Unlocking the power and potential of data-enabled healthcare

pwc

For decades, scientific observations and medical data have been the basis of clinical decision making. Now, with the advent of Virtual Health and other emerging technologies we can extract ever-greater volumes of data and gain ever-greater insights from such data to enhance decision-making and improve patient outcomes. To capitalise on this opportunity, progressive health leaders are now focusing on how data is captured, secured, analysed, and shared to deliver the data-enabled healthcare of the future.

Over the past two years, the proliferation and uptake of virtual health services in Australia has been extraordinary. New health delivery models have been implemented at lightning speed to navigate through the immediate challenges of the COVID-19 pandemic. Rather than striving for perfection, health leaders and their teams have leapt into action to meet clear and urgent community needs. For many patients, these delivery models have been life-changing (and, for many, lifesaving).

Informed by the lessons of the past two years, health leaders and clinicians can now establish permanent, more sustainable models of virtual (and non-virtual) care that achieve better data-enabled outcomes for patients over time.

This isn't about throwing out the traditional ways of treating patients and only adopting new virtually-enabled approaches; it's more about enhancing traditional delivery with newer patient-led hybrid ones to achieve balance across the models of care.

This is a rare window of opportunity, and the key to unlocking it can be summed up in one word: Data

Health interactions generate substantial quantities of high-quality, secure data that can be captured, retained, analysed, and shared. When harnessed well, this data increases the capability of clinicians to make reliable observations and evidence-based decisions that achieve better patient outcomes (in virtual and traditional settings alike).

However, many health institutions currently lack sufficient systems and processes to manage this data. This exposes organisations, clinicians and patients to unnecessary risks and missed opportunities.

The long-lasting rewards of managing data effectively

Health organisations that collect, engineer and harness data effectively can elevate the quality of care they provide, building trust and improving the experience for clinicians and patients alike. And the good news is that – with many virtual health channels still in their infancy – now is the ideal time to get the right data foundations in place ahead of the scaling up and scaling out.

The more that health data is captured, aggregated and analysed, the better that patient conditions can be monitored and managed. Ultimately, this can enable faster, better, and earlier clinical decisions that benefit patients, clinicians and administrators. The potential of improved data management could be felt across the health system, including:

Patient outcomes

When interacting with data-enabled health services, patients not only have better experiences (in how they are treated and managed) but – most importantly – they also have better clinical outcomes.

Clinical decision support

Clinicians are better able to determine the risk profile and most effective interventions for each patient based on previous outcomes for thousands of patients with a similar profile (not just in that institution, but potentially across the country or even internationally). This can help identify patients who require early intervention and/or preventative measures and help reduce unwarranted variation.

Operational improvements

By learning from large troves of data, health services can improve the flow of patients through the system. (For example, if recent virtual and/or community care generated data is available to clinicians when a patient presents at a bricks and mortar facility, this can expedite initial interactions and inform decision-making throughout the patient's care journey.)

Frictionless interactions

Improved data practices allow greater sharing of data among different parties on a patient's healthcare journey. Continuity of care makes the experience more consistent and seamless for both patients and clinicians alike.

Improved trust

Effective and secure use of data sends a reassuring message to patients; it tells them that their health provider is listening to them, monitoring their progress, maintaining their privacy, and making evidence-based decisions.

Wider community benefit

Collecting and sharing data can help develop a better understanding of health in the wider population (e.g. for the purposes of research and development).

Peace of mind for health leaders

When you know where all your information assets are – and how they are connected – then you can take every possible measure to protect them and ensure third parties are doing likewise.

Less disruption

Having your data better protected means fewer data compromises and fewer cyber-attacks. This minimises disruption to health services (and minimises the costs of having to urgently scramble to address security breaches).

Expanded accessibility

Secure data analytics, AI and cloud services are not limited by geography. Data-enabled healthcare allows health leaders to reliably and confidently scale up and scale out, delivering services to people who may not otherwise have access by systematically highlighting inequalities.

How to leverage health data

When various different models of care are available (e.g. face-to-face, online video, phone), patients, with the support of their clinical team, should be able to select their preferred channel. People will be much more likely to opt for new healthcare models when the experience is intuitive, trusted and simple.

It is, therefore, vital to put clinicians and patients at the heart of any attempts to improve data. Having a clear view of patient journeys (across multiple health providers) can help identify opportunities to:

Capture data

The aim here is to record accurate, current, trusted data at source – irrespective of whether that source is analogue or digital. This could be both health data as well as health relevant data entered by health providers, administrators, as well as data entered by patients themselves.

Retain data

The aim here is to ingest and store data in a way that is secure and yet also accessible to health providers. To ensure clinicians can maximise its value, data needs to be presented in a simple way that can be easily understood and analysed.

