Editorial Preface

Health Information Security:
Paper Records May Still Be a Good Thing

Steven Walczak, School of Information and Florida Center for Cybersecurity, University of South Florida, Tampa, FL, USA

Electronic health records (EHRs) are being widely adopted worldwide (Wager, Lee, and Glaser, 2013) as a means to improve communication and workflow efficiencies, reduce costs, and ultimately hopefully to improve the quality of care received by patients (King et al., 2014). However the advent of EHRs introduced a new cyber-based attack surface for compromise of medical information and services including ransomware, hacking and other data breaches, and denial of service attacks, all of which can be devastating to medical providers and their patients (Kruse et al., 2017). Research has reported that healthcare is the industry which suffers from the greatest number of data breaches and corresponding costs (Liu, Musen, & Chou, 2015).

The integration of new medical technologies which contain or transmit medical data into the healthcare information platform, such as wearable and embedded devices (e.g. pacemakers and insulin pumps) and mobile devices (e.g. smart phones with patient portal apps or home monitoring devices), continues to expand the cyber-attack surface. It is estimated that Internet of Things (IoT) connected devices will exceed 50 billion before the end of the decade (Swan, 2012).

Let's take a step back for a moment. Healthcare organizations should certainly be performing as and counted as highly reliable organizations (HROs). Roberts (1989) indicated that the United States among other economically developed countries feels pressure to adopt new technologies, including information technologies like EHRs, to become more reliable and handle ever increasing demand. This is certainly true in the United States with payments for services to Medicare and Medicaid patients tied to successful completion of advancing levels of information technological implementations to achieve meaningful use (Held, 2016). Technological systems, including healthcare information systems, are highly interdependent and problems in any part of the system may propagate to other parts of the system (Roberts, 1989). As an example, a recent cyber-attack against the electronic systems at Northern Lincolnshire and Goole NHS Foundation Trust forced the cancelation of hundreds of operations at multiple area hospitals for over two days and also affected general practitioners in the area since electronic requests and reporting of lab results were unavailable (BBC, 2016; Linconite, 2016).

Healthcare systems must be able to continue uninterrupted operations even when EHRs and other healthcare information technology becomes unavailable due to cyber-attacks or for any other reason, or as Roberts (1989) puts it systems must still be managed "even when the electricity goes off." At a recent information security conference (at the time of this writing), a panel stated that there is a zero percent chance of defending against a determined hacker and that organizations, including healthcare organizations, must learn to be able to "continue in a degraded manner" (Charney et al., 2016).

A non-medical example comes from the cyberwarfare attack against Ukraine's power grid. Immediately following the cyber-attack power was shut down in eight provinces within the Ivano-

Frankivsk region affecting over 80,000 customers (Zetter, 2016a). However, unlike the multi-day shutdown of the Lincolnshire hospital noted above, power was restored in 1 to 6 hours due to technicians reverting to manual control of breakers in the system (Zetter, 2016b). These technicians used essentially manual systems to immediately overcome the damage being done by the cyber-attack. The above example also points out that healthcare systems and services may be affected by cyber-attacks against other industries, in particular the power-grid, which could cause difficulty in accessing patient information and other health service problems (Klinger, Landeg, & Murray, 2014).

What can hospitals and other healthcare providers learn from the Ukranian power service? If healthcare continues to invest completely in electronic information systems, then they must be willing to pay the price when cyber-attacks occur. A more manual or paper based system may also be threatened via various threats including: fire, natural disasters, and theft. However, paper-based records do not require a properly functioning electronic information system. The purpose of this editorial is not to say that EHRs should be abandoned and revert back to paper-based systems, but that having a paper back-up is not necessarily a bad idea from a disaster (in this case a cyber-attack disaster) recovery perspective. Previous research has already documented well the benefits of EHRs and other information technology to clinical efficiency (King et al., 2014; Persell et al., 2011; Schooley et al., 2016) and quality of care (Middleton et al., 2013). Paper medical records have other issues that may affect the quality of care, such as reading physician handwriting (Shachak et al., 2009), but if pertinent paper records can be maintained in parallel to EHR records this will provide a means for healthcare providers to continue to provide service, though in a degraded manner, even when their information systems are completely offline to deal with a cyber-attack.

Implementing a parallel paper record system has other significant issues, including the need for a much larger storage space and physical security of the paper records. Research is needed to investigate ways, such as a parallel paper system, to enable healthcare providers to rapidly and effectively overcome cyber-attacks against their information systems. Investigations should examine how data recency may be maintained by non-electronic information back-ups, as well as storage/space requirements of such systems and effective methods for transitioning between an electronic information system that may be currently offline to non-electronic information usage.

