GlobalResearch
Center for Research on Globalization

Thriving on Dark Web: The My Health Record and Data Insecurity

By Dr. Binoy Kampmark
Global Research, August 03, 2018

Region: Europe, Oceania
Theme: Intelligence, Police State & Civil Rights

Note to readers: please click the share buttons above

Data is rarely inert. It moves, finds itself diverting, adjusting and adapting to users and distributors. Ultimately, as unspectacular and banal as it might be, data sells, pushing the price in various markets whoever wishes to access it. Medical data, given its abundance, can do very nicely in such domains as the Dark Web. With governments attempting to find the optimum level of storing, monitoring and identifying the medical health of citizens, the issue of security has become pressingly urgent.

Britain's National Health Service is a case in point. Last year, that venerable, perennially criticised body of health provision received the full attention of the WananCry virus. Much of this was occasioned by carelessness: a good number of organisations were running on out-of-date Windows XP software. The principle of insecurity was, however, affirmed.

Last month, the Singaporean government faced the grim reality that 1.5 million health records had been accessed by hackers including, audaciously, the records of Prime Minister Lee Hsien Loong. This well landed blow riled all the more for that state's heralded insistence on the merits of its own cybersecurity. In the words of the government statement,

> "Investigations by the Cyber Security Agency of Singapore (CSA) and the Integrated Health Information System (IHiS) confirmed that this was a deliberate, targeted and well-planned cyberattack."

Lee, in an obvious effort to reassure, perhaps more himself than anybody else, claimed that his data had nothing of value. (If a thief takes your goods, make sure they are worthless.)

> "My medication data is not something I would ordinarily tell people about, but there is nothing alarming in it."

Obtaining medical data enables a stealthy plotting for the attacker, hoarding information clandestinely then deploying it with maximum effect.

> "Patients who have had their medical information stolen," goes Aatif Sulleyman for The Independent, "might not realise it's even happened until the attackers have already set their plans in motion."

Patient profiles can be built, with credentials mustered for reasons of impersonation to obtain health services. Medical equipment and drugs can be duly purchased, and claims with insurers lodged. That prospect is somewhat bleaker than one whose credit card details have been pinched; the bank, at the very least, might be able to put a halt on transactions with immediate effect.

Such excitement turns in anticipation and worried focus to the My Health Record proposition of the Australian government, which, it must be said, belies the usual blissful ignorance about what such an invitation tends to be. Here, information utopia is paraded and extolled: to have such material in one spot, rather than diffused and intangible; to have the picture of one's medical being in one location for those providing health care services.

Australia's political representatives and bureaucrats have assumed a certain cockiness far exceeding health providers in other jurisdictions, making the My Health Record scheme a pinnacle of insecurity in medical care. A pervasive sense exists that privacy concerns will simply vanish in a bout of extended apathy. The scheme is astounding for the scope it enables prying of medical data that would otherwise be deemed private.

Deficiencies were spotted early on. Far from being clinically-reliable as a record, it is dated and far from comprehensive. Any such record would be, at worse, a distraction in an emergency. Nor is there a track on who has seen it, except institutions en bloc.

If Australians do not opt out of the centralised medical scheme by October 15, a record by default will created, stored and used. This will mean that those in the healthcare provision business, be it pharmacists, nurses or podiatrists, not to mention a whole string of unknown providers, will have automatic access to the medical record without patient consent. The notions of express and fully informed consent have been given a dramatic, contemptuous heave ho, with a focus on the patient's volition to avoid the scheme altogether. The Australian government's refusal to engage the public in any meaningful way, be it through a sustained advertising or information campaign, has been patchy, and, in some instances, entirely absent.

Such an approach flies in the face of such recommendations as those made by the UK Information Governance Review from 2013 acknowledging "an appropriate balance between the protection of the patient user's information, and the use and sharing of such information to improve care". This balance was struck on principles derived in the 1997 Review of the *Uses of Patient-Identifiable Information*, chaired by Dame Fiona Caldicott. While admitting that information governance might at stages have to give way to sharing confidential patient information for the sake of that patient's welfare, the principles of data security remain fundamental.

A skirt through the My Health Record system yields the extent of its shabbiness, and the level of its aspiration. The My Health Record privacy policy is hardly glowing, acknowledging the problems with having such a database in the first place.

> "In any online platform, including the My Health Record system, there are inherent risks when transmitting and storing personal information."

Then comes the mandatory, if hollow reassurance:

> “Despite this, we are committed to protecting your personal information, and ensuring its privacy, accuracy and security.”

A rich opportunity for the prying and the pilfering await.

*

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research. Email: bkampmark@gmail.com

---