Share data

The value of data can be multiplied when it is shared or integrated with other health providers. Furthermore, if data is accessible to patients themselves, this can empower them to self-regulate their behaviour and be proactive about their treatment and prevention.

Mobilise data

Perhaps most important of all, viewing the above three steps (capture, retention and sharing) as the launchpad to translate data into meaningful information and insights that can be actioned to improve health services and patient outcomes.

To effectively capture, retain, share and mobilise data, health providers need a comprehensive strategy that encompasses:

1. Standards, governance, and interoperability
2. Privacy and security
3. Monitoring and evaluating outcomes

Let's explore each of these strategic priorities, in turn.

1 Standards, governance, and interoperability

With virtual health models still in their nascent stages, now is the perfect time to establish rigorous standards, governance, and interoperability.

In its rawest form, a lot of virtual health data is unstructured. Standardisation allows health organisations to process unstructured data (that is stored in different places and formats) and combine it with structured data for analysis.

To convert unstructured data into meaningful information, healthcare providers also require governance practices to underpin data recording, optimisation, and analysis. Governance should extend across the organisation itself and also encompass data-sharing agreements with third parties. Therefore, governance needs to be flexible enough to adapt data and analytics to different healthcare scenarios.

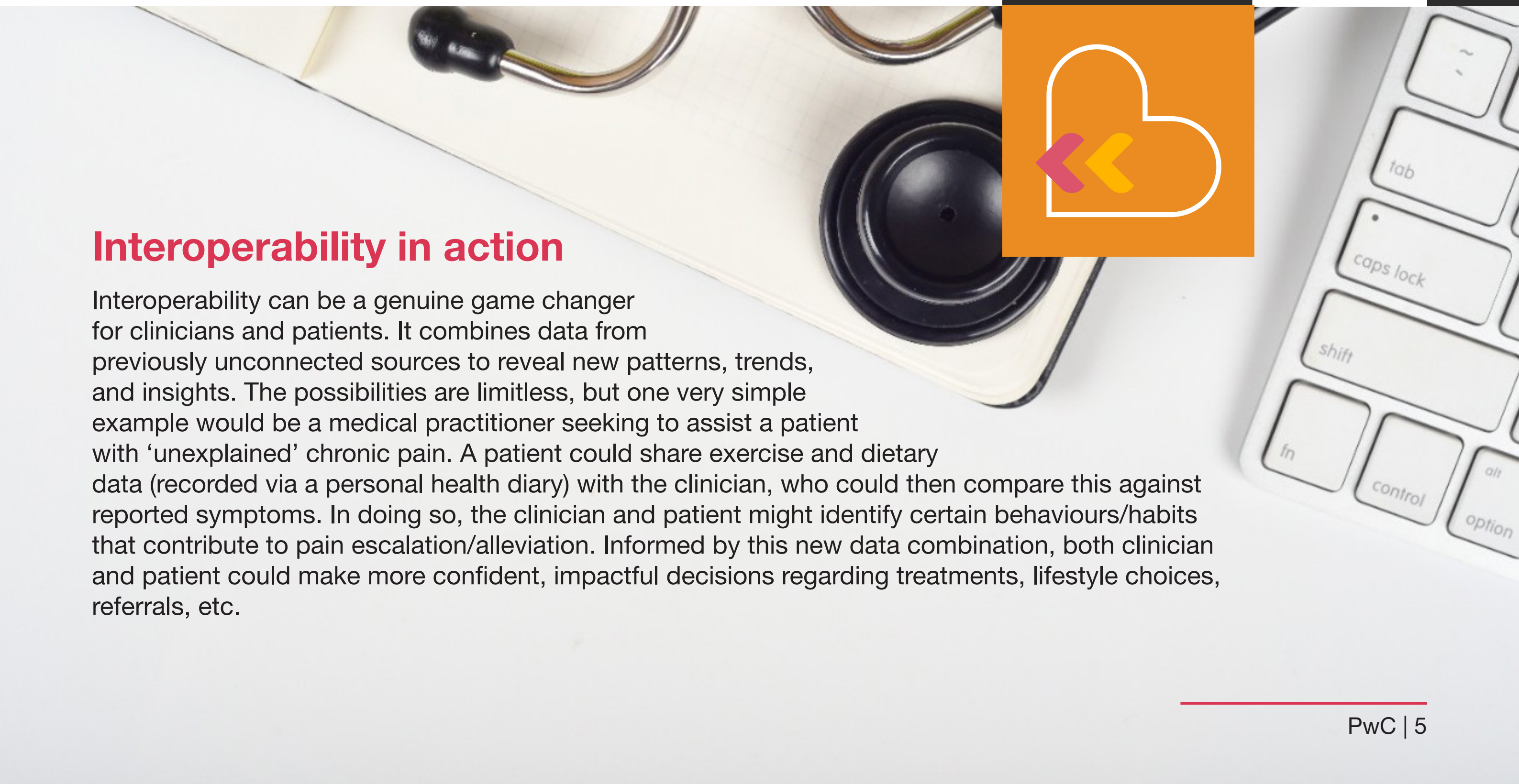
One essential pillar of good data governance is privacy and security. It's important to embed this early in the design phases of new health models, rather than making it an afterthought that is (expensively) retrofitted later on. Mapping entire patient and clinician journeys can help identify where data needs to be exchanged or combined with different parties, and in what format. At each point, security and privacy requirements should be specified.

