Ethical Issues in Secondary Use of Personal Health Information.

3 authors:

Thomas Gallagher
University of Montana
10 PUBLICATIONS **11** CITATIONS

SEE PROFILE

Kudakwashe Dube
Massey University
49 PUBLICATIONS **135** CITATIONS

SEE PROFILE

Scott Mclachlan
Queen Mary, University of London
12 PUBLICATIONS **7** CITATIONS

SEE PROFILE

Ethical Issues in Secondary Use of Personal Health Information

By: Thomas Gallagher, Kudakwashe Dube, and Scott McLachlan

May 2018

The accessibility of personal health information (PHI) will increase on the Internet of the future to provide timely support for both primary and secondary uses. Although PHI for secondary uses is generally anonymized, its widespread distribution on the Internet raises ethical concerns. The PHI should remain an individual's most closely guarded asset[1, 2]. While other forms of personal data represent what the person does, owns, or knows, PHI represents what the person is. PHI describes the biological attributes of the human being, often containing longitudinal records of wellness, illness, test results, and treatments[3]. These characteristics amplify the seriousness and un-reversible consequences that uniquely differentiate breaches or disclosures of PHI data from other forms of data breach. In conducting risk assessment analysis, the result of even a single PHI data breach can be catastrophic. As it is impossible to place a price on our health, it is similarly impossible to place a price on PHI. Risk assessments calculations[4] involving annual loss expectancy, single loss expectancy, or annualized rate of occurrence are irrelevant when PHI has been breached. In light of this, the questions of: (1) granting the patient the right to consent, that is, opt-in or out, of the de-identification and subsequent secondary use of their PHI; and (2) finding synthetic alternatives to de-identified PHI for certain type of secondary uses to protect patient privacy, urgently need to be addressed.

Primary and Secondary Use of PHI

Primary use of PHI is defined as exclusive use by the organization which acquired the data, in providing real-time direct care to the patient[5]. Technologies like the Electronic Health Record (EHR) provide a digital archive of patient PHI. In the US, meaningful use of EHR systems have been mandated for all healthcare facilities through the Health Information Technology for Economic and Clinical Health Act (HITECH, 2009). Secondary use of health data is deemed non-essential to direct care of the specific patient[5]. Some secondary uses directly supplement the needs of primary care. Examples include medical billing and hospital administrative and management operations. While secondary use includes benevolent causes that support medical research and public health, other secondary use involves sales, marketing, and financial gain[6]. Secondary use regularly occurs without the patient's knowledge or consent.

While the secondary use of PHI without patient consent in research activities, public health protection, and patient safety can be rationalized, personal privacy concerns need to take precedence. Furthermore, the secondary use of PHI for auxiliary activities involving finances, marketing, system development, or training, is more difficult or in some cases impossible to justify over personal privacy concerns[7, 8]

Health and privacy laws including the US Health Insurance Portability and Accountability Act (HIPAA, 1996), Australian Privacy Act (1988), New Zealand Privacy Act (1993), Canadian Personal Information Protection and Electronic Document Act (PIPEDA, 2000), and the OECD Information Privacy Principles[9] imply the guarantee of a fundamental right to patient privacy. Although privacy laws require patient consent to use and disclose PHI, exceptions for secondary use exist in these jurisdictions. Legislation ensures protection of PHI, but also contain clauses allowing use of limited data sets without patient consent for the purpose of secondary use provided specific direct patient identifiers have been removed.

Data Breach through Re-identification

Re-identification occurs when an anonymous medical record has been linked back to the identity of the subject patient, sometimes through trivial means[9]. De-identification techniques such as Safe Harbor[10] are widely accepted as adequate measures in protecting patient privacy. The Safe Harbor de-identification process consists of removal (anonymization) or generalization (pseudonymization) of 18 personally identifying elements associated with the patient. De-identification is the standard method for PHI protection in most western jurisdictions, yet several use cases exist where de-identified health data has been released to the public and PHI has been breached through re-identification[11, 12, 13]. One response to the re-identification threat does not involve revision of anonymization and health data release practices, rather the use of legislation making re-identification unlawful and punishable through fines and imprisonment[14]. The first such legislation proposed was in response to Melbourne University researchers quietly informing Australian Health Department officials that prescriber details in Medicare prescription data released on a government website could be easily re-identified[15]. The precedent set by this legislation expressly discourages further data security research efforts and enhanced anonymization techniques aimed at safely enabling access to private health information datasets.

