

A person wearing teal scrubs and white sneakers stands in the center of a long library aisle. They are holding a stack of several books. The aisle is lined with tall shelves filled with books, many of which have colorful labels on their spines. The perspective is from a low angle, looking down the aisle towards the person.

**IS PUSHING
HEALTH CARE'S
GREEN BUTTON
A KILL SWITCH FOR
PATIENT PRIVACY?**

By Janice F. Mulligan and Mark R. VonderHaar

A gravely ill 13-year-old girl is rushed to the emergency room of a state-of-the-art hospital. She has a history of lupus, a chronic inflammatory disease that causes her body's immune system to attack its own tissues and organs. Inflammation caused by lupus can affect many different body systems—including blood cells, brain, heart, and lungs, with the potential for either hemorrhaging (in which case she may bleed to death) or clotting (which could cause a stroke). Lab results show that the adolescent is at a high risk of clotting, but should she be given blood thinners (anticoagulants) because she may also be at risk of hemorrhaging? Finding no published medical literature on teens with lupus and the risks of clotting, the doctor surveys her medical colleagues. The first specialist says yes, immediately anticoagulate this patient. The second colleague is equally adamant that no, the child cannot be safely anticoagulated. Time is ticking . . . what should the treating doctor do?

Fortunately, this hospital is part of a prestigious academic medical center. The treating doctor just happens to have access to other patient data. This creative physician searches for teenagers with lupus who have been treated at this medical center in the last five years. She finds 100 similar patients, and within hours of the teenager's admission to the hospital, the doctor is able to determine that the teen's lab findings put her at six- to sevenfold increased risk of clotting. The child is immediately anticoagulated. She recovers and is discharged from the hospital. Science fiction? Hollywood blockbuster? No—this actually happened at Stanford Medical Center, and the physician, Jennifer Frankovich, MD, is the pediatric rheumatologist who conducted this unique method of analysis in order to treat her patient and later published her findings in the *New England Journal of Medicine*.¹

Dr. Frankovich's novel method of data mining as a form of medical research to treat an individual patient came to be called a "green button." Dr. Christopher Longhurst, then chief information medical officer at Stanford Children's Health, and his colleagues developed the health data aggregation theory of a green button. As he explained:

the idea behind the green button is that in the absence of good peer-reviewed evidence on a clinical decision, that you would be able to use the aggregate data in your electronic health record—or perhaps federated across multiple databases—to generate real-time, personalized comparative effectiveness cohorts, or "patients like mine."²

With a push of a green button, the physician is allowed to access and compare similar data from

electronic health records (EHR) nationwide. Why is this important? Because with a green button, an individual patient's specific race, age, and particular chronic diseases or conditions (comorbidities) can be compared to other individuals who are similarly situated in order to more precisely tailor treatment options. While the concept of a green button may revolutionize patient care management, it also presents significant challenges to patient privacy.

Other articles have examined the serious threat to privacy through phishing, malware, and other cyberattacks on EHR.³ This article examines the benefits to patient care management against the risks to patient privacy when EHR is shared and aggregated for the development of a diagnostic green button function.

EHR Then and Now

While EHR have been around for decades, only 18 percent of physicians were using an EHR system in 2001.⁴ The rest of the medical profession recorded medical information such as vital signs, orders, prescriptions, lab results, and progress notes either by hand or dictation. All of this clinical data was then stored on paper in color-coded paper charts on office shelves, until it was shipped to giant warehouses filled to capacity with other countless documents. Not only was the storage expensive, but the records decayed over time and were difficult to locate. If patient health records needed to be shared between health care providers, they were retrieved and then either mailed ("snail mail") or faxed. This traditional paper chart system was slow, expensive, and inconsistent.

Since the passage of meaningful use economic incentives⁵ and the HITECH Act in 2009, the use of EHR has skyrocketed. By the end of 2017, it is expected that approximately 90 percent of office-based physicians nationwide will be using EHR.⁶

The collection of EHR is a part of the larger "big data" movement: an astonishing 2.5 quintillion bytes of data has been collected—and 90 percent of that data in the world today has been created in the last two years alone.⁷

What is to be done with all of this data, specifically EHR? As Dr. Longhurst suggests, aggregate it to generate real-time personalized care—develop a green button functionality. Presently, one company manages 54 percent of all EHR in the United States and 2.5 percent of patients *worldwide*. In doing so, it is aggregating EHR and developing a green button function.⁸

EHR Sharing: The Precision Medicine Initiative

In 2015, the Precision Medicine Initiative was announced by the White House. One aim of the initiative was to manage and analyze EHR to empower



TIP

Electronic health records enable health care providers to aggregate patient data and deliver superior outcomes. But what are the privacy costs as technologies emerge in this growing sector?

patients and researchers to develop individualized care.⁹ It encouraged the further use of EHR and health information exchanges (HIEs).