Another essential pillar of good data governance is interoperability; establishing connections between systems to allow the secure, timely, accurate exchange of data. When this is managed well, health data and health relevant data can be combined from various sources (e.g. virtual health interactions, electronic health records, patient case histories) and activity and lifestyle data (e.g. real-time digital data from sensors, wearable devices and trackers).

To enable interoperability, health organisations should identify silos and barriers to sharing data, and then seek ways to remove these. This can pave the way to adopt digital tools that empower patients to be more proactive about their own health.

There is also the potential for health organisations to go beyond the minimum regulatory requirements of Health Level 7 standards to implement FHIR (Fast Healthcare Interoperability Resource) data interoperability to support risk management strategies and security of data formats. Here, there is an opportunity for health leaders to work with their industry bodies to establish interoperability standards that provide common security and privacy requirements.

For example, natural language processing, information retrieval and machine-learning techniques can convert unstructured free-text data into computable data for AI applications. The Australian e-Health Research Centre is partnering with Queensland Health to extract information from the free-text contents of cancer pathology reports. This allows a real-time cancer registry to process pathology reports daily to provide cancer incidence data to inform activities such as cancer monitoring, health service planning and research.



Interoperability in action

Interoperability can be a genuine game changer for clinicians and patients. It combines data from previously unconnected sources to reveal new patterns, trends, and insights. The possibilities are limitless, but one very simple example would be a medical practitioner seeking to assist a patient with 'unexplained' chronic pain. A patient could share exercise and dietary data (recorded via a personal health diary) with the clinician, who could then compare this against reported symptoms. In doing so, the clinician and patient might identify certain behaviours/habits that contribute to pain escalation/alleviation. Informed by this new data combination, both clinician and patient could make more confident, impactful decisions regarding treatments, lifestyle choices, referrals, etc.

2 Privacy and security

Activating virtual health, in particular the use of remote patient monitoring and asynchronous communication, increases the surface area an organisation must defend from a cybersecurity perspective. It's therefore important to assess whether the organisation's existing technologies and procedures can handle the increased and varied scope of devices and threats.

Assessments should review current data protection policies and security program controls to establish whether they are sufficient to cover the more complex network boundary and architecture brought on by virtual health (not to mention the full 'reach' of data interactions with third parties).

It is important to look ahead and consider the organisation's long-term goals for virtual health expansion. This helps clarify what security and privacy capabilities will be required in future, and therefore what measures should be established now in readiness for this (e.g. data interoperability, tracking and interventions, device integration, cyber threat mitigation).

25%

The 2021 Australian Cyber Security Centre report[1] indicates that the nation's rate of cyber-attacks is increasing and that approximately one quarter are targeted at critical infrastructure providers such as health institutions.

[1] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

Broadly, good security and privacy processes for virtual health include:

- **Security assessments:** Testing the efficacy of the security controls protecting health information (using a variety of tests such as vulnerability assessment, penetration testing, security configuration review, etc).
- **Digital identity:** Establishing the security discipline to enable the right individuals to access the right resources at the right times for the right reasons.
- **Monitoring:** Clarifying the required capabilities to construct, collect, aggregate, and correlate cyber risks and events.

3 Monitoring and evaluating outcomes

The beauty of virtual health models is that – with the right preparation – they can evolve and flex in line with changes in consumer behaviour and clinical results. In this way, service delivery and patient outcomes can continually improve.

To enable this, it's essential to understand how results will be measured. While virtual health is in its (relative) infancy, now is the time to collect baseline outcomes to compare against future outcomes. Longitudinal data can reveal patterns and trends that can inform further improvements.

To determine what data matters most, consider this from the clinicians' perspective: What data could best support their decision-making? And how might findings be presented to clinicians to support their decisions on 'best practice' given a patient's characteristics (e.g. visualisations, dashboards)? It's also important not to overlook the possibility that – if clinicians know certain metrics are being calculated – this might affect their behaviour when recording certain data.

