# 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 to lock computers or encrypt data that healthcare systems need to function[2].

**Evidence**

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[7, 8]. 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.

Cybercrimes targeting healthcare systems are becoming increasingly more frequent[9] 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{Langer, 2017 #33} [2].

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 [9, 10]. The intensity and diversity of cyber-attack targets are likely to increase with the more widespread use of electronic health records, smart devices and technologies like virtual currencies.

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 {Blake, 2017 #34}. 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. Studies of how novel technologies could be used to protect healthcare data are needed.

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{Langer, 2017 #33}, and carrying patient data on portable storage devices {Blake, 2017 #34}. 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, the impact of improvements on current technologies is limited because it depends on regulating human behavior. Human errors can be avoided through implementation of advanced technologies such as blockchain and cloud computing services. For example, portable data storage devices could be avoided if all computers had access to cloud-based data systems. In the case of suspicious emails, sender identity can be verified using an authentication system called hashing {Langer, 2017 #33}.

Two gaps

The future implementation of novel technologies should be done

Policymakers must provide guidance and support to healthcare institutions that are required by The path forward is, however, not clear and the

Global budgets for hospitals (not fee for service). Investment at the state level.

Combine blockchain and cloud.

Gaps in literature

Examples of solutions exist in the literature, and practical demonstrations of blockchain in healthcare have been presented [16], but the literature does not include any systemic reviews focusing on solutions to the healthcare information security crisis. Notably, Estonia is a pioneer in the implementation of blockchain in healthcare recordkeeping [17, 18]. Information on the progress towards this goal in other countries is lacking.

**Alternatives**

**Criteria**

**Story**

The goal of this memo is to convince the US Health and Human Services Department that a nationwide vaccine campaign is necessary to increase immunization rated among American adults, and provide information on whether such vaccine campaigns should be compulsory or voluntary.

Table 1. A basic comparison of voluntary and compulsory vaccine campaign types

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Criteria | Status Quo  Hospitals responsible | Private solutions – grants for private institutions | Government | Private-Public Partnership |
| Cost | - | + | ++ | + |
| Security | -- | + |  |  |
| Efficiency |  |  |  |  |

References

1. Alam, M.J. and M.F. Rahman, *Herd Immunity: A Brief Review.* Mymensingh Med J, 2016. **25**(2): p. 392-5.

2. Adashek, J., *When Herd Immunity Is the Only Protection.* Am J Public Health, 2016. **106**(6): p. 965.

3. Sobo, E.J., *What is herd immunity, and how does it relate to pediatric vaccination uptake? US parent perspectives.* Soc Sci Med, 2016. **165**: p. 187-95.

4. Tan, L., *Adult vaccination: Now is the time to realize an unfulfilled potential.* Human Vaccines & Immunotherapeutics, 2015. **11**(9): p. 2158-2166.

5. Williams, W.W., et al., *Surveillance of Vaccination Coverage Among Adult Populations - United States, 2014.* MMWR Surveill Summ, 2016. **65**(1): p. 1-36.

6. Williams, W.W., et al., *Surveillance of Vaccination Coverage among Adult Populations - United States, 2015.* MMWR Surveill Summ, 2017. **66**(11): p. 1-28.

7. Friesen, P., et al., *Rethinking the Belmont Report?* Am J Bioeth, 2017. **17**(7): p. 15-21.

8. Miracle, V.A., *The Belmont Report: The Triple Crown of Research Ethics.* Dimens Crit Care Nurs, 2016. **35**(4): p. 223-8.

9. Department of Health, E., et al., *The Belmont Report. Ethical principles and guidelines for the protection of human subjects of research.* J Am Coll Dent, 2014. **81**(3): p. 4-13.

10. Adams, D.P. and T.P. Miles, *The application of Belmont Report principles to policy development.* J Gerontol Nurs, 2013. **39**(12): p. 16-21.

11. Sims, J.M., *A brief review of the Belmont report.* Dimens Crit Care Nurs, 2010. **29**(4): p. 173-4.

12. *Protection of human subjects; Belmont Report: notice of report for public comment.* Fed Regist, 1979. **44**(76): p. 23191-7.

13. Beauchamp, D.E., *Public health as social justice.* Inquiry, 1976. **13**(1): p. 3-14.