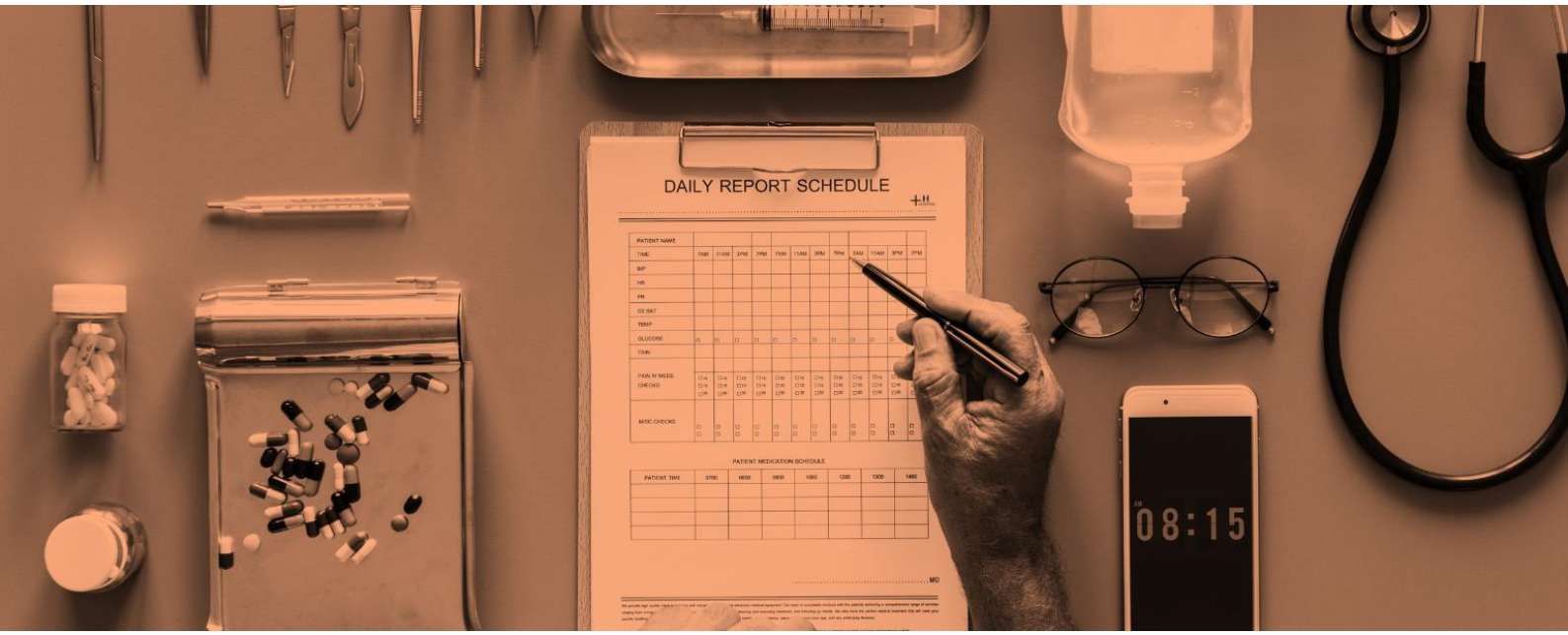
Medical Records Trust & Transparency

The recent HealthEngine Controversy and the troubled launch of the government's My Health Record Opt-out has propelled the Australian Healthcare Industry into the data privacy spotlight.



HIGHLIGHTS

- Medical Records Trust & Transparency
- A Quick Recap
- Lessons Learned and Acting on Them

Data use and an individual's rights have become very topical with the increasing number of data breaches that impact us as individuals, including reports on data issues in the health sector. Take the Facebook/Cambridge Analytica problems as an example.

The Facebook–Cambridge Analytica data scandal was a major political scandal in early 2018 when it was revealed that Cambridge Analytica, a company that had worked on Donald Trump's US presidential election campaign, had harvested the personal data of millions of people's Facebook profiles without their consent and used it for political purposes. It has been described as a watershed moment in the public understanding of personal data and precipitated a massive fall in Facebook's stock price and calls for tighter regulation of tech companies' use of data.

People are rightly concerned about the security of their personal information. Is the information held securely and confidentially? Will it only be used for the purposes for which is was provided and by the people it was provided to? Individuals now raise questions about the safe collection and storage of sensitive personal information. Accordingly, the healthcare industry needs to take a proactive approach when handling patient data.

In this article, we look at the steps that healthcare businesses can take to increase patient trust and handle data transparently. We identify lessons learned from recent digital health information mishaps and outline what healthcare businesses should be doing to avoid suffering a similar fate and risking their reputations.

ARTICLE

Patients are "…more likely to give permission to share their data if they understand how their data will be used".

