This week it was reported an online medical appointment service, HealthEngine, was sharing patients’ private information with a firm of solicitors specialising in personal injury claims.

As reported, HealthEngine, which boasts 15 million annual users, requested details of the patient’s symptoms and medical conditions as part of their booking process. It then passed this information to law firm Slater and Gordon at an average rate of 200 patients per month. This was called a “referral partnership pilot” program, and operated between March and August of 2017.

HealthEngine denies sharing this information without patient consent, stating consent was provided by way of a “simple pop up”. Despite the company’s best efforts, HealthEngine continues to face queries regarding their treatment of patient information.

On the face of it, it appears several Australian Privacy Principles may have been breached.

Read more: What should Australian companies be doing right now to protect our privacy
Did patients provide informed consent?

HealthEngine assures visitors to their website the collection of information is done strictly by consent, and it has provided disclosures of the use of collected information.

For instance, in its Privacy Policy, HealthEngine notes information may be disclosed to third parties “but only for the purpose of providing goods and services to [HealthEngine]”.

HealthEngine also notes disclosure may be made to:

other persons notified to you at the time we collect your personal information, who you give consent to, or to whom we are authorised or required by law to make such disclosure.

In their “Collection Notice” - one of three policies to which patients must agree, HealthEngine further states it may disclose personal information to “third party providers who may be of interest to the patient”, including health insurance comparison providers, finance companies for credit for cosmetic or dental procedures, and providers of legal services.

This appears to contradict their Privacy Policy, which is itself bound by the Australian Privacy Principles.

Read more: Questions still need answering in Australia's largest health data breach

The Australian Privacy Principles

The Australian Privacy Principles specify requirements regarding how organisations collect and use patient information. These include how and in what circumstances information is shared with third parties. The principles specify all information collected by HealthEngine must be reasonably necessary for the provision of services.

And they must not collect information unless there is consent, the information is necessary for the function of the organisation, or there’s a “permitted health situation”, which means the information must be necessary to provide services to the patient.

Click-wraps and bundled consent

A type of agreement HealthEngine uses to ensure patients using their services agree to the terms and conditions, called the “click-wrap”, involves the patient clicking through the booking process and thereby agreeing to the terms and conditions, links to which are provided.

So the patient is agreeing to three separate sets of agreements (called the “bundled consent”) — the Terms of Use, the Privacy Policy, and the Collection Notice — in the one action. This also means
agreeing to secondary use of patient information and the provision of direct marketing, as found in the Collection Notice.

The privacy principles broadly prohibit direct marketing unless there is informed consent. And they require the patient to be provided with a simple way to opt out of direct marketing. HealthEngine assures patients they’re under “no obligation” to provide their information, though accepting these bundled terms is necessary to complete the booking and there is no option to opt out.

Informed consent requires the individual to be able to have a genuine ability to provide or withhold consent. This means having informed knowledge of the impact of their decision. It’s evident that with contradictory policies, bundled consent, and potentially misleading terms, a patient could not make a truly informed decision of the impact of their choice to use HealthEngine as the provider of this service.

Read more: When data privacy goes missing, will the regulators hear it cry?

Where to from here?

Laws that ought to protect individuals online do exist, but the potential for harm online is neither immediate nor always evident. So, as an immediate recourse to online threats, people need to take greater care with personal information online and ensure they seek recourse when issues arise. This requires being better informed about both the law and and individual’s rights and responsibilities online.

The Australian government also needs to take individual privacy and personal information protection more seriously and crack down on violators.

The establishment of the Office of the eSafety Commissioner was a positive move forward, but effective cuts to funding to the Office of the Australian Information Commissioner has the potential to hinder progress.