CUBESYS

Data security in the healthcare industry

How to tackle the issue of cyber security in healthcare head-on, and embrace the advantages of a digitally connected workplace.

A state of digital flux in healthcare

Bold digital aspirations

Across Australia, many hospitals and healthcare providers are aspiring to a digitally connected healthcare environment.

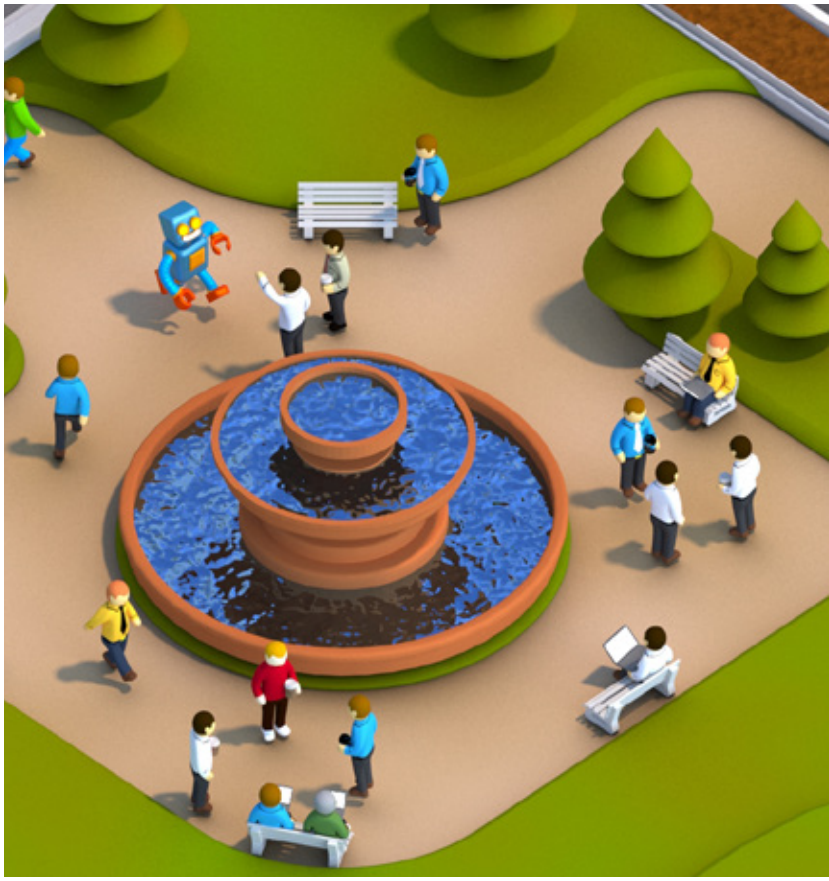
Think innovations like TeleHealth, patient personalisation and wearables; the switch from clipboards, pens and paper to smart devices to give clinicians instant access to patient records in the ward, in a clinic or at home; or the use of the latest communication and collaboration tools to improve patient care.

Pressing security questions

These innovations are transformational for healthcare providers. But how do you expose critical patient data in real-time without compromise? How do you enable end-user self-service so that clinicians can access personal data from any device, without risking non-compliance with rigorous data protection laws?

> ***There's a direct correlation between the growing trend for mobility and the number of data breaches within the healthcare industry. Unless you have the very latest systems in place, you may be vulnerable to security breaches.***

Healthcare providers want to use cloud technologies and connected devices to facilitate records management, improve patient care and cut costs. Question is, how can you do it quickly and cost-effectively, with minimal impact to service levels and maximum protection?



Under attack:
Threats to the healthcare industry

Before we look at what's possible in the healthcare industry, it's important to acknowledge the very real data security threats faced by the industry. Healthcare providers around the world are consistently targeted by hackers, with new vulnerabilities in healthcare security systems emerging daily.

Here are some of the key considerations for healthcare providers keen to improve their security standing.

> ***"Nearly 90% of healthcare organisations in the US suffered a data breach in the past two years, and nearly half had more than five breaches during that period. The total cost was estimated to be around $6.2 billion."***
>
> Ponemon Institute

Beware ransomware

Ransomware is a common problem. Cybercriminals prey on hospitals' reliance on their data, locking them out of their own technology systems and then charging hefty ransoms. For example, when a healthcare provider in Indiana, US, was locked out of its systems it ended up paying $60,000 in bitcoin to get its data back.

Protecting identities

Identity theft is another issue. Healthcare records are hot property for cybercriminals. It is a huge reputational risk to lose confidential patient records through identity theft; and identity theft doesn't stack up well against the responsibility to secure personal information under the Privacy Act 1988.

