AUSTRALASIAN
PSYCHIATRY

Psychiatric electronic health records in the era of data breaches – What are the ramifications for patients, psychiatrists and healthcare systems?

Australasian Psychiatry
2024, Vol. 32(2) 121–124

DOI: 10.1177/10398562241230816
journals.sagepub.com/home/apy
Sage

Jeffrey CL Looi Academic Unit of Psychiatry and Addiction Medicine, Canberra Hospital, The Australian National University School of Medicine and Psychology, Canberra, ACT, Australia; and Consortium of Australian-Academic Psychiatrists for Independent Policy and Research Analysis (CAPIPRA), Canberra, ACT, Australia

Richard CH Looi Independent Scholar, Canberra, ACT, Australia

Paul A Maguire Academic Unit of Psychiatry and Addiction Medicine, Canberra Hospital, The Australian National University School of Medicine and Psychology, Canberra, ACT, Australia; and Consortium of Australian-Academic Psychiatrists for Independent Policy and Research Analysis (CAPIPRA), Canberra, ACT, Australia

Steve Kisely Consortium of Australian-Academic Psychiatrists for Independent Policy and Research Analysis (CAPIPRA), Canberra, ACT, Australia; School of Medicine, Princess Alexandra Hospital, The University of Queensland, Woolloongabba, QLD, Australia; and Departments of Psychiatry, Community Health and Epidemiology, Dalhousie University, Halifax, NS, Canada

Tarun Bastiampillai Consortium of Australian-Academic Psychiatrists for Independent Policy and Research Analysis (CAPIPRA), Canberra, ACT, Australia; College of Medicine and Public Health, Flinders University, Adelaide, SA, Australia; and Department of Psychiatry, Monash University, Clayton, VIC, Australia

Stephen Allison Consortium of Australian-Academic Psychiatrists for Independent Policy and Research Analysis (CAPIPRA), Canberra, ACT, Australia; and College of Medicine and Public Health, Flinders University, Adelaide, SA, Australia

Abstract

Objective: To update psychiatrists and trainees on the realised risks of electronic health record data breaches.
Methods: This is a selective narrative review and commentary regarding electronic health record data breaches.
Results: Recent events such as the Medibank and Australian Clinical Labs data breaches demonstrate the realised risks for electronic health records. If stolen identity data is publicly released, patients and doctors may be subject to blackmail, fraud, identity theft and targeted scams. Medical diagnoses of psychiatric illness and substance use disorder may be released in blackmail attempts.
Conclusions: Psychiatrists, trainees and their patients need to understand the inevitability of electronic health record data breaches. This understanding should inform a minimised collection of personal information in the health record to avoid exposure of confidential information and identity theft. Governmental regulation of electronic health record privacy and security is needed.

Keywords: e-health, healthcare management, information management, electronic health records, psychiatric care

'It is impossible to completely mitigate cyber threats: "Today it has become a question of "when," and "at what level"" systems such as [MyHealthRecord or electronic health records] will be breached (p. 574)'.[1]

Corresponding author:
Jeffrey CL Looi, Academic Unit of Psychiatry and Addiction Medicine, Australian National University School of Medicine and Psychology, Canberra Hospital, Building 4, Level 2, PO Box 11, Garran, ACT 2605, Australia.
Email: jeffrey.looi@anu.edu.au

Australian public healthcare services have embraced the enhanced centralisation and accessibility of electronic health record systems (EHRs). The prevalence of these systems creates new privacy risks that are especially important in psychiatric care. Private healthcare services have also increasingly adopted similar digital systems.

Such digital systems have been compromised by external attackers through the exploitation of technical vulnerabilities. In 2018, the Victorian Auditor-General's Office conducted digital penetration testing, using basic hacking tools, and was able to access health data systems in four audited health organisations.[2]

Data breaches of digital healthcare systems and records in Australia[1] and internationally,[3] including publication of personal healthcare data for extortion or ransom, have occurred, such as for Medibank Private[4] and Australian Clinical Labs[5] customers.

These data breaches are particularly salient for EHRs that contain sensitive information on the mental health of patients. Apart from the usual medical and demographic history, these EHRs contain details of psychiatric and substance abuse diagnoses, which were specifically targeted for extortion to prevent publication in the recent Medibank Private data breach.[6,7]

To date, Australia does not have legislation similar to the US Health Insurance Portability and Accountability Act (HIPAA) which, in addition to legislating for health insurance coverage, provides governmental regulatory guidance regarding the privacy and security of EHRs.[8,9] Despite the best cybersecurity measures,[10] the authors of a systematic review have concluded it is inevitable that EHRs will be compromised by malicious attackers resulting in a loss of confidentiality of healthcare data.[1] It has therefore been recommended that regulation of EHRs and healthcare data is necessary in Australia and could follow the model of the HIPAA.[1]

In this context, patients, trainees, psychiatrists and healthcare networks need to be informed about the risk of EHR data breaches involving psychiatric records and supported for adverse consequences.