With this emphasis on EHR and HIEs, aggregation of all EHR across

Janice F. Mulligan is an attorney and founding partner in the California law firm of Mulligan, Banham & Findley. For over three decades, her practice has been limited to representing patients in catastrophic medical negligence, personal injury, and nursing home neglect cases. A past member of the ABA House of Delegates, TIPS Council, and emeritus chair of the Standing Committee on Medical Professional Liability, she currently serves as a member of the ABA Standing Committee on the American Judicial System and TIPS Cybersecurity Task Force. A frequent lecturer both nationally and internationally, Mulligan has authored numerous peer-reviewed journal articles and book chapters in both medical and legal texts. She is also the ABA's 2013 recipient of the TIPS James K. Carroll Leadership Award. **Mark R. Vonderhaar** is a partner at Haight, Brown & Bonesteel LLP and a member of the Construction Law, Employment Law, and Risk Management & Insurance Law Practice Groups. He has a diverse array of risk management experience, including: analysis of emerging insurance coverage issues, providing opinion letters, drafting of underwriting and policy forms, representation of general insurance agencies, representation of insureds and insurance companies in insurance coverage litigation, representation of insurance companies in first- and third-party extracontractual litigation, and training of claims department personnel on insurance coverage and Fair Claims Practices Certification. They may be reached, respectively, at mulligan@janmulligan.com and mvonderhaar@hbblaw.com.

multiple different HIEs is now possible, and is called “interoperability.” It is this interoperability that permits the aggregation of EHR and the development of a green button function.

EHR aggregation and interoperability require patient consent. Therefore, patients need to balance the benefits of EHR sharing against the risks. The benefits include individualized patient care management (Care Everywhere), research (All of Us), development of artificial intelligence (Watson), and a diagnostic green button function. The risks involved with sharing EHR include re-identification, nationalized EHR, and suspect use of EHR data.

EHR Sharing Benefits: Care Everywhere, All of Us, and Watson

Within one software system, a nationwide EHR exchange exists called Care Everywhere, with participants from all 50 states, including over 900 hospitals, 20,000 clinics, and 115,000 providers. Care Everywhere allows health care providers to access a patient's EHR from other treating facilities. The system also allows users to interface with pharmacies, labs, immunization registries, and specialty registries.¹⁰ It may also provide for a “break glass” function to EHR in an emergency when normal access avenues are not available. Care Everywhere is clearly a benefit to the patient as it permits immediate EHR sharing with other treating facilities whenever needed.

Another benefit, more altruistic in nature, is EHR sharing for research. Research can speed up health innovation, pass research along to others, and provide patients more information and the power to decide. As Michael J. Fox, diagnosed with Parkinson's disease, states: “Every clinical study aims, in some way, to fulfill the promise

of scientific innovation—but none of these studies can be successful without the participation of committed volunteers. There is no Department or Secretary of Cures. It's us.”¹¹

The National Institutes of Health “All of Us” research program is part of the Precision Medicine Initiative first advanced by President Barack Obama in his 2015 State of the Union address in order to “give *all of us* access to the personalized information we need to keep ourselves and our families healthier.”¹² All of Us is a volunteer research program that intends to gather EHR data from millions of Americans with the goal of accelerating medical research and treatment while improving overall health outcomes. As with Care Everywhere, programs like All of Us provide a clear benefit to EHR sharing.

A third benefit of EHR sharing is artificial intelligence. IBM's Watson has acquired and digested hundreds of millions of EHR “lives” through acquisition of health-related companies.¹³ IBM seeks to aggregate EHR, claims data, imaging data, and other medical health data all in one data warehouse to improve Watson's fountain of knowledge.

