Discussion outputs from DIGITAL HEALTH LEADERSHIP SUMMIT, March 2021

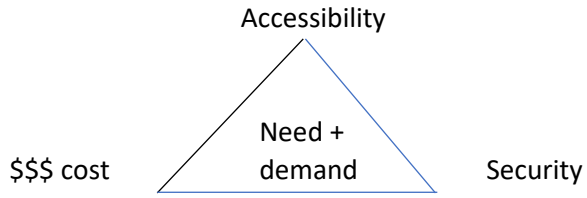
Topic 14: Accessibility vs security of systems: How do we balance the tension in a way that makes sense for clinicians and consumers?

This topic was discussed by groups in Auckland, Wellington and Christchurch.

Auckland delegates' responses

Barriers/challenges	• Business, multiple systems, lack of education on how to properly use the systems
	• Skimp on training on IT projects, i.e., RMOS well
	• Figure it out:
	  ○ Breaches (some inside)
	  ○ Need better things than passwords
	  ○ Password changes every three months/multiple passwords
	  ○ Security becomes a barrier to the job
	  ○ High cost – clinicians pay cost to secure systems
	• Procurement of systems – look for cheapest/compromise security
	• Multiple systems and lack of interoperability
	• Consent:
	  ○ How far can the organisation pass the data?
	  ○ Informed consent
	• Consumers – cyber naïve
	• New systems/applications – need accessibility without too many barriers, i.e., Privacy access assessment and Cloud risk assessment
	• Challenge creating flow from a browser site to other providers
	• App can be a barrier, as how to download
	• Systems must be robust/secure
	• Currently, patients believe GPs etc. own their data
	• Patient information access issues – can be too much, timing needs to be right

	• Ease of access vs. security
	• Patient portal – no multi-factor authentication
	• About risk and what is personally acceptable – informed consent key
	• Accessibility – extra secure but not accessible, i.e., break glass policies – difficult for next of kin to access information
	• Clinicians – also about protecting them
	• Portability needed, i.e., patient portal:
	  ○ App
	  ○ Browser access
	• Difficulties with patients interpreting their own notes, being supported to understand them – improve health literacy

Solutions/ideas	• Consumers:
	  ○ Access via home
	  ○ Multi-factor authentication
	• Technology won't solve the issue
	• User centric access – design in the way people work
	• Think long term, involve iwi
	• Look globally at developed systems – look outside to other systems, i.e., banks
	• Banks work – regulated, Privacy Act, law enforcement
	• Good law enforcement procedures, responsibilities of boards
	• Consumers should have a choice re access to data and where their health information is used
	• Consumers need control of their data – permission to share information
	• Consent from patient re sharing of data at sign-up, i.e., research, services
	• Achievable, need trust, cost high
	• Need and demand:
	 

	• Ability to change consent
	• Patient consent should be required before passing on data
	• Educate:
	  ○ as to why security is needed
	  ○ impact if don't share data, i.e., health programmes, vaccination
	• Tap on and off and sign on – accessibility for technicians
	• Doesn't have to be a tension – remove it – make security that works around people
	• Single sign-on
	• Roadmap for accessibility without barriers
	• Transparency – ability to consumers to access all their information which is held
	• Education/selling to patients what the use of your data means for you and your community
	• Education around what it can mean for your whanau/community
	• Ownership of data and sharing – guidelines would be useful
	• Guidelines needed re use of data - to mitigate the grey areas around the use of primary care data, e.g., historic data that sits outside the DHB (PHOs)
	• Trusted leaders, e.g., COVID app NZ:
	  ○ information stayed on phone
	  ○ trusted
	  ○ Melbourne app – open all the time
	• Accessibility – give patients the choice to share their data with whom they like, easily, i.e., family members
	• Patient information needs to be owned by the patient:
	  ○ Can control who sees what information
	  ○ Need transparency (understand who can see their information)
	  ○ Needs to be choice for whānau accessibility
	• Guidelines around being able to access data
	• Australian health record – opt in /opt out choice
	• Log into system lasting long enough to complete work, entering patient data during patient interaction
	• Patients having choice and deciding who to share information with
	• Assessment case by case – who being used by? Who for?
	• Identity management – actively managed and context appropriate

Christchurch delegates' responses

Goals/observations	• Common understanding of terms • Clinical need = risk management • Consumer need is information I want in a way I understand • Common understanding of terms • Trust in systems/solutions to be used for main needs • Leverage data to make better solutions • Interoperability -joined up information • Co-design with patient centric approach • Patient and clinician collaboration • Built and information security is addressed • Anonymised and aggregated data to drive outcomes • Access along customer journey – right person, right time, right reason • Less siloed information between operators • Health eco-system accessibility (i.e., NGOs) • Practical realisation of health information platform • Single digital identity
Barriers/challenges	• Can we trust the provider accessing the data (scope of practice)? • Can the consumer trust the data security? • Who decides access? • Technical complexity of meeting customised solutions • Difference between what GP writes in notes vs. what they tell them • Encore rates/permissions in systems • Retaining information – to do list (for patients, e.g., intellectual disabilities) • Clinician – early access to complete notes → is it complete? • NEOs – not visible • Consumer access to episode of care