Complying with tough new laws

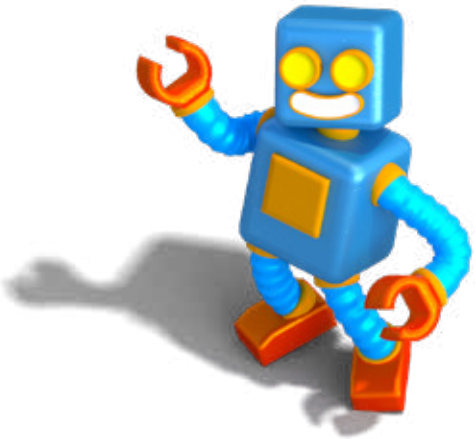
Australia's mandatory Notifiable Data Breach scheme is increasing the pressure to protect patient records, too. From hospitals to GP surgeries, all healthcare providers need to comply with the new legislation introduced in early 2018 – which requires organisations to let patients know if their private information has been leaked, stolen or lost.

If a healthcare provider markets into the EU or holds data on EU citizens, they could also be exposed to significant fines if they don't comply with the rigorous General Data Protection Regulation (GDPR), enforced from May 2018.

Other risks

Then there are data breaches from the likes of malware, denial-of-service (DOS) attacks, employee negligence, mobile device insecurity, employee-owned mobile devices or BYOD, and the security of mobile apps.

It all adds up to a highly volatile environment that, if not controlled, puts your healthcare organisation at significant risk of data breach.



Gold standard:
Bendigo Hospital

Bendigo Hospital is the first healthcare facility in Australia to use Microsoft Azure public cloud technology to create a digitally connected healthcare environment.

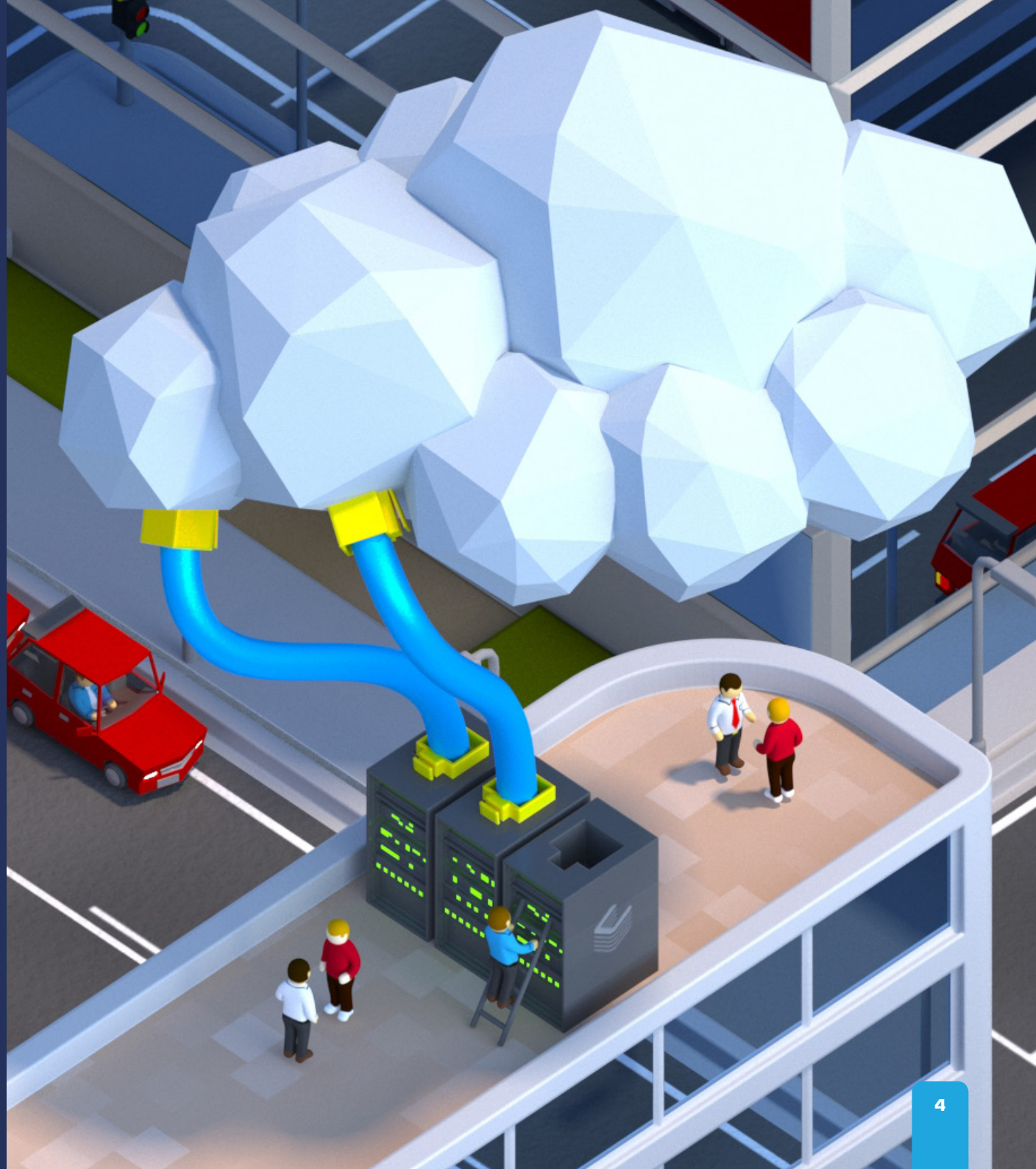
Whereas previously, clinical teams may have had to log into seven or eight separate systems to access the patient information they required, it's all now available instantly to all Bendigo Health employees, from any device.

