To: Don Rucker, M.D.**,** National Coordinator for Health Information Technology

Re: Healthcare Information Security Crisis

Problem Definition

Technological advancements and the increasing digitization of healthcare information provide many new opportunities to improve the efficiency of the United States healthcare system, but also make our nation's healthcare institutions increasingly susceptible to cyber-attacks. Past cyberattacks against U.S. healthcare institutions have already compromised the healthcare information of millions of Americans[1] and directly threatened human lives through the use of so-called ransomware or denial-of-service attacks that lock computers or encrypt data which healthcare systems need to function.[2]

Evidence

Cyber-attack magnitude

In 2015, there was a disturbing spike in the number of healthcare records accessed by hackers through cyber-attacks. In total, over 112 million healthcare records were stolen that year.[1] Healthcare breaches remain a serious problem for the United States healthcare system.[3, 4] The massive breach in 2015 should have served as a wake-up call to the healthcare industry that current practices of safeguarding health information are insufficient, yet common problems persist throughout the healthcare system. The costs and risks of vulnerable healthcare information systems are undeniable.

Cyber-attack methods

Cybercrimes targeting healthcare systems are becoming increasingly more frequent[5] and hackers are getting more sophisticated in their methods.[2] Healthcare record breaches can lead to concerns that stolen records may be held ransom, leaked or used for identity theft. In addition to these privacy concerns, hackers can disrupt healthcare systems in novel ways. Instead of stealing data, hackers can encrypt data on healthcare institution computer systems rendering them unusable until hackers provide decryption keys.[2, 6] When holding healthcare institutions ransom, hackers often demand payment in bitcoin, a virtual currency that allows for anonymous payments that are difficult or impossible to trace.[5, 7] The intensity and diversity of cyber-attack targets are likely to

surge with the increasingly widespread use of electronic health records, smart devices and technologies like virtual currencies.

Blockchain technology in healthcare

Paradoxically, while the widespread use of bitcoin has been linked to an increase in healthcare cyber-attacks,[8] some experts suggest that the answer to cybersecurity problems in healthcare may lie in blockchain,[9] the underlying technology that allows bitcoin to function. Blockchain records information in a series of timestamped, encrypted chunks called blocks, which are uniquely identified by cryptographic keys called hashes that are available to the public.[10] Importantly, a practical demonstration of blockchain's utility in healthcare has been presented by US researchers.[11] Despite this evidence, there is no universal consensus on whether healthcare information in the US should be managed like bitcoin financial transactions.

Healthcare data management

There are two general methods of healthcare information management: 1) healthcare data are stored on central servers (so-called data silos) at healthcare institutions as they are now, 2) healthcare information is stored in a decentralized form (a so-called data lakes or warehouses) that is governed by blockchain technology and/or secure cloud computing system,[12-14] such as Amazon Web Services, Google Cloud Platform, or Microsoft Azure. Proponents of the first model focus on making existing healthcare information infrastructure more secure by updating obsolete systems and providing information security training to healthcare employees.[5] Proponents of the second model, highlight the many potential benefits of a blockchain-based healthcare information system.[9, 15, 16]

Technology is the problem, but may also be the solution

From the literature, we have some understanding of current technologies and practices that put healthcare data at high-risk. These include using clicking on infected emails, visiting websites using the Microsoft browser Internet Explorer,[6] and carrying patient data on portable storage devices.[17] This is logical, because the first step towards addressing the healthcare information security crisis is to identify high-risk practices that affect the present. Yet, this approach is limited because it depends on regulating human behavior. Human errors can be avoided through

implementation of advanced technologies. For example, portable data storage devices could be avoided all together if all computers had access to the data on secure cloud-based networks. Information can be protected through encryption, while emails and websites can be verified using an authentication system called hashing.[6]

Current policies

Current policies for protection of electronic health records in the United States are dictated by the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 2002 Federal Information Security Management Act (FISHMA) the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, and the 2010 Affordable Care Act.[17] These current policies require healthcare institutions to embrace digitization of health records but also leave them critically unprepared for the management and protection of large amounts of healthcare data. New policies for mandating cyber-security requirements and cyber-attack preparedness are required, but research to inform the creation of new policies for healthcare information security area is lacking in two critical areas.

