Hyperconnectivity Is A Double-Edged Sword. **Tū Ora Compass Health** Wields It Well

Industry Healthcare
Location New Zealand
Product BlackBerry® UEM
http://www.compasshealth.org.nz/

At a Glance

As we move ever closer to a hyperconnected future, digital technology is rapidly and fundamentally changing the medical industry. Through tools such as connected medical equipment, cloud-based patient care platforms, and advanced collaboration software, practitioners are able to deliver better, more flexible, and more affordable healthcare.

This hyperconnectivity is not without its risks.

Health data is extremely valuable on the black market, with a single patient record potentially fetching thousands of dollars[1]. By contrast, a credit card number may only net a hacker twenty-five cents. Healthcare is a target, and medical industry organisations must keep patient data from falling into the wrong hands.

Yet they also have a responsibility to provide the best care possible. Ignoring the potential represented by hyperconnectivity is not an option. Instead, care providers must balance user enablement and patient outcomes with cybersecurity.

It's a considerable challenge – but one New Zealand-based Tū Ora Compass Health is more than capable of addressing.

A Leader in New Zealand's Health Industry

With more than 150 staff, primary health organisation Tū Ora Compass Health supports a network of sixty general practices. Based in the Wellington, Porirua, Kapiti, and Wairarapa regions, these practices provide primary healthcare services to approximately a third of a million people.

"Nearly all general practices in New Zealand are small businesses," explains Alistair Vickers, Tū Ora Compass Health's Chief Information Security and Privacy Officer. "They're usually owned by general practitioners and other people who work within the practice and rely on Primary Health Organisations (PHOs) for a range of administrative, advisory, and clinical support services. There are about thirty PHOs in New Zealand, across a population of 4.5 million or so - Tū Ora Compass Health is one of the largest and has been operating for over twenty years."

Due to both its size and how long it has been in operation, Tū Ora Compass Health occupies an important role in New Zealand's primary healthcare industry. For one, it is part of the N4 Group – a forum comprising the leadership of the country's four largest primary health organisations. Leaders from the N4 regularly meet to discuss the state of primary healthcare in the country, and how it might be improved.

Being based in the capital city of Wellington, Tū Ora Compass Health is also an active healthcare lobbyist, often called on for its leadership both regionally and nationally on behalf of primary healthcare. The organisation's CEO recently led negotiations to implement a new scheme enabling cheaper access to primary care for low-income individuals across New Zealand.

As a result of the agency's innovative, collaborative approach, it is frequently chosen to lead new health initiatives. Most recently, it was trusted with the implementation of a government pilot programme focused on integrated therapies for young people with mild to moderate mental health concerns.

"Ensuring the wellbeing of all our people is at the core of Tū Ora Compass Health," says Vickers. "We constantly seek ways that we might improve healthcare not just for our patients, but for our clinicians and support staff, as well. It's why in addition to my internal duties, I regularly liaise with district health boards, New Zealand's Ministry of Health, and other primary health organisations and agencies – effective care at any level requires collaboration."

"Especially in the health industry, device security is critical. Usually, people are left to their own initiative in terms of how they manage their personal and work tools. With BlackBerry UEM, we have control over that – over security, the applications we deploy, and the updates we push out. We can mandate the device settings that best protect our data with ease."

Tristan Santer
IT Team Lead,
Tū Ora Compass Health

Aligning Cybersecurity and Patient Outcomes

Health organisations in New Zealand are subject to two national regulatory frameworks, developed by the Ministry of Health and the New Zealand Privacy Commission. The first is the Health Information Security Framework, focused on the security policies, processes, and controls that protect health data. The second, the Health Information Privacy Code, establishes rules around the collection, storage, and usage of health information.

These regulations aside, New Zealand care organisations must also be cognizant of laws like the European Union's General Data Protection Regulation (GDPR). Although Tū Ora Compass Health does not process the data of EU citizens, the standards and best practices are valuable when it comes to protecting patient data. At the same time, the patients must ultimately come first.