A Quick Recap

Managed by Australian Digital Health Agency, My Health Record is a digital medical record system that collects and stores the health and pharmaceutical data of every Australian. It aims to give a person access to health records, give a person's health providers access to upload information and then share the data with an individual's healthcare professionals Australia wide. The objective is to improve delivery of health services and reduce over-prescribing and errors. The system has been supported by medical practitioners in the most part, but heavily criticised for its perceived privacy and security inadequacies.

Critics argue that health data that is shared with third parties could be combined with other personal data to identify an individual, even where the health data is anonymised. Individuals with medical conditions, such as HIV and mental health problems, fear that their data may not remain confidential and could be accessed by employers, the police or health insurance providers. To add to the controversy, a My Health Record will be automatically created for each Australian unless you actively opt-out by **31 January 2019**.

HealthEngine, an online clinician appointment booking service, has also been involved in a privacy and security crisis concerning the handling of Australian patient data. HealthEngine requires users to enter details about their medical conditions when making a booking. In June 2018 an **ABC TV exposé** revealed that HealthEngine had used the information collected from patients to provide client leads to personal injury law firms. Those law firms used the data to target individuals and offer legal services to patients who for example had a potential worker's compensation or personal injury claim. HealthEngine customers complained of being contacted by law firms after booking appointments with the service, and HealthEngine argued that customers had consented to receiving the calls.

Lessons Learned and Acting on Them

To better understand what the healthcare industry should be doing in terms of privacy and data, it is important to note the main lessons learned from My Health Record and Health Engine.

1. ***We need transparency***

Data breaches have dominated the news in recent months. What we have learned from these examples is that there is a disconnect between businesses complying with their legal privacy obligations on the one hand, and what individuals expect businesses to do with their data on the other. Even where businesses have complied with their privacy requirements, often consumers are still left in the dark about what exactly happens to their data.

To reconcile this disconnect, businesses need to be more transparent about their data handling practices. Transparency ensures businesses are clear about their practices and aligned with customer expectations.

Generally, businesses seek consent for their data handling practices in lengthy terms and conditions and promise to handle data in accordance with **unreadable privacy policies** and statements.

This is despite the fact that most consumers do not read terms and conditions. A **report by the Consumer Policy Research Centre** released in May 2018 revealed that only 6% of Australians read the privacy policies and terms and conditions for the products or services that they signed up to in the past 12 months. The current method of consent to data handling through terms and conditions alone is ineffective.

While businesses may think they are being transparent about their data

Level 2, 117 Clarence Street, Sydney NSW 2000 Australia | +61(0) 2 9660 9630
lawyers@saintylaw.com.au | www.saintylaw.com.au

"...forcing people to choose when they don't want to... is offensive to their dignity because it requires them to devote their attention to something to which, on reflection, they don't want to devote their attention"

practices, consumers are often astounded at how their data is being handled because of complex terms and conditions that are not easily understandable.

HealthEngine is just one example of classic and legally correct corporate compliance leading to poor press. The HealthEngine data collection statement on their Website stated that all users were required to accept their terms in order to use the HealthEngine booking service. HealthEngine also revealed in those terms that they disclosed data to health insurance brokers, lawyers and finance providers for dental and cosmetic procedures. Though HealthEngine had seemingly met their privacy requirements in seeking consent, the public outcry about them sharing patient data with personal injury law firms makes it clear that consumer expectations were not met. Users' expectations were not consistent with their corporate data use.

HealthEngine said that consent was not hidden in its Terms and Conditions. They highlighted the consent with a pop-up form in the App. *"The referrals do not occur without the express consent of the user,"* the company's CEO, Dr Marcus Tan, said. But there was still an outcry from some consumers.

HealthEngine may be changing its practices. In an updated statement after publication of the ABC article in June 2018, Dr Tan said *"HealthEngine has no referral arrangements in place with marketing agencies or law firms. Our referral partnerships remain constantly under review to ensure patient feedback is taken on board and patients are getting access to the services they request."*

To mitigate the risk of failing to meet consumer expectations, healthcare businesses need to be upfront and clear about how they handle patient data. If businesses wish to seek consent in their terms and conditions, the terms should be simplified. The Consumer's Health Forum has stated that patients are *"...more likely to give permission to share their data if they understand how their data will be used"*.

The location of these terms and conditions is also important. Having a statement that is hard to access or one that is only available upon request is not sufficiently transparent.

Companies that wish to further assist consumers' understanding, especially for younger individuals or those that are unable to read, could even consider creating "explainer videos" to detail specifically how patient data is handled.

HealthEngine highlighted their consent via a pop up. It was clear and obvious. Many users were still not happy to accept but did so to be able to use the service. Transparency is not the answer to everything.