Gaps in the literature

These two fundamental gaps in the literature are analyses of 1) which novel technologies can best improve US healthcare cyber-security and 2) how to implement such technological innovations in the US healthcare system. The first gap is important because policymakers cannot endorse in any particular technological solution without ample proof that it is effective deterrent to cyber-attacks. The second gap is important because having proof of the effectiveness of a technology is meaningless if we do not also have evidence that the technology can be implemented in a cost-efficient manner.

Regarding these two gaps in the literature, what little we do know is from the small Baltic country of Estonia, which is a pioneer in employing a blockchain technology in its healthcare recordkeeping.[18, 19] While this example is encouraging, implementation of novel solutions in the United States will be much more challenging than in Estonia, because of the size and diversity of our healthcare system. Rather than wait for further research on which technologies could be the

most promising and how best to implement them, policy makers must act now to stimulate improvements in healthcare cyber-security.

This can be done through various funding mechanisms and does not require prior selection of a certain technology or implementation method. Policymakers can instead utilize an open-ended strategy by providing funding to support pilot programs that offer customized cyber-security solutions. This approach would have the added benefit of generating data to fill the above-mentioned gaps in the literature. Filling the gaps in the literature is necessary to move beyond local and regional pilot programs to state- and national-level federal policy that can make nationwide improvements to our healthcare information systems.

Alternatives

Status quo

The current data management method used in the US healthcare system is that data are stored on central servers, which users access through a local network. Transferring files between computers that are not connected to the local network requires use of portable data storage devices or sending files using an internet browser. These files can be intercepted physically, as in the case of personal data storage devices, or virtually, as in the case of files transmitted online. [17, 20] Hackers can also gain control of user accounts and access all of the data that the user permission settings allow. Once hackers obtain access, they can steal data or cripple healthcare systems by encrypting essential data.[2, 3, 6]

1. Cyber-security grants to healthcare institutions

Healthcare institutions are at a disadvantage in the cyber-security arms race, because they lack expertise and resources relevant to cyber-security. This is not surprising, given that the major responsibility of these institutions is to provide high-quality healthcare, and not follow the latest technological advances and developments in the cyber-security field.[5, 21, 22] The alternative to this dire situation is to give healthcare institutions the opportunity to compete for grants that would provide funding for cyber-security upgrades to their computer systems. These grants would allow healthcare institutions to train users on best practices, hire cyber-security experts and purchase necessary infrastructure. The rationale for this alternative is that the healthcare institutions know

their users and computer systems best, but are lacking in the resources and expertise to improve their cyber-security capabilities.

2. Cyber-security industry contracts

Instead of offering grants to healthcare institutions, funding could be made available in the form of contracts for which cyber-security companies bid. These contracts could be small, for example at the level of an individual healthcare institution, or up to the level of state healthcare system. The rationale for this alternative is that the cyber-security companies have the resources, expertise and cutting-edge skills needed to stay one step ahead of hackers, but normally contract out their services out to entities that have substantial cyber-security budgets, such as certain government agencies or other companies in the private sector.

3. Government cyber-security task force

Rather than providing funding for healthcare institutions or private companies, a government task force could be organized to implement changes at various levels across the country. The rationale for this alternative is that the task-force would have central control over the funding, personnel and execution of the cyber-security effort.

4. Public-private partnerships for cyber-security

This alternative can be thought of as a mix of the first two alternatives, in that funds would be made available to healthcare institutions and cyber-security companies that submit proposal to form partnerships designed to prevent successful cyber-attacks. The proposals would be reviewed by government officials and adequate evidence of progress towards goals outlined in the proposals would be required to renew funding or release subsequent portions of funds. This alternative represents a means of crowd-sourcing ideas for cyber-security improvements from healthcare institutions and cyber-security companies. The major rationale for this alternative is that it encompasses all of advantages of the first two alternatives and provides incentives for cooperation between healthcare institutions and cyber-security companies.

Criteria

The following criteria, which were weighted on a scale of 0.0 to 1.0. were used in considering policy alternatives:

1. Security

Preventing successful cyber-attacks is of the utmost importance to our nation, because the damage done by cyber-attacks is already immense [1, 23] and cyber-attacks projected to continue to grow both in frequency and scale.[2, 5] For this reason, the Security criterion is given the most significant weight (0.5) in this analysis.

