clinician oversight and AI providing scale. Among a number of advantages, this improves the contextual information needed for patient care, optimizes the hospital network and reduces hardware at the bedside. To achieve this, it is critical your network is highly available, ubiquitous and optimized for the necessary digital throughput. This gives hospitals the opportunity to transform the way care is delivered.

At EMRAM Level 7, an ICT failure can result in loss of life.

## HIMSS Analytics EMRAM

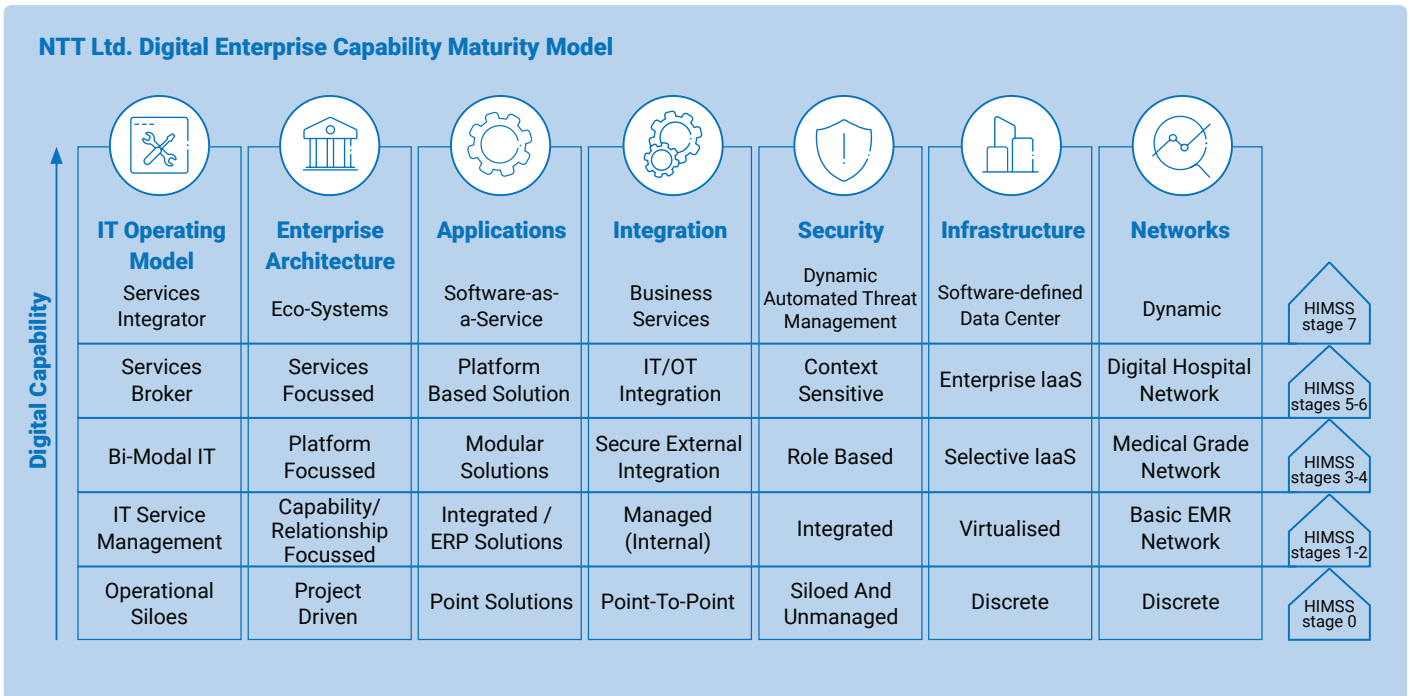
### EMR Adoption Model Cumulative Capabilities

#### Stage

- 7 Complete EMR: external HIE, data analytics, governance, disaster recovery, privacy and security
- 6 Technology enabled medication, blood products, and human milk administration; risk reporting
- 5 Physician documentation using structured templates; full CDS; intrusion/device protection
- 4 CPOE; CDS (clinical protocols); Nursing and allied health documentation; basic business continuity
- 3 Nursing and allied health documentation; eMAR; role-based security
- 2 CDR; Internal interoperability; basic security
- 1 Ancillaries - Lab, Rad, Pharmacy, PACS for DICOM & Non-DICOM - All Installed
- 0 All Three Ancillaries Not Installed

#### HIMSS Electronic Medical Record Adoption Model

- **Charts** progression of adoption for clinics that deliver inpatient care.
- **Advances** hospitals toward better ancillary integration.
- **Drives** organizations to a paperless environment.
- **Provides** a roadmap for system implementation to achieve computerized physician order entry (CPOE), security and analytics to improve health and healthcare.



While the focus of a secure, reliable and fast network is better service and responsiveness to patient care, patient morale is also important. At the more experiential level, patients are now expecting to be able to log on to their own streaming services and watch their favourite shows from their beds.

