Patient privacy: why so polarising?

This is the edited text of Stephen Wilson's column in the iappANZ members bulletin no. 10.

Why is it that privacy is so polarising? For a basic human right that we treasure and guard instinctively the moment we get home every evening, privacy is remarkably dispensable in public discourse and policy.

Technologists have an unfortunate tendency to belittle privacy in words and in deeds. Scott McNally's quip that 'you have no privacy, get over it' usually tops the list of gaffs, yet a more insidious viewpoint was actually revealed by the then-chair of IBM, Lou Gerstner, who in 2000 boldly asserted that "privacy is not a technology issue".

Perhaps Gerstner meant no harm, but his slogan is often read by technologists as a disclaimer that distances them from "business" issues like privacy. Positioning privacy apart like this gives licence to technologists to ignore their own role in privacy, and it exacerbates the difficulty we all face in building privacy into complex systems. I'm often asked by IT project managers 'Why should we be doing a PIA now, when the design hasn't been finalised?', and my answer is 'You should do a PIA early precisely *because* the design isn't finalised!'.

Make no mistake: anyone who asserts that "privacy is dead" is trying to sell you something, whether it's a national security ideology, or a new pair of runners as you leave the gym, walk by a shoe shop for the fifth time in a week, and your mobile phone announces the presence of an assumed exercise junkie.

But cynicism isn't confined to entrepreneurs. We're in the midst of a late, rushed and therefore rather shallow debate over national health identifiers, where the privacy issues are being played down or underestimated by many e-health proponents.

I engaged with the recent senate inquiry into the Health Identifiers Act.[1] Many advocates of the proposed system maintain that the identifier is "just a number" and that no clinical information is associated with it. But I'm afraid that's just not true. While I am in generally favour of health identifiers, I worry that the identifier proposal before us is indeed privacy invasive, its implications are not thought through, and there aren't any alternative architectures on the table.

Without questioning the claim that the ID is inherently non-clinical, privacy is treated in the legislation and in the debate as simply a governance issue. And those who are still digging deeper into privacy have been characterised as 'hijackers' who are "defending privacy to the exclusion of all thought of benefits to the individual brought about by better healthcare".[2]

But privacy advocates aren't uncaring about e-health, and they don't see privacy and healthcare efficacy as competing with each other.

So dig deeper we must. The proposed Individual Health Identifier (IHI) is designed around a central directory which serves up patient identifiers to any provider authorised to request them. Neither the design nor the legislation contemplate any way for patients to carry and present their identifiers for themselves (and thus the draft law is oddly technology-specific). So here's the problem: each and every time a provider draws down an IHI —which will be routine the first time a patient presents at any clinic—this event will be logged, creating an elaborate track of the individual's journey through the health system. If the IHI service knows that I have attended an emergency room, then a drug & alcohol clinic and finally been admitted to a mental health facility, then a wealth of clinical information is actually being aggregated, personal information that would otherwise remain totally confidential between the providers and me.

The IHI service will also know, for no good reason, every time a rural patient visits a doctor in another town, a teenager sees a doctor who is not their family GP, or a patient seeks a second opinion. The sheer visibility of these intensely personal encounters will inhibit some from seeking the healthcare they desire.

It doesn't have to be this way.

All agree that privacy is a cornerstone of healthcare, so let's not be drawn into the grim myth that efficacy and privacy are at odds, or that privacy is simply a governance issue. Like e-health itself, privacy is complex and subtle, and deserves more collaboration, multiple disciplines, and optimism.

---

[1] http://www.aph.gov.au/Senate/committee/clac_ctte/healthcare_identifier/index.htm.

[2] Dr Mukesh Haikerwal, Sydney Morning Herald, 22 March 2010, http://bit.ly/bS8DBF.