2. Cost of implementation

Of course, we must be mindful of the monetary costs of implementing policies. Ideally, policies should be cost-effective and the cost can be thought of as the denominator by which we divide the projected impact of policy. The Cost criterion was given the second highest weight (0.3). This weight (0.3) is far less than the Security criteria (0.5), because cyber-attack prevention has economic value estimated to be on the scale of hundreds of billions of dollars.[23] Furthermore, the policies proposed in this memo would generate significant economic activity, which would bring a substantial return on investment in the form of tax revenue.

3. Scalability

The Scalability criterion was given the third highest weight (0.2), because it is important for the cyber-security pilot programs to be adaptable in terms of the size and types of health systems to which they can be applied. This criterion will also be crucial if we choose to use the same alternative for a nationwide cyber-security initiative. Such an initiative would likely need to be able to deal with healthcare institutions of various scales and types, for example small clinics in rural areas and large hospitals in city centers.

Projected Outcomes:

Outcomes / Criteria	Status Quo	Healthcare Institution Grants	Industry Contracts	Government Task Force	Public-Private Partnerships
Security (0.5)	--	+	+	+	++
Cost (0.3)	0	-	-	--	-
Scalability (0.2)	0	+	+	--	+

Key
"0" = no effect, "+" = positive effect, "-" = negative effect,
"++" = substantial positive effect, "--" = substantial negative effect

To obtain projected outcomes, the four alternatives to the status quo were assessed by the three

criteria described in the previous section. Obviously, maintaining the status quo does require any monetary investment, which was denoted in the above outcomes matrix as a zero under the Cost criterion. The status quo, however, carries with it a substantial economic cost in the form of continued cyber-attacks.[23] For this reason, the status quo was projected to have a substantial negative effect (two minuses) according to Security criterion (weight=0.5). All four of the alternatives were considered to be effective means of increasing cyber-security, but the Public-Private Partnerships alternative was thought to combine the advantages of the Healthcare Institution Grants and Industry Contracts alternatives, and was therefore given two pluses (substantial positive effect) under the Security criterion. The Government Task Force alternative received two minuses (substantial negative effect) under both Cost and Scalability criteria, weighted 0.3 and 0.2 respectively, while the other three alternatives were scored equally, with a single minus (negative effect) and a single plus (positive effect) respectively, in these criteria. The Government Task Force alternative was assessed as being the most expensive and least scalable, because the task force would not be able to rapidly adapt its personnel and resources to various scales and would have to maintain a large workforce and pool of available resources. The key to scalability and cost effectiveness of the other three alternatives is that funds could be released in the form of grants or contracts of various sizes, as deemed appropriate, while government personnel would only be needed for the review of proposals and progress reports.

Trade-offs

The status quo and Government Task Force alternative brought the fewest positive points under the criteria used for this analysis. The status quo was scored as -1 (two minuses in the Security criterion weighted 0.5, i.e. -2 x 0.5 + 0 + 0 = -1) because of the continued negative impact of cyber-attacks. The Government Task Force was also given a score of -1 (one plus in the Security criterion and two minuses in the Cost and Scalability criteria, weighted 0.5, 0.3, and 0.2 respectively, i.e. 1 x 0.5 + -2 x 0.3 + -2 x 0.2 = -1), because such a program even in the form of pilot would be cumbersome and costly. Furthermore, its lack of cost-effectiveness and inability to scale might endanger future policy decisions regarding cyber-security initiatives. These negative aspects were considered to outweigh the positive impact of increasing cyber-security that the

Government Task Force could have. The other three alternatives had similar scores under the Cost and Scalability, but the Public-Private Partnerships received the best score overall because of highest potential to positively affect cyber-security. In the end the score for Public-Private Partnerships was 0.9 (two pluses in the Security, one minus in the Cost criterion and one plus in the Scalability criteria, weighted 0.5, 0.2, and 0.3 respectively, i.e. 2 x 0.5 + -1 x 0.3 + 1 x 0.2 = 0.4), while the scores for the Healthcare Institution Grants and Industry Contracts alternatives were both 0.4 (one plus in the Security and Scalability criteria and one minus in the Cost criterion, weighted 0.5, 0.2, and 0.3 respectively, i.e. 1 x 0.5 + -1 x 0.3 + 1 x 0.2 = 0.4). In this analysis, the Security criterion was weighted so heavily, in part because the impact seen in the pilot program is hoped to provide evidence to support the creation of a national cyber-security intervention program in the future.