In this design phase, it's vital to closely consult with clinicians. Health professionals understand the basic logic that strong evidence generally delivers stronger outcomes for patients. Similarly, the stronger that data (i.e. evidence) is managed, the better that health leaders can assess best practice and optimise delivery models to achieve higher quality clinical (value-based) care.

Of course, the outcomes of health service delivery extend beyond the immediate experiences of patients and clinicians too. So, in clarifying what data to measure, it's also worth considering how to track economic and social participation, and improved quality of life.

Having clarified what outcomes will be measured, health organisations can establish the methodologies to collect data, calculate metrics, and present outcomes.

Getting started

Introducing a comprehensive data management strategy across an entire organisation, service or sector can be a daunting prospect. But it doesn't have to happen overnight. Often, the best chance of lasting, large-scale success is actually to start small.

Many health leaders begin with a pilot project for data management, where lessons can be learned to inform wider rollouts later on. (For example, a pilot might involve an outpatient virtual service that is data rich and doesn't involve care for critically ill patients.) The guiding philosophy for such pilots should be 'build, test and learn', so that the concepts can be gradually shaped and improved by experience and evidence.

For every organisation, good data management is a journey, not a destination. When it comes to data-enabled healthcare, the important thing is to make a start.

What data security means for patients and clinicians

As we've explored elsewhere in this report, new and improved health models have a greater chance of adoption if they are built around the needs of patients and clinicians. This includes instilling trust and confidence among these users that their data will remain secure.

Health data is private and sensitive. It often contains a combination of personal records, financial information, and government identifiers. So, it's highly sought after by cyber criminals seeking to commit hostile acts like insurance fraud.

Poor data security can also directly impact patient safety and outcomes. Consider the consequences if corrupted data is captured from patient interactions before seeping into physical solutions such as biomedical devices. Or, in the most extreme scenario, imagine how a cyber-attack on a public hospital might hamper clinicians and impact patients in emergency or intensive care wards.

Clinician perspectives

"If there are security breaches in our technologies (e.g. online prescriptions, remote monitoring, etc.) then my patients are less likely to adopt virtual health channels and their trust in me is undermined."

"I need absolute confidence in the data I work with. It needs to be accurate, timely and secure."

"I can see the benefits of virtual health for me and many of my patients, but they are still adjusting to it. Some patients trust these channels, some of them don't."

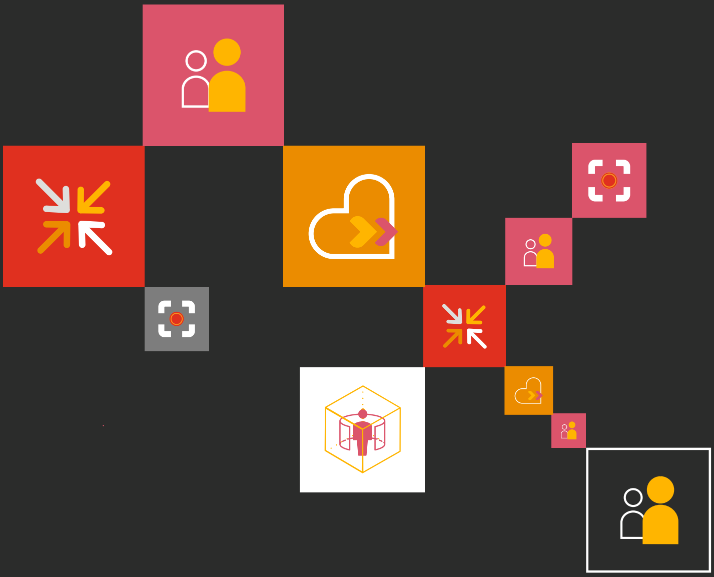
Patient perspectives

"If my credit card gets stolen, I can change my details. If my health information is stolen, then it's compromised forever – I can't change my medical history."

"When I give my personal data to a health organisation, I need to know it will be absolutely secure and that it will be used to benefit my health."

"If my identity data is breached and it's sitting on the dark web, then my trust is permanently undermined in that health organisation."

When establishing data-enabled healthcare, it's vital to anticipate the cybersecurity queries and fears of patients and clinicians, and be proactive about addressing these.



To better understand your organisation's virtual health maturity, complete our Virtual Health Maturity Diagnostic tool self assessment. This assessment enables you to evaluate your organisation's current maturity against nine key dimensions associated with virtual health. By understanding your organisation's current maturity, alongside the vision for virtual health in your organisation, you will gain insight around focus areas for development in future virtual health opportunities.

Get in touch

To discuss how our insights can help your organisation please contact us.

Kevin Sandler
Partner, Consulting, PwC Australia

Tel: +61 411 107 135
Email: kevin.sandler@pwc.com

India Hardy
Partner, Virtual Health Leader, PwC Australia

Tel: +61 424 203 669
Email: india.hardy@pwc.com

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au