Health information held hostage

How storing patient data on a decentralized blockchain can shift the security of the digital healthcare landscape

Jacek Orzylowski, Katherine Fleshner

ABSTRACT

Electronic medical records are increasingly vulnerable to hackers or rogue employees exploiting the consistent lack of cybersecurity expertise in hospitals. Since education in digital hygiene—keeping sensitive digital information secure—will likely never truly conquer the absent-minded nature of humankind, it could be worthwhile to implement the distributed peer-to-peer network of the InterPlanetary File System (IPFS), which would reduce the incidence of patient records being held hostage by hackers. However, this could also result in increased data breaches for informational gain only.

INTRODUCTION TO THE PROBLEM

It is no secret that an increasing amount of systems are being digitized for the sake of efficiency and convenience. These are some of medicine's favourite buzzwords, hence the development of a system of electronic medical records (EMRs) in the early 1970s by the Regenstrief Institute. Of course, the costs of computing in the 1970s were astronomical, and it took until the 1990s for computers to fall in price far enough for medical records to be digitized at scale. The benefits of such an initiative were myriad: minimization of errors associated with handwritten records, better coordination via facilitated information transfer between healthcare providers (HCPs), and maximized cost-efficiency by way of centralizing patient records so as not to waste resources in consolidating physically far-flung information.¹

However, it is this last benefit that has recently evolved into a liability; centres of consolidated information are vulnerable to attack. Just this last year, countless hospitals in Europe were crippled by so-called ransomware attacks, such as the NotPetya incursion, with the virus even spreading overseas to the United States and Canada. The hackers responsible for the breach encrypted the medical data of patients and refused to decrypt it until a ransom was paid by the hospital. Besides draining the already-stressed resources of many healthcare centres, as well as the profound economic impact facing patients, doctors, and government, the temporary loss of access to patients' medical data adversely affected patient care by removing constantly useful medical context and history from previous medical encounters.²

While the above-described NotPetya attack could have been repelled by keeping the affected computers' operating systems updated, more sophisticated methods of intrusion are certainly on their way, especially considering the effectiveness of the NotPetya and other attacks of this past year. And more often than not, even basic measures of cybersecurity fall through the cracks at hospitals

due to IT specialists undertrained in cybersecurity or harried hospital staff who have neither the time nor the inclination to practice digital hygiene. Hospital staff are extensively trained in the medical field, but are unaware that opening a seemingly-innocent email attachment or browsing websites on computers connected to the greater hospital network will expose the system to malware.^{3,4}

FUTURE SOLUTIONS

Since returning to pen-and-paper record-keeping is anathema to the majority of forward-thinking technophiles of this generation, a better solution would be to implement the peer-to-peer equivalent of a distributed blockchain—the IPFS. Taking a step back, it is important to understand the basic concept of a blockchain to begin—in simple terms, it is a record of events shared between many different individuals, not unlike a chain of emails: if you are part of the mailing list, you can see all the previous emails others have sent, while being unable to change those emails. In the specific context of the media buzz surrounding Bitcoin, for example, each email is analogous to an amount of bitcoins. Here the analogy breaks down, however, because one can transfer ownership of an email in the chain (bitcoins) to other parties. Blockchain technology is being touted as revolutionary because it is both public and anonymous—anyone can check the record of transactions for malfeasance (like reading through past emails) but each individual in the blockchain (the list of email addresses) is anonymized.⁵

Though anyone with an iota of marketing sense (and minimal style) can tout that they've created a technology that will revolutionize the future, IPFS may very well fit that label; this may have less to do with the system itself and more to do with the glut of data that will soon need to be incorporated into medical practice—individualized genomic data.⁶ In fact, many clinics are still in the process of completing the shift towards pure EMRs, and this shift will continue well into the future because of the multitude of benefits afforded by digitizing medical records.⁷

Traditionally, something like an EMR is stored on one set of servers. If these servers are breached, all the data inside is available to the intruder for viewing or changing (such as the encryption of the ransomed files). In a decentralized blockchain, the data exists on many different servers simultaneously—to return to the earlier analogy, everyone who received the chain email has all of the emails stored on their computer. These supplemental servers could exist within the hospital itself, in private companies, or in patients' computers. Much of the discussion on implementing IPFS focuses on patients being these servers—this would have the added benefit of allowing patients to be the custodians of their own medical data (a constant validation of their autonomy), and thus to play a more

central role in disseminating their information to their HCPs; these doctors, nurses, and so on would then also act as extraneous servers, therefore increasing security. If an intruder wanted to change the files to make them inaccessible for ransom, they would need to hack into the majority of the servers at the exact same time to have the permissions to change the file—with enough decentralized servers, it is essentially impossible to generate enough computational power to do so, especially because the current and future glut of medical data will create a large enough ecosystem to afford such decentralized protection.⁸ Besides, blockchains store a permanent history of any and all changes made to them, so even if the files were somehow encrypted, one needs only to return to the files' previous iteration to read the information unhindered.^{6,9,10} Therefore, until computing undergoes a foundational change itself, such as the leap to quantum computing and its inherent ability to exploit superposition, implementing blockchains for EMRs will protect the records at a structural level.