Decision

Based on the above-described assessment, the most effective policy would be implementation of public-private partnerships, which would provide the most cost-effective solution to cyber-attack prevention. This solution is especially effective because it engages and fosters cooperation between both healthcare institutions and cyber-security companies from the private sector. Furthermore, this solution can easily be scaled up from individual agreements between individual entities to groups of healthcare institutions and/or cyber-security companies, as needed.

Story

The goal of this memo is to convince Dr. Don Rucker, the National Coordinator for Health Information Technology, who can be reached at the 11th Annual Health 2.0 Fall Conference on October 1-4, 2017 at the Santa Clara Convention Center, that a pilot program of local public-private partnership is necessary to increase cyber-security capabilities of US healthcare institutions and provide valuable information to guide future cyber-security initiatives at the state and national levels.

References

1. Munro, D., *Data Breaches In Healthcare Totaled Over 112 Million Records In 2015.* Forbes, December, 2015. **31**.
2. Chinthapalli, K., *The hackers holding hospitals to ransom.* BMJ, 2017. **357**: p. j2214.
3. Murphy, C.J., *Healthcare Industry Held Hostage: Cyberattacks and the Effect on Healthcare Critical Infrastructure*. 2017, Utica College.
4. Terry, N., *Existential challenges for healthcare data protection in the United States.* Ethics, Medicine and Public Health, 2017. **3**(1): p. 19-27.
5. Martin, G., et al., *Cybersecurity and healthcare: how safe are we?* BMJ, 2017. **358**: p. j3179.
6. Langer, S.G., *Cyber-Security Issues in Healthcare Information Technology.* Journal of Digital Imaging, 2017. **30**(1): p. 117-125.
7. Farringer, D.R., *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals.* Seattle UL Rev., 2016. **40**: p. 937.
8. *In the Bitcoin Era, Ransomware Attacks Surge.* Wall Street Journal (Online), 2016: p. 1.
9. Linn, L.A. and M.B. Koo, *Blockchain for health data and its potential use in health it and health care related research*.
10. Morgan, R., *It's All about the Blockchain: Amid the Hoopla over Bitcoin and Other Virtual Currencies, It's the Underlying Documentation Platform That's Revolutionizing Transactions.* ABA Banking Journal, 2016. **108**(2): p. 51.
11. Azaria, A., et al., *MedRec: Using Blockchain for Medical Data Access and Permission Management.* Proceedings 2016 2nd International Conference on Open and Big Data - Obd 2016, 2016: p. 25-30.
12. Nardi, E.A., et al., *Emerging Issues and Opportunities in Health Information Technology.* Journal of the National Comprehensive Cancer Network, 2016. **14**(10): p. 1226-1233.
13. Natarajan, P., J.C. Frenzel, and D.H. Smaltz, *Demystifying Big Data and Machine Learning for Healthcare*. 2017: CRC Press.
14. Coffron, M. and F. Opelka, *Big promise and big challenges for big health care data.* Bulletin of the American College of Surgeons, 2015. **100**(4): p. 10-16.
15. Adhikari, C., *Secure Framework for Healthcare Data Management Using Ethereum-based Blockchain Technology.* 2017.
16. Yue, X., et al., *Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control.* Journal of Medical Systems, 2016. **40**(10).
17. Blake, L., et al., *Developing Robust Data Management Strategies for Unprecedented Challenges to Healthcare Information.* Journal of Leadership, Accountability and Ethics, 2017. **14**(1): p. 22.
18. Avital, M., et al., *Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future.* 2016.
19. Mettler, M. and Ieee, *Blockchain Technology in Healthcare The Revolution Starts Here.* 2016 Ieee 18th International Conference on E-Health Networking, Applications and Services (Healthcom), 2016: p. 520-522.
20. Thimbleby, H., *Cybersecurity problems in a typical hospital (and probably in all of them).* 2017.
21. Kruse, C.S., et al., *Cybersecurity in healthcare: A systematic review of modern threats and trends.* Technology and Health Care, 2017. **25**(1): p. 1-10.
22. Cuenca, J.V., *Cybersecurity Challenges in Healthcare Industries*. 2017, Utica College.
23. Gandel, S., *Lloyd's CEO: Cyber attacks cost companies $400 billion every year.* Fortune. com, January, 2015. **23**.