Cybersecurity cannot, in other words, interfere with patient outcomes.

"Most practices are driven by a combination of positive patient outcomes and business needs," Vickers explains. "They do not always see the need for additional IT spend. Although they recognise cybersecurity as important, they view it more in terms of hygiene than as a business directive."

In addition to the legislation described above, Tū Ora Compass Health faces several unique challenges of its own. For one, it is a not-for-profit, meaning it must take a conservative approach to IT spending. It also seeks to adhere not just to New Zealand's national regulations, but also to international frameworks such as ISO/IEC 27001.

"General practitioners are holding a lot of sensitive patient data," he explains. "They need to consider how best to secure that information. It's the same for us – Tū Ora Compass Health has a very large dataset, collected from both general practices and a wide range of other sources. We need to keep that data safe at all times."

The most important data Tū Ora Compass Health must protect is clinically-sourced, collected by general practitioners and captured by staff during clinical work. Other relevant information includes human resources data, financial details, and confidential business documents.

Tū Ora Compass Health uses a Corporate-Owned, Personally-Enabled (COPE) deployment model, meaning employees can use their devices for personal matters and the organisation must consider their security alongside the security of patient data.

"We have a duty of care to secure and manage the data of end users and patients effectively," says Vickers. "We need to protect it, protect our staff, protect the integrity of our organisation, and at the end of the day, protect our practices and patients. Often, that means being intelligent and sparing with our security – applying standards specifically where failing to do so will put patient data at risk."

"There is little value in applying standards that have no bearing on patient care simply so we can claim we are compliant, especially if doing so adversely affects patients," he adds.

Delivering Care Where It's Needed

Over half of Tū Ora Compass Health's staff are clinicians trained in a variety of medical disciplines. These include mental health professionals, sexual health experts, podiatrists, dieticians, hepatitis C nurses, and diabetes specialists. Much of their work is done in the community, providing additional services to augment skill gaps amongst general practitioners.

"Our staff, particularly our medical staff, travel frequently," explains Vickers. "When they do, it's imperative that they're able to stay in contact with us. They also need to be able to check emails and calendars, share and capture information, and reach out to colleagues for consultations. Smartphones are absolutely critical to their work."

Primarily, remote staff use their devices for email and calendar. Recently, Vickers and his team began exploring the implementation of a new patient management system accessible via a secure browser. This would allow clinicians remote access to patient files, and greatly increase the quality of care.

Before it could do so, however, Tū Ora Compass Health knew it would need to update its mobile infrastructure. An aging, disparate device fleet and a lack of endpoint management software represented more than just a barrier for new initiatives. It was a potential security risk, and a drain on man-hours for IT staff.

"At the time, we couldn't really enforce a unified device policy," recalls Tristan Santer, Service Deck Team Lead, Tū Ora Compass Health. "We could make recommendations, but it was up to the end user to configure things. We also managed our mobile fleet entirely by hand, manually walking each user through setup and configuration. It made deploying new devices incredibly difficult."

In Search of Better Mobility Management

Vickers and his team knew they needed a platform that would allow them better control over and visibility into Tū Ora Compass Health's fleet of mobile devices.

First and foremost, remote device configuration and tracking were a must. This would allow the organisation to seamlessly update its mobile device fleet as-needed, remotely wipe devices in the event that they were lost or stolen, and remotely update devices to keep them secure. Additionally, it would ensure staff were using smartphones for their intended purposes, and not using too much data.

"Coverage can be an issue, particularly in rural areas such as Wairarapa," notes Vickers. "Since our content plan is fairly limited in terms of mobile data allocation, we need to ensure people are using the devices for their intended purposes and not using too much data in the process."

Fine control over device features was also a must, as the organisation identified password enforcement as critical for device security. Since Tū Ora Compass Health's smartphones are personally-enabled, the capacity to keep work and personal data separated through containerisation was also essential. Finally, the solution had to be intuitive – both for IT and for end users.

