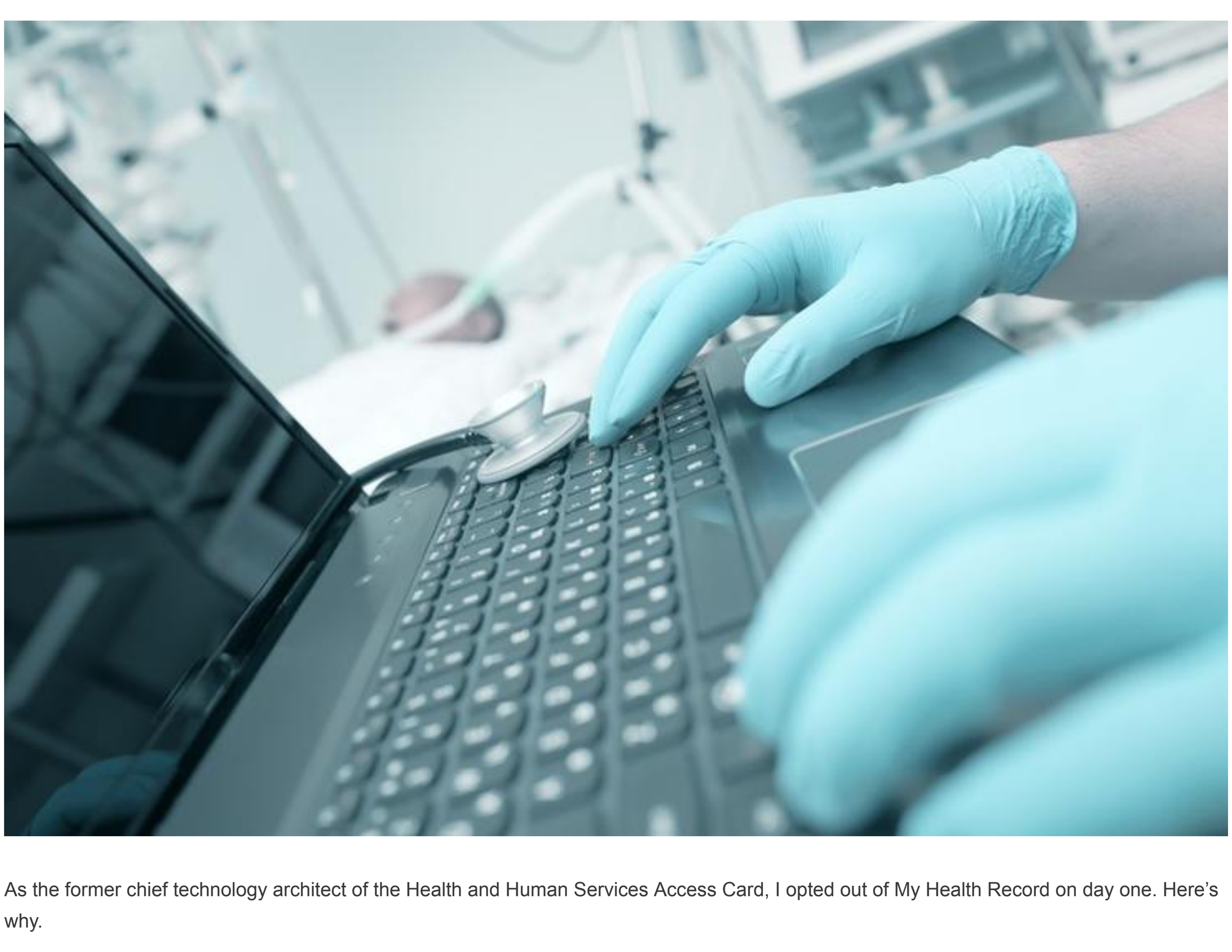
Why My Health Record is flawed

A politically-designed or influenced centralised database with widespread access is problematic

Marie Johnson (CIO)
21 August, 2018 11:49



As the former chief technology architect of the Health and Human Services Access Card, I opted out of My Health Record on day one. Here's why.

The politically designed or influenced model of a centralised database with widespread access at the edge is deeply flawed. This was the Access Card model and it's being done again with My Health Record.

Everything else that flows from that defective model is problematic and unresolvable: legislation; operational performance; privacy; security; informed consumer choice; and highly contested value proposition.

Politically driven or influenced design – in any domain - usually always ends in failure or compromised outcomes. Access Card was terminated on political grounds, notwithstanding alternative architecture models presented and some of which have now been implemented elsewhere.

And for all those who will be horrified, and argue that I am not an advocate of e-health, quite the contrary. Kudos to the many great hospitals, medical practices and health entrepreneurs with foresight who are innovating and digitising their services. The centralised My Health Record approach is not a precondition for this to occur and this innovative transformation work should continue and accelerate.

What I am advocating, is a complete redesign of the model. The current My Health Record model is not just of questionable value but I believe potentially dangerous – and that is why my husband (with chronic and life threatening health conditions and disability) and I opted out on the first day.

