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 Ukrainian 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


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