"What we needed was a corporate endpoint management solution that would allow us to secure devices and data, guarantee management of and visibility into our assets, and standardise our mobile fleet," says Vickers.

To assist in its evaluation, Tū Ora Compass Health approached its telecommunications provider, which recommended VMware Airwatch® over BlackBerry® Unified Endpoint Management (UEM). For Vickers, however, it was a simple decision.

"BlackBerry UEM was a wise investment for us. We have an enterprise-grade fleet that's much easier to manage and secure, better-defined policies and processes, and a more uniform update process. Thanks to BlackBerry UEM, I can stand confidently in front of my board and executive team and say that our mobile assets are protected."

Alistair Vickers
CISO/CPO,
Tū Ora Compass Health

"I have known of BlackBerry for several years now," he explains. "I felt it was the best solution for us. I've seen their solutions in action, and I am very comfortable with their software. BlackBerry also indicated during the selection process that it was willing to work with Tū Ora Compass Health to ensure our deployment was a success – that their solution charges per user rather than per device was important as well."

Visibility. Ease. Control.

A complete endpoint management and policy control solution for diverse and growing fleets of devices and apps, BlackBerry UEM securely enables the Internet of Things, allowing businesses to easily manage endpoints either on-premises or in the cloud. It provides a single, integrated view of the users, devices, apps, and policies, with comprehensive support for a wide range of endpoints and platforms. More importantly, it scales to a business's needs, with the ability to quickly ramp up deployments while still controlling IT costs. Working with BlackBerry, Tū Ora Compass Health rolled out the solution in a matter of weeks.

Thanks to BlackBerry UEM, Tū Ora Compass Health can now track and secure all assets internally, from healthcare data to corporate documents. The capacity to remotely track and wipe devices provides additional peace of mind, and containerisation prevents the exfiltration of sensitive data, whether accidental or intentional. Firmware and software updates can be pushed remotely to all users, and IT is able to quickly identify any devices that are non-compliant.

Security aside, BlackBerry UEM has also allowed Tū Ora Compass Health to easily update its device fleet. The organisation recently purchased and deployed over 100 enterprise-grade Samsung devices. According to Santer, the deployment process was completely seamless.

"With BlackBerry UEM, we can simply push out the settings we need to apply," he explains. "We just send the user their phone, they run through some basic instructions, and they're good to go. It's helped immensely in updating Tū Ora Compass Health's mobile fleet, and BlackBerry UEM's self-service portal has taken a lot of strain off of IT in terms of device support."

Perhaps most importantly, BlackBerry UEM has been painless from an end-user perspective, as well – for clinicians, it's business as usual, and they can continue to focus on providing exceptional patient outcomes.

"People here are very good at picking up on changes that negatively impact them, and they aren't shy about providing me with feedback," says Santer. "No one has complained about BlackBerry UEM, which means it's a seamless transition. It hasn't impacted the day-to-day of our end users."

Along The Road To Digital Transformation

For the immediate future, Vickers is in the process of setting up an internal service desk team, which will use the BlackBerry UEM console for a real-time view of all mobile assets. Previously, Tū Ora Compass Health was reliant upon a third-party provider for this oversight. Shifting this internally will allow for better asset management, and even more fine-tuned security.

Vickers and his team are also working with the local District Health Board to see how Tū Ora Compass Health might use the BlackBerry® AtHoc® crisis communication platform. As the largest primary healthcare provider in the region, Tū Ora Compass Health is responsible for mobilisation in the event of a significant crisis such as an earthquake – BlackBerry AtHoc could be invaluable in helping it achieve this.

"Whatever the next step in our digital journey, it will involve BlackBerry," says Vickers. "I've been very impressed with the level of detail and commitment BlackBerry has displayed towards us, and I have full confidence in their ability to help us stay secure and compliant."

[1] https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#502080cf50cf

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit www.BlackBerry.com and follow @BlackBerry.