In addition to the hundreds of million EHR “lives” Watson has consumed, it has also digested all of PubMed and Medline (two massive databases of medical journals), scores of medical textbooks, and thousands of training cases, and had tens of thousands of clinician hours spent fine-tuning its decision accuracy. Humans at University of North Carolina School of Medicine tested Watson by having the artificial intelligence (AI) analyze EHR on 1,000 cancer patients. In 99 percent of the cases, Watson recommended treatment plans that matched actual suggestions from oncologists. Because it had digested thousands of documents, it was

also able to recommend additional treatment options the human physicians missed in 30 percent of the cases.¹⁴

IBM's efforts are just one of many in the race to collect and use "lives" to teach AI more about the human condition.¹⁵ Through the use of algorithms and software, AI seeks to replicate human cognition in the analysis of complex medical data. The goal is for AI to render diagnoses, create and analyze the best treatment protocol, develop personalized drug treatment, and facilitate in personalized medicine. But to do this best, it needs all of our "lives"—including all of our EHR. As with All of Us, Watson may be viewed as a benefit, despite the developing fears involving autonomous AI.

EHR Sharing Risks: De-Identification, Nationalization, and Suspect Use

Patients expect that EHR is accessible to their own health care provider and available for their care.¹⁶ However, when the patient's EHR is transmitted to an HIE, subject to certain exceptions, all of the EHR may be transmitted. Even when certain identifying EHR is excluded, the combination of patient information from various other sources can lead to the identification of individual patients' EHR.¹⁷

For true anonymity to be achieved, personal identifiers need to be irrevocably stripped and deleted. A problem is that to be effective, many of the de-identifiers have to be reversed and reconnected to the research subject. The lack of unique identifying information is a barrier to the usefulness of the shared data.

Rather than strip and delete all identifiers, various software systems *de-identify* only certain data before the dataset is shared. Under this de-identified approach, the information is typically coded and a key

is separately maintained to the fully identified data set containing all of the data. Links exist in the coded de-identified data, allowing the information to be indirectly identifiable, so that a large amount of such incremental data is available for use by researchers including government agencies, universities, and even marketers.¹⁸

Furthermore, studies show it is possible to re-identify a person in a database from other information,

Even "anonymous" genetic data can be identified by cross-referencing it with information available online.

such as ethnic background, location, and medical factors unique to the individual. Additionally, studies have shown that it is easy enough to identify even "anonymous" genetic data by cross-referencing it with information available online, without the need for any special tools.¹⁹

For example, there are 1.5 million Americans with lupus. Of those, 20 percent are children of both sexes.²⁰ We know from Dr. Frankovich's medical journal article that she treated a 13-year-old female and was only able to identify 100 other adolescents treated at Stanford for lupus in a five-year period. No doubt the data she accessed contained much more information about each lupus patient, including race, ethnicity, zip code in which they reside, and probable family history. Given the prevalence of social media postings, how much effort would it take for someone to identify the individual patient she treated? Ultimately, despite de-identification technology, there can be no guarantees of anonymity given the likely development of re-identification technology.

Another risk involves nationalized EHR that creates one EHR target for those on the dark web. Stolen health records with EHR can be accessed, sold, and sometimes resold on the dark web. In just one example, a pregnant woman used a stolen medical identity of a Utah woman, Anndorie Cromar, to pay for maternity care at a Utah hospital. Because the baby was born with methamphetamine drugs in her system, Child

Protective Services took custody of the infant. But because of the stolen medical identity, the state incorrectly assumed that the child belonged to Cromar, and that Cromar was therefore a drug addict and a neglectful mother. As a result, the state attempted to take custody of Cromar's children. Only after a DNA test proved that Cromar was not the newborn's biological mother was Cromar able to recover custody of her children. She spent years trying to correct her medical records and clear her name.²¹ While a nationalized EHR provides for further development of a green button function, it also provides a one-stop target for hackers, and as such is a risk to patient privacy.

Additionally, wellness programs recently became a risk to EHR sharing. H.R. 1313 would limit Genetic Information Non-discrimination Act rules so that its protections would not apply to workplace wellness programs. These programs, originally promoted in the Affordable Care Act, were meant to encourage a healthy lifestyle, with the goal of reducing costly medical bills by creating healthier patients. Employees

who participate in such employer-sponsored wellness programs are promised the potential for lower premiums. Under the pending bill, if a company's wellness program includes genetic tests to identify health risk, then employees who refuse the tests would risk paying a penalty equaling hundreds or even thousands of dollars more per year in premiums.²²

One wellness program, albeit for livestock, promotes technology that permits a cow to "talk" with a farmer and aggregates the data to "monitor, react, and predict" livestock in real time to keep them healthier and more productive.²³ Similarly, aggregated EHR can be used by employers to keep their employees "healthier and more productive." While this risk may today be remote, the recent H.R. 1313 bill suggests otherwise. Unexpected uses of shared EHR will certainly develop, even a "Cows to Cloud" type function, and thus are a risk to patient privacy.