Informed consent and a minimum dataset

Perhaps the simplest approach is to assume that a patient's EHR will eventually be breached, and to thus limit the personal and confidential information that is recorded in the form of a minimised dataset. There needs to be careful discussion of the substantial likelihood of a data breach with patients and carers, and that any consequent reduction in the amount of data recorded may therefore limit EHR usefulness.

The key areas that might be minimised include those personal or health historical details that are likely to cause complications if publicly available through a data breach. This may include, among other matters, interpersonal disputes in which others are named, historical details of abuse or trauma and even family histories.

It will be important to seek the patient's view on what data should be recorded, based on the patient's capacity to do so. A very minimal dataset might be restricted to certain details (see section below) but will reduce utility, and effectiveness to personalise care.

There are also privacy implications for psychiatrists, trainees and other healthcare workers (HCWs) from EHR data breaches. The personal details for the digital identities of staff and patients will likely be exposed in breaches. In addition, once a digital system such as an EHR is compromised, it may be possible for a malicious attacker to pivot (https://csrc.nist.gov/glossary/term/pivot) to other systems to access financial and personnel records that present further identity theft risks for patients and HCWs. As the psychosocial safety and wellbeing of patients and HCWs can be adversely affected by data breaches, there is a responsibility for health system administrators and health governance boards to inform and support those affected (see further below).

Suggestions for an EHR database sufficient for clinical purposes but without unnecessary personal details

We suggest some considerations towards a minimum patient EHR dataset for psychiatry and addiction medicine, as follows, although practical implementation of such changes will be complex and challenging:

- Purpose of consultation or entry.
- List of current medication.
- Medication changes.
- Risk assessment.
- Therapy changes, including limited details on psychosocial supports.
- Limit details of personal events, and interpersonal information, including full names, to that necessary to support the above. For example, a sibling might be designated 'the patient's brother Michael' without using the full name, and similarly for a genogram.
- For statements about other people made by the patient, it is suggested this may take the form of '…the patient stated that their manager has shouted at them….', without including names.
- Psychotherapy notes may need to be stored securely offline due to the sensitive nature of the material and, instead, a brief procedural summary included in the EHR. For example, a summary might be as follows: 'We explored trauma issues related to the initial childhood exposure'.
- The most sensitive issues will relate to safety, including the necessary documentation of self-harm, risky, suicidal and threatening behaviour. It may be

better to describe the behaviours neutrally, to avoid the perception of value judgements if data is breached. For example, '…the patient stated she had cut her arm to relieve distress…'.

- There may be important exceptions, such as in forensic or medico-legal matters, where all names and details must be recorded. This would include patients who are under psychiatric treatment orders according to governmental mental health legislation.

This list cannot be exhaustive and what material is recorded should be discussed in a collaborative care framework with the patient. There may be a necessary exception to such discussion, regarding documenting threats by patients against HCWs and others.

Given the privacy implications for psychiatrists, trainees and other HCWs from EHR data breaches as discussed above, consideration should be given to essential HCW identity information to be stored in EHRs. HCWs should also ensure that records are neither defamatory nor stigmatising.

Aftercare for psychiatric health record data breaches and other access

For patients seeking psychiatric care, there is a special responsibility for providing psychological support in the event of an EHR data breach. Based on current international healthcare data breach trends, extortion and ransom of healthcare organisations is most likely, and the healthcare sector has incurred the most costs from data breaches worldwide compared to other business sectors.[3]

Cyber-criminals published the health records of people with potentially embarrassing or private medical histories (such as termination of pregnancy, mental health and substance abuse treatment), in order to extort the Medibank Private health insurance provider.[6,7] For example, the breached personal details for '…100 people [were] singled-out for having medical diagnoses of psychological disorders and drug addiction'.[7]

In addition, there may have been attempts to directly contact insured people and extort funds to prevent publication of their personal data,[7] which would be distressing and particularly challenging for people with mental illness and substance use problems. It was noted: 'Blackmail, fraud, identity theft and targeted scams are the three most obvious options for the hackers now in possession of Medibank customers' data'.[7]

Apart from the specific advice from experts cited above,[7] there appears to be little specific guidance on aftercare for patients with personal data exposed via EHR data breaches available from the governmental, industry and NGO-sponsored IDCARE support site (https://www.idcare.org/). Medibank Private data-breach-affected customers were provided access to counselling support for distress arising from the breach.[7] For public sector healthcare records, the most appropriate psychological support would be provided by patients' existing psychiatrists and HCWs. If, however, the HCWs themselves are compromised by the same data breach through exposure of personal information, there may be limited capacity to respond.