	• Accuracy determined by consumer • Philosophical and cultural problem, not tech problems` • Consumers vs. junior doctor – why can doctor add notes, but not an informed consumer? (Risk – anyone could add notes to their record) • Security is easy compared to privacy • Don't want public seeing private information • Patient expects that their clinician (or advisor) knows their record and no-one else • Visibility of "my" data • Options to modify/inform any profile/data • Owner vs. custodian vs. security guard • Uptake and implementation of a common interoperability standard • "Telling my story over and over and over again" • Time to access data • Problem definition – not a natural tension, need trust – not competing • Trust! • Time for clinicians • Data quality • Consumer driven solutions (apps etc.) • ICT challenges • Who pays for innovation/development/support? • Ethical tension to explore as well • Physical and information security • Consumers are using apps in the Cloud – commoditised → outside of Health Information Privacy Code • Demand for access. Payment to be on secure network MFA • Data lifecycle – cost of archiving/managing data/storage over time • Streamlined security – key deliverable accessibility. Timelines give time back to clinicians. • Who are the customers? They are both clinician and consumer. Need trust • Common needs – if come from consumer perspective, you miss other aspects • Ownership of data

	• Patch protection by providers • Siloed data • Defining the balance security/human error/accessibility • If we can crack it in the health space (personal), can we solve it elsewhere? • How do you minimise human error? Avoid Excel sheet of my information being emailed • Tension between clinicians, e.g., midwife vs. obstetrician • Scenarios for conflict: Custody battles, mental health, insurer incentives, → manage exceptions • Commercial sensitivity of data • Opt out should be allowed – we make it too difficult • Have we created a tension that doesn't naturally exist? • Why is health so difficult? vs. banking? • Avoid front page of the paper for wrong thing • ICT, including passwords, due to number of systems • Fear of practice • Identities auditing organisations and facilities (clinician) • Additional burden of auditing data • Clinicians moving across roles and facilities • What does "Joe Average" expect? • MoH mandatory standards, e.g., digital identity • Tension between accessibility and security, e.g., more access = less secure and vice versa • Security - treat the data with the respect it deserves • Could my information be used to prejudice me?
Solutions/ideas	• Co-design and development • No one size fits all – customised for user needs • Feedback loops to continuous development • Multi-institutional access – circle of care • Education for both clinicians and consumers • Interoperability • Safe identification of consumer

	• Common understanding of terms, accessibility vs. security, privacy vs. consent • New level of mid-tier systems, i.e., not clinical but appointment, continuity of care etc., permissions • Selling points for consumer – you can hold onto it • Dynamic situation, important feedback loops to adapt and change to best serve patient • Recognise importance of non-clinical advisors/navigators, difference between clinical advice and interpreting and actions • Patient is a source of their complete record • Educational framework for consumer support • Granular customised consent matrix • "Gamify" data process to educate and encourage • Awareness – what's in it for me • Uniform platform for systems use • Springboard off compelling event (COVID) – don't go backwards • A "folder about their disease" (a story example) • Co-design to help with balance of tension • Validated identity • Develop solutions for interoperability • Clear statement of patient data ownership • Read only access to data by patient, but add notes available • Exceptions developed outside norm • Teach, don't preach. Need good consent process • Data as competitive advantage • Co-design with whole health network • Outreach – engagement – education • Leverage identity platform (RealMe) • Governance framework defined by Ministry • Ask why not? Start the journey!

Wellington delegates' responses

Barriers/challenges	• Managing data – who has access ?
	• How do we secure data?
	• How is the data used?
	• Where does the data flow?
	• Who owns the data (patient, GP, DHBs)?
	• nHIP:
	  ○ Manager
	  ○ My Health
	  ○ Old fashioned
	• Wearable health and wellness data intersecting:
	  ○ PHI
	  ○ (FHIR)
	• Slack/Xero/ASB Banking/Tracer App/Cloud tools
	  ○ SNOMED – clinical and general/common language
	  ○ Interoperability between systems – tensions sharing records between systems
	• Balance of governance and accessibility
	• Mechanisms of consent
	• Data is not neutral
	• Marketing vs. consumer led
	• Development opportunities mindset – 'not tensions'
	• Clinicians' stewards' patient data – upskilling
	• Consumer responsibility
	• Access control
	• Wearable vs. DHI
	• Complexity of consent systems
	• Inconsistent practices
	• Maintain trust
	• Consumer expectations

	• Legacy technology vs. new stuff
	• Information overload
	• What does good look like – Slack, Xero, ASB Banking App/COVID Tracer App
	• How long would data be kept?
	• Consumer interpretation of clinical data:
	  ○ Translation
	  ○ Ongoing education
	• Does state override consumer data if safety concerns?
	• Fear of commercialisation of data
	• Where is the data kept?
	• Tension with legislation/unions and management and reporting

Solutions/ideas	• GP is the primary contact
	• Security and governance/ethics
	  ○ Ability for consumer to make notes to provide updates re wellness
	  ○ Access control – all/portion
	• Mechanism of consent
	• Mapping the patient journey
	• Open up secure data access:
	  ○ API
	  ○ Digital identity
	• Social license – needs to be earned
	• Education
	• Co-design
	• Clinician centred care
	• Patient centred care
	• Police/MOJ – checks
	• Security must be job zero
	• Synthetic data sets for testing new apps/research
	• Test data sets
	• Labs, MVP development

	• Ask consumers – access and security – trade-offs:
	  ○ Decisions – value
	  ○ Benefits
	• Research in healthcare technology
	• Relationships – consumer and provider – human interaction ↑ trust
	• Delegation of access – whanau – audit processes
	• Considerations of sensitive information
	• Including chat bots
	• UX and UI
	• Ongoing education
	• Focus on health – accessibility to start
	• Consumers must have options
	• Digital health passport
	• Option to see who accesses My Health data – choice. Only people who are involved in my health centre