2. ***Ensure your customer is spoilt for choice***

Maintaining consumer satisfaction is essential for businesses. Public approval for a product or service is compromised when customers feel manipulated or deceived. Former U.S. White House Administrator of Information and Regulatory Affairs, Cass Sunstein, said, *"...forcing people to choose when they don't want to...is offensive to their dignity because it requires them to devote their attention to something to which, on reflection, they don't want to devote their attention"*.

This seems to be the case for My Health Record, a system experiencing backlash from the Australian public. Australians must make the effort to opt-out to prevent an automatic record from being produced. The opt-in approach taken over the last five years did not generated sufficient take-up. The health benefits from the

It is your responsibility to keep track of information you collected and to ensure that your customers have the full protection at law from mishandling or wrongful collection of information.

system was seen by the Australian Government as a superior need and societal cost saving. But by implementing an **opt-out mechanism**, users feel that they have been stripped of free will. That are also distrusting of the uses and who can access the data now and in the future.

In the recent Senate hearings, medical experts and unions raised serious concerns. The Australian Digital Health Agency is making moves to accommodate these. The Health Minister, Greg Hunt, is 'tweaking' the legislation. Data was going to be stored for 30 years after a person's death. Now users can permanently delete their records. Police must now get a court order to access records. Australians, 14 years or older, can have control of their records and nominate who can view them. An individual can choose to receive notifications if their data is accessed. Recently, Federal Labor called for a rewrite of the controversial legislation to prevent insurers and employers from exploiting patient data and to protect domestic violence survivors.

Former AMA president, Dr Kerryn Phelps, who ran as an independent in the Wentworth by-election, told the Senate committee it was not enough to stop third parties, such as insurers, from accessing My Health Record data, but that consumer protections were needed to prevent third parties from discriminating against individuals who do not agree to the release of their My Health Record data. She also called for strict privacy laws to be introduced, along the lines of the EU General Data Protection Regulation, to circumvent misuse of the information, warning that there were currently no protections to stop data being "leveraged for financial gain".

Around **1.15 million Australians have opted out** of My Health Record.

Healthcare businesses need to ensure the consumers are 'on their side' by giving patients the ability to have their say how their data is handled. They need to build consumer trust. Consumers that do not trust the system are typically less inclined to share their data with the business, claims Justin Warren, Board Member of digital rights organisation, Electronic Frontiers Australia. Patients that feel manipulated into sharing their data are unlikely to recommend the system to others.

Businesses in the healthcare industry should therefore provide users with the opportunity to actively opt-in or opt-out without being restricted by timeframes or the threat of limited access to services. Ideally, as recommended by the recent review into Open Banking, businesses should succinctly and plainly summarise all the possible uses and disclosures of an individual's data so that users can individually select their preferences.

3. ***Keep track of the information you collect***

It is your responsibility to keep track of information you collect and to ensure that your customers have the full protection at law to prevent mishandling or wrongful collection of information. Ask yourself:

- What information are we collecting about our patients?
- How do we intend to use that information?
- What information of our patients might we share with others and what will they do with it?
- What information and choices are we giving our patients about personal information we collect?

Present your answers to these questions in a clear and unambiguous statement so that customers understand what will happen to their personal information. For instance, if you are sharing their information with technology providers who provide you services, your customers need to know.

Level 2, 117 Clarence Street, Sydney NSW 2000 Australia | +61(0) 2 9660 9630
lawyers@saintylaw.com.au | www.saintylaw.com.au

4. ***Don't fail to manage expectations***
Ignore the lessons learned at your peril. Consumers are more educated and demanding. A continued lack of corporate transparency means data practices and consumer expectations will clash, regardless of whether any privacy laws are broken. When consumers lose trust, they go elsewhere for their services. Businesses could not only suffer customer disappointment but also risk a scandal and reputational damage.

Businesses in the healthcare industry should be leaping at the chance to improve the security and privacy of their digital health data handling and communication of those practices. Prove to customers that you can be trusted to handle sensitive customer data and you will engender loyalty.

5. ***Help consumers help themselves***
If businesses tell consumers how their data is being used and who they may be sharing information with, then consumers can be prepared. Consumers take note of data breach news. They will be more aware of what is a real email from a service provider. If they know the uses of their data they will be more vigilant to prevent misuse.

Consumer satisfaction is a key component of business success. Earning trust and loyalty while maintaining transparency and improving data handling practices will strengthen business success in the healthcare industry.

KATHERINE SAINTY
is the founder of Sainty Law, a corporate and commercial lawyer and expert in digital, privacy, technology and media law. Katherine specialises in complex technology and data transactions advising clients across all aspects of their businesses, from back-end system change to the use of technology and data to transform interaction with customers and protect and grow their businesses.

Contact us for advice on your privacy and health records data strategy.

Level 2, 117 Clarence Street, Sydney NSW 2000 Australia | +61(0) 2 9660 9630
lawyers@saintylaw.com.au | www.saintylaw.com.au