The Edict of Patient Privacy

Patient privacy is a universal edict for all health professionals as it is a fundamental pillar in establishing trust within the patient-clinician relationship. The Hippocratic Oath[16] and its modern derivatives are based upon the concept of patient-clinician relationships in which confidentiality is ensured, along with the clinician's edict to do no harm. Although patient consent for medical treatment is the gold standard in healthcare, patient consent for the release and use of de-identified patient records is not adequately recognized. The lack of patient consent for de-identified health records is based on the false pretense of privacy and absolute safety assumed by anonymization processes and emerging legislative trends prohibiting re-identification as a result of anonymizations' failed promise to protect patient privacy. A relevant ethical question in this discussion is: At what point does the patient have the opportunity to opt-out of PHI data sharing activities? The reality in modern medicine is that the patient has neither the ability to opt-in or opt-out when their PHI is anonymized, released and/or sold.

PHI and Electronic Health Records

As the EHR matures as a healthcare technology and shared care records become ubiquitous, data sharing of PHI is likely to rapidly increase. As the demand for highly available EHRs grows, society's laws and policies addressing secondary use of healthcare data must evolve beyond sole reliance on de-identification. New technologies such as the Realistic Synthetic EHR (RS-EHR)[17] have resulted in successful synthetic EHR prototypes including CoMSER[18] and Synthea[19]. Rather than sharing PHI data, synthetic records are generated from publicly available aggregates drawn from protected PHI data. The premise in using synthetic records is that real PHI is never exposed. The use of synthetic records is a risk avoidance strategy for protecting PHI eliminating any potential risk of data privacy breaches suffered by de-identified PHI. Synthetic records should be made highly available and serve as an additional safety mechanism where a realistic, but not the real PHI is required. Synthetic records are useful for many albeit not all secondary uses[15]. Hence, investigations into advanced methods for generating realistic synthetic PHI would seem to be urgently required due the increasing trend to share de-identified PHI for such secondary uses.

Conclusion

The primary ethical issues brought forward in this discourse are patient consent and further reduction of unnecessary exposure of vulnerable de-identified PHI through use of systematically generated realistic synthetic PHI where possible. The assumption that de-identification guarantees privacy is simply not true[11, 12, 13], thus all patients should have the right to opt-out of data sharing. At the very least, further precautions should be implemented to protect patient PHI from many non-essential secondary uses. Despite a call to the research community to construct a framework for secondary use of health data[5], little work has yet to been done in this area. It is time that a new taxonomy and ontology[20] of secondary use be developed and adopted by the medical profession [21] with a call for action to protect PHI from those classifications of secondary use that need access to the real PHI found in EHRs, and those that are adequately served by a realistic, but not real, EHR. The medical community are bound by Hippocratic Oath and derivative professional codes of ethics to protect patients by embracing new technologies, such as generators of RS-EHRs, for PHI protection which enhance risk avoidance from data breach involving secondary use.

References

1. Spencer, K., Sanders, C., Whitley, E. A., Lund, D., Kaye, J., & Dixon, W. G. (2016). Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: a qualitative study. Journal of medical Internet research, 18(4).

2. Moskop, J. C., Marco, C. A., Larkin, G. L., Geiderman, J. M., & Derse, A. R. (2005). From Hippocrates to HIPAA: privacy and confidentiality in emergency medicine—part I: conceptual, moral, and legal foundations. Annals of emergency medicine, 45(1), 53-59.

3. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE transactions on parallel and distributed systems, 24(1), 131-143.

4. Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. Computers & Security, 24(2), 147-159.

5. Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., & Detmer, D. E. (2007). Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. Journal of the American Medical Informatics Association, 14(1), 1-9.

6. American Medical Informatics Association. (2007). Secondary Uses and Re-uses of Healthcare Data. https://www.amia.org/sites/amia.org/files/2007-Policy-Meeting-amia-taxonomy-Secondary-Data-Use-Version.pdf

7. Tanner, A. (2016). How data brokers make money off your medical records. Scientific American, 1. https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/ Accessed 2018-04-02.

8. Robertson, J. (2013). Your medical records are for sale. Bloomberg Businessweek https://www.bloomberg.com/news/articles/2013-08-08/your-medical-records-are-for-sale. Accessed 2018-04-02.

9. OECD. (2013). The OECD Privacy Framework. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, Accessed: 2017-12-29.

10. US Department of Health and Human Services. Methods for De-Identification. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html Accessed: 2018-01-12.