Finally, profiting by using a patient's EHR to aggregate and develop a green button function may be suspect use. Software companies are currently aggregating EHR to provide a diagnostic green button function. Patients will benefit from this function while they remain with the participating HIE. But if a patient changes HIEs, the benefit of previously sharing EHR is lost, while the software company retains its benefit (i.e., billions of dollars). This lost benefit to the individual patient is a risk to EHR sharing.

EHR Sharing and Meaningful Consent

Patients in need of care rarely read consent documents before signing them, either because they think their insurance will not authorize care or the health care will not be provided without a signature. A typical consent form authorizes the sharing of EHR, for purposes

including preventing disease, reducing serious threat to anyone's health, research, promoting public health and safety, law enforcement, health oversight, "special government functions," and administrative order.

Options to EHR sharing are not clearly presented, or if they are, options are limited. To the point, patients should inquire: Is

de-identification protocols, the green button may unavoidably serve as a kill switch for patient privacy. ■

Notes

1. Jennifer Frankovich, Christopher A. Longhurst & Scott M. Sutherland, *Evidence-Based Medicine in the EMR Era*, 365 *NEW ENG. J. MED.* 1758 (2011).

If a patient changes health information exchanges, the benefit of previously sharing EHR is lost, while the software company retains its benefit.

EHR being shared? Is there an HIE involved? Have software developers of functions like Care Everywhere, All of Us, Watson, and a green button been provided access to EHR? Other consent considerations include EHR sharing for employer wellness programs, sales, marketing, and fundraising.

Conclusion

In 2012, the Institute of Medicine reported that 89 percent of patients agreed that their own EHR should be used to improve the care of other patients.²⁴ Directly stated, "we must be willing to share our most personal asset: the data about our lifestyle, state of health, and disease."²⁵

The benefits of EHR sharing cannot be disputed. Green button functions will reduce suffering, extend lives, and stop disease by providing doctors with greater diagnostic and managed care tools.

A green button function, however EHR is de-identified, puts at risk privacy at a scale never before contemplated. Even with transparency in the consent, uses, and

2. *HISTalk Interviews Chris Longhurst, MD, MS, CMIO, Stanford Children's Health*, *HISTALK* (Aug. 20, 2014), <http://histalk2.com/2014/08/20/histalk-interviews-chris-longhurst-md-ms-cmio-stanford-childrens-health/>.

3. See, e.g., Janice Mulligan & Mark VonderHaar, *Health Hackers: Questioning the Sufficiency of Remedies When Medical Information Is Compromised*, 29 *HEALTH LAW.*, no. 1, Oct. 2016, at 29 (discussing the current law and evolving remedies to cyber risk in the health care system).

4. CHUN-JU HSIAO & ESTHER HING, *NCHS DATA BRIEF NO. 143, USE AND CHARACTERISTICS OF ELECTRONIC HEALTH RECORD SYSTEMS AMONG OFFICE-BASED PHYSICIAN PRACTICES: UNITED STATES, 2001-2013* (2014), www.cdc.gov/nchs/data/databriefs/db143.pdf.

5. Meaningful use regulations are Medicare and Medicaid programs that provide financial incentives for the "meaningful use" of certified EHR technology. In order to qualify for an EHR incentive, providers must show they are "meaningfully using" their certified EHR technology by meeting certain measurement thresholds that range

from recording patient information as structured data to exchanging summary care records. *Meaningful Use Regulations*, HEALTHIT.GOV, www.healthit.gov/policy-researchers-implementers/meaningful-use-regulations (last updated July 19, 2016).

6. Ryan Shay, *EHR Adoption Rates: 20 Must-See Stats*, PRAC. FUSION (Mar. 1, 2017), www.practicefusion.com/blog/ehr-adoption-rates/.

7. *Bringing Big Data to the Enterprise*, IBM, www-01.ibm.com/software/data/bigdata/what-is-big-data.html (last visited July 18, 2017).

8. Jeff Glaze, *Epic Systems Draws on Literature Greats for Its Next Expansion*, MADISON.COM (Jan. 6, 2015), http://host.madison.com/news/local/govt-and-politics/epic-systems-draws-on-literature-greats-for-its-next-expansion/article_4d1cf67c-2abf-5cfd-8ce1-2da60ed84194.html.

9. PRECISION MEDICINE INITIATIVE: DATA SECURITY POLICY PRINCIPLES AND FRAMEWORK (2016), https://allofus.nih.gov/sites/default/files/security-principles-framework.pdf.