CAVEATS

However, there does exist a distinction between changing data and simply viewing it. With more points in a network having a copy of the records, it would actually be easier to hack into one to simply read the data. Though it is worth mentioning that the data being discussed would likely be encrypted as a default. So without the cryptographic key (password), the data would be meaningless. This nullifies many methods of hacking wherein obtaining a password is unnecessary. While gaining access to one server would not be enough to change the data for ransom, it would nevertheless expose sensitive patient information. While this would not impede medical treatment, nor cost a hospital anything in ransom money, it nevertheless constitutes a serious breach of privacy.¹¹ And there could be little done to stop a hacker from using the information they have gained from blackmailing particularly vulnerable patients in a more traditional way.

At the core of this hypothetical rewrite of record-keeping is the question of where to place responsibility—on the patients or on the healthcare system? Traditionally, doctors have been the keepers of such information, since they are the most knowledgeable on the subject, and make the most use of the information in the course of treating their patients. This method also likely streamlines the sharing of patient data between different healthcare providers. However, the issues of data breaches and digital hygiene persist; the success of ransomware attacks will only encourage further attacks, and greater ransoms. The ethical imperative to secure medical data will therefore continue to force hospitals to devote resources to paying these ransoms with capital that would have been infinitely better spent on maintenance, treatments, equipment, staff, etc.

If, however, patients were given the power over their own medical records, this framework of ransom would cease. Ransoms specifically targeted towards individuals may rise in its place, but would most likely happen much less often and at a smaller scale; although it would directly affect a patient instead of the hospital. This would shift the responsibility of digital hygiene to

the patient—it is likely that patient hygiene would far exceed that of healthcare staff, since the patient would have a much more personal interest in keeping their data secure, especially if they had particularly sensitive and vulnerable data in their records. Even with this scenario, however, hospitals and their lax security remain a point of entry for hackers to view multiple patients' data at once (assuming multiple cryptographic keys have been attained), unless, of course, hospitals employ multiple servers and avoid placing all of their patient data on each of them. Once the immense file size of personalized genomic medicine enters the clinical picture, it is likely that such multiple servers would have to be implemented regardless.⁷

CONCLUSION

Barring a planet-wide failure of the digital landscape, EMRs will continue to be adopted as storage technology becomes ever cheaper and more efficient. At its core, the shift to EMRs allows physicians to better coordinate their treatments among different healthcare teams, and minimizes errors and costs of consolidating far-flung handwritten notes. However, as sensitive information is increasingly found on digital mediums, criminals are adapting accordingly, hacking into secure servers to access data, which is integral to both privacy and treatment. A decentralized, distributed peer-to-peer network like the IPFS shows great promise in solving such a problem, outside of a rapid and profound escalation in resources devoted to IT security and digital hygiene. With IPFS, the medical community must decide whether it is acceptable to disseminate patient information throughout multiple points of access for safety from ransomware at the cost of putting patients in charge of their records, and at the cost of a possibly higher incidence of privacy-only breaches. Whatever the decision, it should be made and implemented before the EMR system becomes any more compromised than it has been recently. After all, an ounce of prevention is worth a pound of cure.

REFERENCES

1. "EMR: The progress to 100% electronic medical records." The University of Scranton. <https://elearning.scranton.edu/resource/health-human-services/emr-the-progress-to-100-percent-electronic-medical-records>.
2. Glaser, April. "U.S. hospitals have been hit by the global ransomware attack." Recode. June 27, 2017. <https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals>.
3. Rasch, Michael. "What keeps a hospital's immune system healthy?" Healthcare-in-Europe. May 16, 2017. <https://healthcare-in-europe.com/en/story/18021-what-keeps-a-hospital-s-immune-system-healthy.html>.
4. Nicholls, Mark. "Hospitals need a holistic approach to cyber security." Healthcare-in-Europe. February 20, 2017. <https://healthcare-in-europe.com/en/story/17337-hospitals-need-a-holistic-approach-to-cyber-security.html>.
5. Augur, Hannah. "WTF is the blockchain? A guide for total beginners" Dataconomy. October 19, 2015. <http://dataconomy.com/2015/10/wtf-is-the-blockchain-a-guide-for-total-beginners/>.
6. Nichol, Peter. "An IPFS addressable storage model for healthcare

- with blockchain.” CIO. February 22, 2017. <https://www.cio.com/article/3171132/innovation/an-ipfs-addressable-storage-model-for-healthcare-with-blockchain.html>.
7. “Storage gets a dose of medical data.” TechTarget. July 2008. <http://searchstorage.techtarget.com/magazineContent/Storage-gets-a-dose-of-medical-data>.
 8. “How blockchain technology keeps data secure.” Fraedom. <https://www.fraedom.com/496/blockchain-technology-keeps-data-secure/>.
 9. Kaal, Wulf. “How can blockchain be used as a database to store data?” Quora. July 18, 2017. <https://www.quora.com/How-can-blockchain-be-used-as-a-database-to-store-data>.
 10. Nichol, Peter. “The permanent web for healthcare with IPFS and blockchain.” ContentLoop. March 2, 2017. <https://www.content-loop.com/the-permanent-web-for-healthcare-with-ipfs-and-blockchain/>.
 11. Kakouros, Nikolaos. “Distributed storage healthcare — The basis of a planet-wide public health care network.” The Open Medical Informatics Journal, 7, 2013, 1-7. <http://doi.org/10.2174/1874431101307010001>