11. Sweeney, L. (2015). Only you, your doctor and many others may know. Technology Science. http://techscience.org/a/2015092903/ Accessed 2017-01-29

12. Ohm, P. (2007). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57(1701).

13. El Emam, K., Jonker, E., Arbuckle, L., & Malin, B. (2011). A systematic review of re-identification attacks on health data. Plos One, 6(12)

14. Australian Federal Register. Privacy Amendment (Re-identification Offence) Bill 2016. https://www.legislation.gov.au/Details/C2016B00156/Explanatory%20Memorandum/Text

15. Phillips, M., Dove, E.S. & Knoppers, B.M. Bioethical Inquiry (2017) 14: 527. https://doi.org/10.1007/s11673-017-9806-9

16. W.T. Reich (Ed.). (1995). Encyclopedia of Bioethics, Vol. 5, Macmillan, New York, NY, p. 2632.

17. Dube, K., & Gallagher, T. (2013, August). Approach and Method for Generating Realistic Synthetic Electronic Healthcare Records for Secondary Use. In FHIES (pp. 69-86).

18. McLachlan, S., Dube, K., & Gallagher, T. (2016, October). Using the CareMap with Health Incidents Statistics for Generating the Realistic Synthetic Electronic Healthcare Record. In Healthcare Informatics (ICHI), 2016 IEEE International Conference on (pp. 439-448). IEEE.

19. Walonoski, J., Kramer, M., Nichols, J., Quina, A., Moesel, C., Hall, D., Duffett, C., Dube, K., Gallagher, T., & McLachlan, S. (2017). Synthea: An approach, method, and software mechanism for generating synthetic patients and the synthetic electronic health care record. Journal of the American Medical Informatics Association.

20. Bukhari, A. C., Nagy, M. L., Krauthammer, M., Ciccarese, P., & Baker, C. J. (2015, July). BIM: an open ontology for the annotation of biomedical images. In ICBO.

21. Bukhari, S. A. C., Krauthammer, M., & Baker, C. J. (2014). SEBI: An Architecture for Biomedical Image Discovery, Interoperability and Reusability Based on Semantic Enrichment. In SWAT4LS.

Dr. Thomas Gallagher is a professor in the Department of Applied Computing & Engineering Technology at the University of Montana where he directs the Information Technology program of study and oversees the recently developed Cybersecurity Center for Academic Excellence (CAE) at Missoula College. He teaches courses in information technology and computer science, and leads student internship efforts. He has developed and continues to lead the undergraduate, general education course Social and Ethical Issues in Computer Science which examines policy, law, and ethics in computing, including privacy issues associated with data collection practices. As a visiting faculty member at Massey University (NZ), he and Dr. Dube developed the Realistic Synthetic EHR (RS-EHR) project and later co-founded the HIKER Research group with Queen Mary University Researcher, Scott McLachlan. Dr. Gallagher possesses Ed.D and M.Ed degrees in Education Leadership from the University of Montana, the MS degree in Computer Science from Western Washington University, and the BA degree in Mathematics from Carroll College.

Dr. Kudakwashe Dube is a lecturer in Computer Science and Information Technology within the School of Engineering and Advanced Technology at Massey University where he teaches undergraduate and postgraduate courses including the IT ethics and professionalism course, Social and Professional Issues in Information Technology. Dr Dube's research interests are in knowledge modelling and representation, decision-support systems, computer security and information privacy. His current research projects investigate: (1) modelling Clinical Practice Guidelines for integrating them in a manageable way, into computer-based solutions in healthcare, e..g., modelling caremaps for use in algorithms for generating the RS-EHR; (2) new paradigms and metaphors for security and privacy for sensitive personal information, e.g., the healthcare record; and (3) investigating domain knowledge incorporation into established and new solution models and algorithms for solving problems in Healthcare, Food and Nutrition Science and Agriculture. His research work is undertaken within the HIKER Group. Dr Dube holds the PhD degree in Computer Science from the Dublin Institute of Technology, Ireland, the BSc in Computer Science and Mathematics, and the BSc Honours degree in Computer Science from the University of Zimbabwe.

Scott McLachlan is a researcher with the Risk and Information Management group at Queen Mary University of London. He researches the application and integration of intelligent computer systems, or *Learning Health Systems*, in clinical practice. He regularly delivers undergraduate lectures and tutorials on a range of computing ethics, cyber law and practical programming and networking skills courses. Mr. McLachlan possesses MPhil(Sc) (distinct) and GDip degrees in Information Science from Massey University, a GDip in Business from the Open Polytechnic, a GDip in Law (GDL) from the University of Waikato, and a GCert in Tertiary Teaching and

Learning Practices from the University of Wollongong. During the first half of 2018 he also expects to complete the requirements for an LLM from the Australian National University.