10. Specialized registries must collect data from providers' EHR for the benefit of tracking "outcomes over time." Specialized registries, like state and local immunization registries and clinical data registries, are public health reporting options under the public health reporting for the stage 3 meaningful use program optional in 2017 and required in 2018. See Theresa Hush, *ABC's of Specialized Registries for 2016 MU Public Health Reporting*, BECKER'S INFECTION CONTROL & CLINICAL QUALITY (Mar. 08, 2016), www.beckershospitalreview.com/quality/abc-s-of-specialized-registries-for-2016-mu-public-health-reporting.html.

11. Michael J. Fox, *We Are All the "Department of Cures"*, SAN DIEGO UNION-TRIB., July 30, 2011, www.sandiegouniontribune.com/opinion/commentary/sdut-we-are-all-department-cures-2011jul30-story.html.

12. PRECISION MED. INITIATIVE, THE PRECISION MEDICINE INITIATIVE COHORT PROGRAM: BUILDING A RESEARCH FOUNDATION FOR 21ST

CENTURY MEDICINE 9 (2015) (emphasis added), www.nih.gov/sites/default/files/research-training/initiatives/pmi/pmi-working-group-report-20150917-2.pdf.

13. *IBM Watson Health Closes Acquisition of Truven Health Analytics*, PR NEWswire (Apr. 8, 2016), www.prnewswire.com/news-releases/ibm-watson-health-closes-acquisition-of-truven-health-analytics-300248222.html.

14. Dom Galeon, *IBM's Watson AI Recommends Same Treatment as Doctors in 99% of Cancer Cases*, FUTURISM (Oct. 28, 2016), https://futurism.com/ibms-watson-ai-recommends-same-treatment-as-doctors-in-99-of-cancer-cases/.

15. Press Release, IBM, *IBM Reveals Five Innovations That Will Help Change Our Lives within Five Years* (Jan. 5, 2017), http://www-03.ibm.com/press/us/en/pressrelease/51322.wss.

16. Pouyan Esmaeilzadeh & Murali Sambasivan, *Patients' Support for Health Information Exchange: A Literature Review and Classification of Key Factors*, 17 BMC MED. INFORMATICS & DECISION MAKING 1 (2017).

17. José Luis Fernández-Alemán et al., *Security and Privacy in Electronic Health Records: A Systematic Literature Review*, 46 J. OF BIOMEDICAL INFORMATICS 541 (2013).

18. See GIOVANNI LIVRAGA, *PROTECTING PRIVACY IN DATA RELEASE* 12 (2015); Erika Check Hayden, *Informed Consent: A Broken Contract*, NATURE (June 20, 2012), www.nature.com/news/informed-consent-a-broken-contract-1.10862.

19. Susan Young Rojahn, *Study Highlights the Risk of Handing Over Your Genome*, MIT TECH. REV. (Jan. 17, 2013), www.technologyreview.com/s/509901/study-highlights-the-risk-of-handing-over-your-genome/.

20. *Lupus in Children and Adolescents*, LUPUS RES. ALLIANCE, www.lupusresearchinstitute.org/lupus/lupus-children-and-adolescents (last visited July 18, 2017).

21. *America Tonight: How One Woman's Stolen ID Made Her the Mother of a Meth-Addicted Baby* (Al Jazeera America television broadcast Dec. 29, 2015), http://america.aljazeera.com/watch/shows/america-tonight/2015/12/how-one-womans-stolen-id-made-her-the-mother-of-a-meth-addicted-baby.html.

22. Sarah Zhang, *The Loopholes in the Law Prohibiting Genetic Discrimination*, ATLANTIC (Mar. 13, 2017), www.theatlantic.com/health/archive/2017/03/genetic-discrimination-law-gina/519216/.

23. *Cows to Cloud. Farm to Fridge*, DELL TECHS., www.delltechnologies.com/en-us/what-we-do/customer-stories/chitaledairy.htm (last visited July 18, 2017).

24. George Hripcsak et al., *Health Data Use, Stewardship and Governance: Ongoing Gaps and Challenges: A Report from AMIA's 2012 Health Policy Meeting*, 21 J. AM. MED. INFORMATICS ASS'N 204 (2014).

25. Beth Seidenberg, *You Should Share Your Health Data: Its Value Outweighs the Privacy Risk*, WIRED (Nov. 6, 2014), www.wired.com/2014/11/on-sharing-your-medical-info/.