FINANCIAL REVIEW

‘Terrible mistake’ could send execs to jail over vaccine certificates

John Davdison
October 19, 2021

Collecting COVID-19 vaccination certificates from customers or employees poses a serious legal and cyber security risk to businesses that exposes them to lawsuits, hefty fines and even executive jail sentences if the data isn’t handled properly, experts warn.

The risk is so grave that businesses that have already stored images of government-issued vaccination certificates from employees or customers are advised to scour their email or human resource systems and delete the images, or at the very least remove a sensitive piece of information prominent on the certificate that exposes businesses to a “world of data security pain”, one expert says.

Australian Government

COVID-19 digital certificate

This individual has received all required COVID-19 vaccinations.

Name

JOE BLOGGS

Date of birth

01 Jan 2000

Document number

1234 1234 1234

Valid from

05 Aug 2021

Vaccinations

Dates received

AstraZeneca Vaxzevria

27 May 2021, 05 Aug 2021

Disclaimer

This certificate shows your COVID-19 vaccination details as reported to the Australian Immunisation Register by your vaccination provider. It is available because you have received all required COVID-19 vaccinations. The valid from date reflects the date from which you received all required COVID-19 vaccinations.

Every effort is made to ensure that the information contained on the Australian Immunisation Register is correct. The data is based on information provided by vaccination providers and the accuracy of data is dependent on the quality and timeliness of information provided.

Australia’s vaccination certificate has a piece of data experts warn shouldn’t be there.

As part of state and federal requirements for emerging out of the pandemic lockdown, businesses are asked to check whether customers and employees are vaccinated before allowing them to enter their premises.

Businesses storing information about whether someone has been vaccinated are therefore storing health information, quite possibly for the first time, exposing them to the Privacy Act, which requires they take “reasonable steps” to secure that information, said Anna Johnston, a former NSW deputy privacy commissioner who runs her own data privacy consultancy, Salinger Privacy.

Worse than that, the federal government certificates contain a unique identifier, known as the Individual Health Identifier (IHI), that is covered by its own law, with much stricter data security requirements and with punishments that could include jail if that one piece of data is mishandled, Ms Johnston told *The Australian Financial Review*.

Together with the Tax File Number, the IHI is the most sensitive piece of data used by government, she said. It uniquely identifies Australians for healthcare purposes, far more so than a Medicare number, which can be shared by family members. It’s so sensitive that, when it was brought in 2010, it came with its own privacy legislation, the Healthcare Identifiers Act.

“Including the IHI on the vaccination certificate, which is a document“I really feel for small businesses in particular. They don’t have an in-house compliance we’re supposed to be showing to our gyms, hairdressers and restaurants, as well as to our employers and customers, was a terrible mistake by the federal government,” she said.

Scrub IHI from any vaccine certificates you store, advises former deputy privacy commissioner Anna Johnston.

“I really feel for small businesses in particular. They don’t have an in-house compliance officer telling them what to do. They don’t have an information security officer telling them how to secure these records. They probably don’t have the foggiest clue that there are special rules for the use and disclosure of the IHI that, if they breach those rules, expose them to both a civil penalty and a criminal penalty.

“You face up to two years imprisonment for use or disclosure of the IHI for any purposes outside of supporting healthcare. And now that number is on a PDF that is being emailed around willy nilly.”

James Turner, whose company, CISO Lens, runs a forum for chief information security officers (CISOs) in Australia, said handling the vaccination certificate had become a major concern, even for organisations large enough to have a CISO.

“There’s a whole lot of stuff in storing vaccination data that is messy,” he said.

One problem is that a lot of businesses are asking their employees and customers to email in images of their vaccination certificates, showing the IHI.

“As we know from when people store credit card information in email systems, this sort of stuff can leak easily,” he said.

Even chief information officers are concerned about how to store vaccination data, says James Turner, Founder, CISO Lens. Dominic Lorrimer

And even if the business is simply sighting the certificate and ticking a box in a database to say that someone has been vaccinated, that tick box still amounts to storing personal health information, which is a big concern for CISOs because of the added privacy requirements it entails, he said.

One large organisation contacted by the *Financial Review*, Optus, said it was treating its employees' vaccination certificates with great caution, storing it only in the employee's personal profile, where other sensitive data such as remuneration entitlements is already stored.

"This information is only accessible for verification by a handful of HR specialists" and not by an employee's manager or other leaders, an Optus spokesman said.

One of Australia's largest providers of human resources software, Nimbus, said it had gone to pains to ensure that, if an employee was required to upload an image of a vaccination certificate, the image upload was encrypted, and it was stored in the HR database in an encrypted format.

Dealing with the technology and compliance issues raised by the need to store vaccine information "is complex, and unless you've got technology in place to address all these issues, you're going to be scrambling, there's no doubt about that," said Grant Custance, the founder and CEO of Nimbus.

"There's a level of anxiety out there. A lot of businesses have manual HR systems that don't have proper compliance reporting in place, don't have formal policies and procedures in place," he said.

Grant Custance, CEO of Nimbus, says his company encrypts any vaccination certificate it stores in databases.

Even once businesses address the serious compliance issues attached to storing vaccination data about their employees and customers, or even if the government chose to overlook the compliance issues because it created the problem in the first place, there's still another issue they need to worry about, said Salinger Privacy's Ms Johnston.

"The vaccination certificate includes your name, your date of birth, and your IHI. These are the three elements that you need to access someone's Medicare records on the dark web," she said.

Rather than store the certificate, it was much better to simply sight it, possibly over a video call such as Zoom, and then only store information about the date and time it was sighted, and by whom, she said.

If a business has to store the certificate, “they should ask their employees and customers to redact it first.”

“Get them to print it out, get out a big black texta and black out the IHI, and then scan it and send it. As a business, you really want to avoid having any record of someone’s IHI, if you’re not a healthcare provider.

“If you’re not part of the healthcare system, which uses the IHI legitimately, it’s just a whole world of data security pain. If you’re a gym or a hairdresser or an airline, you don’t need the IHI,” she said.

Businesses should also think about how they’re going to destroy any vaccination data they collect, once they no longer need it, the Office of the Australian Information Commissioner says.

“Any vaccination information must be collected and stored securely. Access should be restricted to only those staff in the business who need to see it and it is preferable that this information is stored in a separate record or database to other business information.

“This will assist in restricting access and allow businesses to more easily destroy the information once no longer required,” a spokesman for the Information Commissioner said.

John Davidson is an award-winning columnist, reviewer, and senior writer based in Sydney and in the Digital Life Laboratories, from where he writes about personal technology. *Connect with John on Twitter. Email John at jdavidson@afr.com*