HCWs are also likely to be exposed to the same risks of 'Blackmail, fraud, identity theft and targeted scams….'[7] as patients. Publication of health professionals' personal data may expose them to risks from cyber- [11] or personal stalking or bullying.[12] This can include 'doxing' or the publication of personal details such as address and contact details with malicious intent to facilitate targeting of individuals, which is a form of cyberbullying.[13]

Personalised cybersecurity insurance, identity cybersecurity advice and psychological support are therefore necessary for patients, psychiatrists and HCWs, in addition to that extended to healthcare organisations. For psychiatrists and other HCWs, professional indemnity insurance might need to be expanded to provide cybersecurity coverage of workers' personal data held in healthcare data systems, and also identity cybersecurity and psychological support.

Conclusions

There remains a clear and present danger from data breaches of EHRs. Patients with mental illness and substance abuse disorders have been specifically targeted for extortion in the recent Medibank Private data breach[7] and similar cyberthreats internationally.[3] In this context, governmental regulation of health data privacy and security standards, such as legislation similar to the US HIPAA,[8,9] is necessary.[1]

It is essential that healthcare organisations, HCWs and governments remain informed, active and disclose to patients these realised data breach risks. Minimising sensitive psychiatric and substance use disorder information in health records, unfortunately limits the usefulness of the records. This will be challenging to realistically implement due to the size and complexity of EHRs and health data systems. Planned psychological care pathways and cybersecurity resources are needed to support patients and HCWs for these inevitable data breaches.

Author contributions

All authors made substantial contributions to the conception or design of the work; the acquisition, analysis or interpretation of data; drafting the work or revising it critically for important intellectual content; and final approval of the version to be published and also agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Disclosure

The author(s) declared the following potential conflicts of interest with respect to the research, authorship, and/or publication of this article: Authors JCLL, PAM, SK, TB and SA are all editorial team members for the journal - they were not involved in peer review of the paper.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Jeffrey CL Looi https://orcid.org/0000-0003-3351-6911
Steve Kisely https://orcid.org/0000-0003-4021-2924
Tarun Bastiampillai https://orcid.org/0000-0002-6931-2913
Stephen Allison https://orcid.org/0000-0002-9264-5310

References

1. Offner KL, Sitnikova E, Joiner K, et al. Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intell Natl Secur* 2020; 35: 556–585. DOI: 10.1080/02684527.2020.1752459

2. VAGO. *Security of Patients' Hospital Data*. Melbourne: VAGO, https://www.audit.vic.gov.au/report/security-patients-hospital-data?section=33170–3-effectiveness-of-data-security-in-health-services&show-sections=1#33170–3-effectiveness-of-data-security-in-health-services (2019, accessed 29 September 2023).

3. IBM_Security. *Cost of Data Breach Report*. Armonk, NY: IBM, https://mysecuritymarketplace.com/reports/cost-of-data-breach-report-2023 (2023, accessed 25 September 2023).

4. Terzon E and Yang S. *Medibank says all customers' personal data compromised by cyber attack*. Ultimo: ABC, https://www.abc.net.au/news/2022-10-26/medibank-hack-criminals-access-hack-data/101578438 (2022, accessed 25 September 2023).

5. Terzon E. *Pathology company Australian Clinical Labs reveals it was hit by cyber attack in February*. Ultimo: ABC, https://www.abc.net.au/news/2022-10-27/acl-cyber-attack-pathology-lab-health-data/101584072 (2022, accessed 25 September 2023).

6. ABC. *Hackers claim they demanded $15 million ransom as more Medibank customer data posted to dark web*. Ultimo: ABC, https://www.abc.net.au/news/2022-11-10/medibank-data-breach-latest/101637160 (2022, accessed 25 September 2023).

7. Foster J and Williams JJ. *Medibank hackers are now releasing stolen data on the dark web. If you're affected, here's what you need to know*. Melbourne: The Conversation, https://theconversation.com/medibank-hackers-are-now-releasing-stolen-data-on-the-dark-web-if-youre-affected-heres-what-you-need-to-know-194340 (2022, accessed 11 October 2023).

8. US_Department_of_Health_and_Human_Services. *Health information privacy*. Washington, DC: US Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/index.html (2023, accessed 11 October 2023).

9. US_Department_of_Health_and_Human_Services. *What does the HIPAA Privacy Rule do?* Washington, DC: US Department of Health and Human Services, https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html (2023, accessed 11 October 2023).

10. ACSC. *Australian Cyber Security Centre*. Canberra: ACSC, https://www.cyber.gov.au/ (2023, accessed 11 October 2023).

11. Stevens F, Nurse JRC and Arief B. Cyber Stalking, cyber harassment, and adult mental health: a systematic review. *Cyberpsychol, Behav Soc Netw* 2021; 24: 367–376. DOI: 10.1089/cyber.2020.0253

12. Nelsen AJ, Johnson RS, Ostermeyer B, et al. The prevalence of physicians who have been stalked: a systematic review. *J Am Acad Psychiatry Law* 2015; 43: 177–182.

13. Chen M, Cheung ASY and Chan KL. Doxing: what adolescents look for and their intentions. *Int J Environ Res Public Health* 2019; 16: 218. DOI: 10.3390/ijerph16020218