> ***"We wanted to empower staff to provide world-class, quality care to the community."***
>
> Robyn Lindsay,
> Exec Director of Acute Health

Staff have real-time access to patient information to make safer decisions and facilitate smoother clinical handovers. And the cloud-based system has watertight security to protect against all manner of threats.

It's a true connected healthcare model.

Get the full story



Counter-attack: C.O.P.E Cyber Security

Hospitals and many other healthcare providers are 24/7 organisations.

They need round-the-clock access to critical patient records to support decision making and patient care. They need rock-solid ways to manage compliance, liability and risk – while boosting the productivity and connectivity of their workforce.

And they need cyber security approaches, tools and capabilities to combat the modern threat landscape, so they can constantly monitor suspicious behaviours before significant damage is done.

Corporate Owned, Personally Enabled

C.O.P.E, which stands for 'Corporate owned, personally enabled', is an enterprise-grade modern workplace management structure that simplifies migration to a more mobile way of working.

Designed and implemented by cubesys, C.O.P.E and C.O.P.E Cyber Security, deliver the best of Microsoft Office 365, Enterprise Mobility Suite and Windows 10 so that healthcare employees can do their best work from wherever they are, securely protected from the threats coming from this new landscape.

> ***C.O.P.E redefines how healthcare organisations transform into modern workplaces that leverage mobility for enhanced patient care and service delivery.***

It is a fast and cost-effective way to put secure, cloud-based devices in the hands of hospital staff and healthcare workers – without increasing the burden on internal ITC teams.

Enabling threat protection and security management

C.O.P.E Cyber Security switches on the advanced security capabilities within the Microsoft 365 E5 Suite, bringing the security of on-premises systems to cloud applications.

Using proven apps like Microsoft's Advanced Treat Protection to detect, analyse and interact with Microsoft's cloud, it tips security on its head to capture potential threats before they have an impact.

> ***"We use data analytics to look for anomalies from the inside of the platform, and go into immediate lock-down when anything unusual pops up. It's the most powerful approach to security available today."***
>
> Paul Heaton, CEO, cubesys

Security features that deliver complete peace of mind to healthcare providers include:

- Advanced threat analytics – provides direct line-of-sight to suspicious behaviour, including a real-time view of attack timelines, to reduce risk of costly damage to the business.
- Enterprise-grade security – protection for all cloud apps, data and devices.
- Control over identity and access – centrally managed single sign-on, enforced risk-based conditional access policies, and secure B2B collaboration.
- On-premises security in the cloud – bundles the best of Advanced Threat Analytics, Cloud App Security, Identity Management and Azure Information Protection so you can embrace mobility with peace of mind.

Fast to test and implement

Healthcare organisations can have a pilot of C.O.P.E up and running within weeks, with features turned on for a controlled subset of users so that key stakeholders can evaluate the benefits of the technology faster.

Then, implementation is fast and seamless – so that your team will benefit from a new suite of cloud-based devices that enable collaboration and flexible ways of working, sooner.

About cubesys

With over 20 customers in the healthcare industry, cubesys has extensive experience in helping hospitals and other healthcare providers to navigate the journey to the cloud. As a Microsoft Gold partner, we will show you how to leverage the latest technologies to significantly reduce IT spend and ease the burden on management teams.

To learn more about how C.O.P.E could transform your healthcare organisation, contact cubesys today.

1300 163 712 | E-mail: info@cubesys.com.au

www.cubesys.com.au

CUBESYS