Last December, we co-authored an extensive account from a consumer and innovation perspective which discussed the flaws of the government's approach to e-health.

With this Access Card perspective, which I believe is somewhat unique, I further add my voice to the recent comments of other expert commentators. Former privacy commissioner Malcolm Crompton warned of the dangers six years ago. The Australian Privacy Foundation's Dr Bernard Robertson-Dunn considers that the biggest privacy risk to your My Health Record is the government.

From the medical profession, Dr Kerryn Phelps has expressed her concern about the far reaching potential implications and the need for a Senate inquiry. Dr Ruth Armstrong explains why the greatest risk of My Health Record is that the risks themselves are poorly understood and asks if we should be asking doctors how familiar they are with cyber security. In my view, there is a liability risk.

And from a surgeon, Dr Neela Janakiramanan, who has written a detailed account of her concerns about the My Health Record that go way beyond privacy. The surgeon shares a comprehensive analysis of what's at stake – and why youth and women in particular are at risk.

All these concerns were encountered during the Access Card project. The issue is not a resistance by the health profession to e-health; the fundamental issue is the centralised database model controlled by government and from which all other issues flow.

Centralised database and broad access at the edge

The analysis of the My Health Record risks and issues starts with an understanding of the model – side-by-side with the Access Card.

The Access Card and My Health Record effectively are of the same model – a centralised database controlled by government with access by consumers, health professionals and law enforcement. The (then) Howard Government's own Access Card Consumer and Privacy Taskforce headed by Professor Allan Fels, made a dissenting submission to a Senate Committee of this model and the limited protections.

Legislation

Legislation cannot tie the hands of a future government, and this was one of the issues encountered in the Access Card program. One of the deep problems with the Access Card draft legislation – in an attempt to give assurances and protections – was that it stated that the Access Card was not an 'identity card' and further, put into the legislation, the design and architecture of the Access Card chip and the Access Card system.

Feedback through the consultation was strong given the centralised database model: this did not provide sufficient protections and there was great concern that a future government would change this.

In any case, legislation should not define design (effectively legislate design) because this locks in design and technology obsolescence and makes it very difficult for a system to remain resilient and adaptive.

In the same way, any legislative provisions of the My Health Record are insufficient as these can be changed by any future government (or even the current government). The ab initio problem is the centralised database and wide access at the edge model.

Opt-in, opt out or compulsion

Governments use various techniques to encourage participation and the overriding consideration in a democracy is enabling informed choice by the citizen. We are compelled to pay tax. There was a period in the 1960s and 1970s where Australian males were compulsorily conscripted for military service. People can resist compulsion but there are consequences and people need to be informed of these consequences.

The Access Card was described as opt-in as a pre-condition for a person to be able to receive health and human services benefits. A person could choose not to opt-in, but they wouldn't be able to receive benefits, including health benefits.

Commentators at the time described this as in effect a compulsory regime and that many people, including the disadvantaged and vulnerable, would be pressured into opting-in or would opt-in by default without making or being able to make an informed choice about doing so.

So opting-in or opting-out - or not - is a highly contextual decision requiring information to avoid inadvertent decisions by default.

In the case of the My Health Record, being in an informed position to opt-out even further discriminates against the disadvantaged. Not opting-out means that many people are caught by default, silently captured into participation without informed choice and consent.

This raises potential human rights questions in relation to people with disability, indigenous and the vulnerable - as to whether information provided (or not) impacted the ability of disadvantaged groups to make an informed choice.

Further contributing to the confusion about the My Health Record is the timeframe for opting-out – and the consequences if a person does not opt-out within the opt-out window, thereby being "in", but later chooses to opt-out.

Legislative change to extend the opt-out window does not resolve this situation. The 'centralised database and wide access at the edge model' is the problem and all other problems flow from this. Most people do not understand or are even aware of the complexity or personal consequences of this model.

Healthcare scenarios and use cases

The Access Card encountered all same use cases and scenarios as My Health Record is facing: ambulance paramedics, hospital emergency, moving between doctors, diagnosis support, access by minors, complex family situations, the homeless, people with disability, people being able to add additional information, and so on.

It is now more than 10 years since the cessation of the Access Card and none of the complexity around these use cases has been resolved. And this is because the root cause problem is the centralised database and wide access at the edge model.

Before going into some of the privacy and security questions – which other commentators have covered very well – it is worth thinking about the practical operational health delivery implications of reliance on a system based on this model.

Practical operational considerations

During the Access Card program, all the scenarios listed above were also examined from a business process and operational systems performance perspective and the practical implications of these in health delivery.

Detailed in situ business process modelling was done and strong feedback was given by health professionals and practice operators as to the difference between theoretical use cases, however well planned and detailed, and the human experience reality of health service delivery.

It is assumed that the My Health Record program has undertaken similar detailed scenario modelling and business process mapping.

For example, take the use case of a pharmacy transaction involving the presentation of the Access Card: the systems response time between the terminal in the pharmacy to the central Access Card system; the impact on customer service; queues and wait times due to additional processes involved. Also consider the fall back processes due to Access Card system unavailability; pharmacy staff training and so on.