All hospital services will run on the network, hence network and systems availability is no longer trivial. We've seen that from the impact of ransomware attacks having a direct effect on a patient's well-being.

Cisco SD-Access helps to keep users, devices and applications separate while **Cisco DNA Center** proactively monitors, troubleshoots and optimizes the network.

**Security is critical. There is no fall back.** If the network is down, everything stops and patients may die.

There are numerous measures required to ensure an optimum cybersecurity environment is dynamic and effective. From a holistic perspective, we recommend five key focus areas:<sup>8</sup>

- Implementing third-party software and hardware in a zero-trust environment, prioritizing security throughout the design and implementation of a product lifecycle, and creating operational contingency plans for supply-chain disruptions.
- Implementing and prioritizing patch management. Attacks consistently focused on technology with wide customer bases, using a wide variety of significant vulnerabilities.

- Performing continuous monitoring and threat detection and response to improve visibility into attacks targeting cloud, network, and endpoints to minimize the scope and impact of a breach by enabling faster, and more effective response.
- Securing data at rest, in use, and in transit. Organizations should enhance policies, procedures, and practices by adopting recommendations from frameworks such as NIST CSF, ISO27001, and MITRE ATT&CK.
- Frequently reviewing business continuity and disaster recovery plans. An evolving and dynamic threat environment necessitates organizations revisiting plans if they have them or creating ones if they do not.

<sup>8</sup> NTT Ltd. '2022 Global Threat Intelligence Report', p 27

However, how do you secure the network by isolating critical systems, functions or resources – such as securing RJ45 ports where 95% are public-facing – but still make them immediately available when you need to connect devices to them?

Solutions like Cisco Software-Defined Access (SD-Access) help to keep user, device and application traffic separate with end-to-end segmentation, using advanced AI and machine learning to proactively monitor, troubleshoot and optimize the network.

NTT Ltd. has built a library of each medical device type – an approved list – that integrates with SD-Access to make it much easier for devices to be connected securely.

#### 4. Evolution in hospital networks: from medical grade to dynamic

The requirements of a fully digital, fully mature hospital network require a necessary step-up from medical grade, through digital, evolving into a **dynamic network**. A dynamic network needs to be able to automatically identify and authenticate any allowed device connecting to the network, fixed or wireless, and configure ports, VLANs and the network services required for their operation. The hospital needs to maintain a profile of every device, so that when it's plugged in or it connects wirelessly, the network knows what it is, and can automatically configure the port and the network to that device.

One of the first Australian hospitals to achieve EMRAM Level 7 has deployed a dynamic health network that utilizes our medical device library and Cisco SD-Access enabling faster and secure automated network device deployment, and policy-based automation to deliver services based on hospital priorities.

It has helped to improve efficiencies and patient safety with closed loop medication through the electronic barcode scanning of blood and medication products, as well as providing access to online data to monitor and improve care, sharing patient EMR data with other health care providers. It has significantly reduced re-admission rates, medication administration errors and improved overall alerting and early detection across the hospital.

Another Australian hospital (one of our clients) is achieving the highest level of maturity using digital technologies for clinicians to have a more holistic view of each patient's care with a real-time, consolidated view of the entire patient journey and how the different healthcare disciplines are integrating and working together.

It enables accurate, real-time locating systems that do more than just track a device. It allows everything to be automated: support replacement, device deployment, device security, traffic prioritization, etc.; thereby reducing the operational impact on already stretched ICT support teams.

A dynamic network introduces the concept of an 'as-a-service' model, allowing networks and **services to be switched on and off, be scalable and deployable as required.**

#### Conclusion

While the dynamic network is a foundational element to achieving EMRAM Level 7, there are so many more technology, people and process layers required.

We can assist at all stages – in working with hospitals and healthcare providers in developing their strategic plan and roadmap towards achieving maturity across people, process and technology components, and implementing the projects identified to reach each new stage of maturity.



#### About the author

Martin Burns, National Manager of Healthcare, NTT Ltd. Martin has spent the past five years of a 30-year ICT career specializing in the healthcare sector. Through his National Healthcare role at NTT Ltd. and as an executive sponsor for several major health alliances, hospitals and care providers, Martin shares his perspectives and in-depth experiences on current and emerging technology trends occurring within Australia. Martin is a certified HIMSS Analytics Infrastructure Adoption Model (INFRAM) Consultant, a Graduate of the Australian Institute of Company Directors (GAICD) and acts in a number of advisory roles to senior executives and boards on ICT security, risk, innovation and their application in healthcare and improved patient delivery outcomes.

#### Get in touch

au.info@global.ntt | (02) 8249 5000 | [services.global.ntt](https://services.global.ntt)