Addendum: As I was writing this article, actually just after having submitted it to the editorial office at the publisher, a new global cyber-attack occurred. On Friday 12 May 2017, the WannaCry ransomware started propagating around the world, targeting various industries in different countries globally. The National Health Service in the UK was hit and forced physicians to cancel surgeries and thousands of non-emergency appointments and also send emergency patients to other facilities (Perlroth & Sanger, 2017). This latest attack against the healthcare (and other) industry “crippled the health system’s ability to treat patients” (Young, 2017).

Steven Walczak
Editor-in-Chief
JOEUC

REFERENCES

BBC. (2016). Lincolnshire operations cancelled after network attack. Retrieved March 4, 2017 from http://www.bbc.com/news/uk-england-humber-37822084

Charney, S., Clancy, M., Coviello, A., Gorman, P., & McConnell, M. (2016, October 25). Comments made during panel discussion on Emerging Cybersecurity Threats and Mitigation Strategies. In *Proceedings of the Florida Center for Cybersecurity 3rd Annual Conference*, Tampa, FL.

Held, K. S. (2016). New Medicare Payment Rule: A Trojan Horse for Government Takeover. *Journal of American Physicians and Surgeons*, *21*(3), 87–90.

King, J., Patel, V., Jamoom, E. W., & Furukawa, M. F. (2014). Clinical benefits of electronic health record use: National findings. *Health Services Research*, *49*(1, Part 2), 392–404. doi:10.1111/1475-6773.12135 PMID:24359580

Klinger, C., Landeg, O., & Murray, V. (2014). Power outages, extreme events and health: A systematic review of the literature from 2011-2012. *PLoS Currents*, *6*. doi:10.1371/currents.dis.04eb1dc5e73dd1377e05a10e9edde673

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. doi:10.3233/THC-161263 PMID:27689562

Linconite. (2016). Delays still expected at Lincolnshire hospitals after cyber attack. Retrieved March 4, 2017 from http://thelincolnite.co.uk/2016/11/delays-still-expected-at-lincolnshire-hospitals-cyber-attack/

Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. *Journal of the American Medical Association*, *313*(14), 1471–1473. doi:10.1001/jama.2015.2252 PMID:25871675

Middleton, B., Bloomrosen, M., Dente, M. A., Hashmat, B., Koppel, R., Overhage, J. M., & Zhang, J. et al. (2013). Enhancing patient safety and quality of care by improving the usability of electronic health record systems: Recommendations from AMIA. *Journal of the American Medical Informatics Association*, *20*(e1), e2–e8. doi:10.1136/amiajnl-2012-001458 PMID:23355463

Perlroth, N., & Sanger, D. E. (2017). Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool. *New York Times*. Retrieved from https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=1

Persell, S. D., Kaiser, D., Dolan, N. C., Andrews, B., Levi, S., Khandekar, J., & Baker, D. W. et al. (2011). Changes in performance after implementation of a multifaceted electronic-health-record-based quality improvement system. *Medical Care*, *49*(2), 117–125. doi:10.1097/MLR.0b013e318202913d PMID:21178789

Roberts, K. H. (1989). New challenges in organizational research: High reliability organizations. *Organization & Environment*, *3*(2), 111–125.

Schooley, B., Walczak, S., Hikmet, N., & Patel, N. (2016). Impacts of mobile tablet computing on provider productivity, communications, and the process of care. *International Journal of Medical Informatics*, *88*, 62–70. doi:10.1016/j.ijmedinf.2016.01.010 PMID:26878764

Shachak, A., Hadas-Dayagi, M., Ziv, A., & Reis, S. (2009). Primary care physicians' use of an electronic medical record system: A cognitive task analysis. *Journal of General Internal Medicine*, *24*(3), 341–348. doi:10.1007/s11606-008-0892-6 PMID:19130148

Swan, M. (2012). Sensor mania! The internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator Networks*, *1*(3), 217–253. doi:10.3390/jsan1030217

Wager, K. A., Lee, F. W., & Glaser, J. P. (2013). Appendix C: International Adoption and Use of Health Information Technology. In K. A. Wager, F. W. Lee, & J. P. Glaser (Eds.), *Health Care Information Systems: A Practical Approach for Health Care Management* (pp. 665–680). San Francisco: Jossey-Bass.

Young, A. (2017). Health Organizations: What You Need to Know About the NHS Cyberattack. *Cisco Blogs*. Retrieved from https://blogs.cisco.com/healthcare/healthcare-organizations-what-you-need-to-know-about-the-nhs-cyberattack

Zetter, K. (2016a, January 20). Everything we know about the Ukraine’s power plant hack. *WIRED*.

Zetter, K. (2016b, March 3). Inside the cunning, unprecedented hack of Ukraine’s power grid. *WIRED*.