All this presented the prospect of a direct and considerable cost impact on the pharmacy operations.

Similarly, for medical practices, including for example, additional processes for doctors and the time impact in the consulting room, use and access by practice managers and admin staff. Similar mapping was done for emergency situations.

Every second or sub-second (if possible) Access Card system response time in every interaction would have added to costs, imposed additional administration and processes in the consulting room, impacted consumer wait times and critical decision making time.

From a scale and operational performance perspective, with a centralised database and wide access at the edge model, there would be very real challenges in safeguarding the uptime and reliability essential for a nationwide real time system to sustain health service delivery operations.

READ MORE
New thinking required for national disability technology

One might think about air traffic control systems although the difference being air traffic control is a highly regulated and highly redundant network. The My Health Record model however is not a network. The fact that the My Health Record website went down on the first day of the opt-out period, a simple transaction, indicates a critical under-estimation of risk in operational performance.

Privacy

The Senate Committee into the Access Card legislation stated that the program ultimately faced insurmountable challenges in relation to privacy and concerns over function creep.

More extensive than the Access Card data holdings, the My Health Record centralised database will grow to contain potentially the entire Australian population – adult and minors – not basic information, but health records.

The UK care.data program, the controversial NHS initiative to store all patient data on a single database – equivalent to the Australian My Health Record program – was suspended in 2016 by the UK Government following a review into concerns over privacy, the lack of informed consent, and the sharing of medical data with analytics firms.

Similarly, the UK National Identity Card was abolished in 2010 by the UK Government over concerns about privacy and function creep.

The strategic architecture of the UK National Identity Card and the Australian Health and Human Services Access Card was broadly equivalent, including the "voluntary" nature of both: anyone who applied for UK ID card had their personal details automatically logged on to the UK national identity register.

These four national centralised programs – the Australian My Health Record; the Australian Health and Human Services Access Card program; the UK care.data; and the UK National Identity Card – are all broadly equivalent models.

They are each models of national centralised databases of populations with wide access at the edge. They all have faltered on privacy grounds; purpose; confused and default consent models; concerns about security; and concerns about function creep.

Security

There has been strong commentary and concerns about the security of the My Health Record with the program now referred to a Senate inquiry. My Health Record and the Access Card have the same cyber security challenges – the difference is that these issues are exponentially greater now than they were 10 years ago.

And this will always be the case with this centralised database model. The cyber security challenges that will arise during the coming decade are almost unimaginable, particularly if the government persists with this current model.

Former Pentagon cyber chief, Jonathan Reiber said hackers could exploit My Health Record flaws.

What has been learned from the experience of the Access Card, from the abandoned UK care.data, and the abandoned UK Identity Card program? All big centralised database models of population data. Why has this model been adopted again? These are serious questions for the Australian public to have answered.

From my experience as the Access Card chief technology architect, the adoption of this model yet again raises a number of mission critical design issues.

A system is only as resilient as its weakest link. Even if military grade security applies to the centralised database (described by commentators the during Access Card program as a honey pot), securing access at the edge involving some 900,000 individuals in a great variety of environments, is a far greater almost impossible challenge.

The design compromise and risk of the weakest link factor really needs to be understood. It is worth reading the case study of the Space Shuttle Challenger disaster and there are indeed a great many lessons to be drawn from this ranging from governance to risk and decision making involving complex systems.

Two lessons in particular apply for the weakest link risk issue.

Firstly, in the Challenger case, design and manufacture was heavily shaped by political influence and this resulted in the need for O-rings joining sections of the rocket boosters. The O-ring design feature was the weakest link.

The second issue was decision makers ignoring technical advice regarding risk. The night before the Challenger launch, the engineers provided advice to NASA management that the forecast temperature in the morning was for ice and too cold for launch: this would almost certainly cause O-ring failure.

READ MORE
Disability system to tap IBM's Watson

The advice was over-ridden by NASA management which proceeded to launch, resulting in the catastrophic loss of the Space Shuttle and crew.

The Space Shuttle program was suspended while a review and redesign of the Space Shuttle was undertaken. And this is what I'm advocating for the My Health Record.

The weakest link in the My Health Record model is in fact many: each one of the 900,000 users many times a day in a great variety of environments. The My Health Record model creates privacy and security challenges that are practically unresolvable.

Next up: Confused value proposition: What My Health Record is and is not

Page 1 | 2 | next

Tags Marie Johnson
More about Advanced AIIA Apple Australia indeed Microsoft NASA Privacy Foundation Shuttle Technology
0 Comments

Read next
Sydney Trains commences Dwell Track trial to ease crowding, reduce delays
Nicola Dorling leaves digital role at UNSW
CIO50 2022 #4 Richard Taggart, Sydney Local Health District
In pictures: CMOs, CIOs and their role in customer experience
CIO Summit Melbourne 2019

CIO50 2022 #6 Farhoud Salimi, eHealth NSW