Surgical Research Review

Protecting patient information in the information age: Mission impossible?

Benjamin N. Gayed, MD, *and* **Nicholas J. Zyromski, MD,** *Indianapolis, IN*

From the Department of Surgery, Indiana University School of Medicine, Indianapolis, IN

We live in the information age: The click of a mouse, a tweet, or an email puts us in touch with friends and colleagues from across the street to across the globe. Society is more connected than ever before—great news from a communication standpoint, but terrible news considering the clinical/research mandate to protect confidential patient information. Consider, for example, this real-life, terrifying, "true crime" story:

> *Dr. X, a PGY3 surgical resident, was comfortably 2 months into his research fellowship when his car was burglarized; the window was broken and his laptop was stolen. Beyond the indignation (and expense) of a broken car window and replacement of his computer, Dr. X realized that the computer contained research spreadsheets that included patient data. Several thoughts flashed through his mind: "What data did he have? Which data were he allowed to have? How were the data protected, and was this protection adequate? What to do now? What happens now (To the patients? To him? To the department? To the University?).*
>
> *The computer was password protected, but not encrypted. The databases contained records of >3,000 patients, including, unfortunately, a few Social Security numbers. Within days, Dr. X found himself on conference calls with lawyers and compliance officers from the hospital system and university administration. The United States Department of Health and Human Services (HHS) was notified, the state attorney general was notified, and the institutional review board suspended his research protocol. The surgery department sent letters to each of the patients documenting their lost data. Dr. X suffered a degree of infamy among his resident peers as well as the staff because the story was reported in his local newspaper. So far, no one has offered to pay for the car window or to replace Dr. X's computer.*

Loss of protected health information (PHI) has real and potentially catastrophic consequences. Contemporary technologic advances make communication (and data transfer) incredibly easy; the flip side of this coin is that data protection is exponentially more difficult. Although this specific example involves research data, protection of health information is just as crucial in clinical practice; communication of public health information (often electronic) occurs daily in every medical practice. Awareness represents the first step toward a solution. Therefore, the purpose of this review is to highlight the problem of data protection by (1) reviewing the contemporary scope of the problem, (2) identifying potential consequences of data loss, (3) defining which data must be protected, (4) highlighting the most important ways to protect personal health information, and (5) detailing the basic steps to take in the case of data loss. Although these recommendations are generally applicable globally, this document is not intended to be a comprehensive blueprint for data security. The landscape is changing rapidly, and individual institutional security policies are critically important local resources.

SCOPE OF THE (DATA LEAK) PROBLEM

In the United States, healthcare providers are required to report all breaches of inadequately protected patient information to the HHS. The HHS then publishes details about all incidents involving ≥500 individuals to its website.[1] As of December 2011, barely 2 years after reporting became required, the HHS has published 380 reports

Accepted for publication April 12, 2012.

Reprint requests: Nicholas J. Zyromski, MD, Department of Surgery, Indiana University School of Medicine, 535 Barnhill Dr. RT 130, Indianapolis, IN 46202. E-mail: nzyromsk@iupui.edu.

Surgery 2013;153:145-9.

0039-6060/$ - see front matter

doi:10.1016/j.surg.2012.04.004

including >18 million compromised patient files from 47 states, the District of Columbia and Puerto Rico, averaging out to an astonishing number: >23,000 patient files are lost per day.

Considering breaches in data beyond those in medicine provides further insight into the scope of this problem. The Leaking Vault 2011[2] is the largest report of data breaches to date, identifying publically reported incidents worldwide spanning the years 2005 to 2011. This report noted a plateau in the overall incidence of data breaches between 2008 and 2010; however, over the same time period, the medical industry subsector showed an increase in incidence in data breached from 160 in 2010 to 403 in 2011. These data should be interpreted in light of the HHS reporting requirement beginning at the end of 2009. Although trends in reporting incidence continue to emerge, one very clear fact is that data loss is occurring at an alarming rate, especially within the medical field.

CONSEQUENCES OF DATA LOSS

Financial penalties. Loss of PHI is subject to financial penalty at federal, state, and local levels. The most important factors in determining penalties are the degree of negligence leading to the data loss, amount of harm done, and whether the breach was corrected within 30 days. Specific penalties are adjudicated by the Secretary of HHS, through the Office of Civil Rights (OCR). To date, the OCR has entered into a number of "Resolution Agreements"[3] and has issued 1 civil money penalty,[4] establishing a precedent of penalizing institutions rather than individuals. The OCR has several hundred investigations still open at this time.[5] Levying penalties against institutions is practical; institutions can pay large penalties, and it is more efficient to penalize institutions expecting, that they in turn will ensure compliance in their workforces. As the current law is written, however, healthcare providers may be liable as individuals.

States may issue fines separate from any levied by the HHS. Laws vary between states—penalty amounts and enforcement vary as well. Importantly, loss of PHI from residents of multiple states gives each of those states' attorneys general the authority to separately investigate and penalize covered entities for data breaches. Civil suit may also be brought on behalf of the individuals within each attorney general's own jurisdiction.

In addition, civil lawsuits may be filed against any covered entity by any individual whose data were compromised. Again, civil lawsuits are more likely to be brought against corporations than individual providers, but the statue's language allows individuals to be named in civil lawsuits.

Criminal penalties. Individuals who "knowingly obtain or disclose individually identifiable health information" may be punished with up to 1 year in prison. Precedent exists for imprisonment after Health Insurance Portability and Accountability Act (HIPAA) violations[6]; however, criminal prosecution is presently reserved for egregious, willful violations of HIPAA standards.

Professional consequences. Confidentiality is a fundamental component of the physician–patient relationship, but this confidentiality also extends beyond individual interactions to include an entire community. Data loss, which is a breach in confidentiality, affects a community's perception of the care with which their information is handled, regardless of how the breach occurred. For example, in 2006, a man obtained protected information of several individuals who had donated blood to the American Red Cross in Philadelphia. He then used the information to obtain loans and cash counterfeit checks adding up to approximately $800,000. The crime damaged public perception of the Red Cross—blood donations decreased, and 2 corporate donation centers stopped having blood drives entirely.[7]

Identity theft. The specter of identity theft has provided the major impetus driving government regulation of patient privacy and data security. Theoretically, the risk of identity theft is simple to understand, and many reports document crimes of identity theft which have been prosecuted successfully.[8-11] The data regarding the actual impact of identity theft, however, are highly variable. According to a 2011 report from the Government Accountability Office, the IRS reported claims of 245,000 identity fraud in 2010, up from 52,000 in 2008, representing a 471% increase in 2 years.[12] Many of these data come from surveys performed by companies selling identity protection services. A report entitled "Sex, Lies and Cyber-Crime Surveys"[13] explored this issue and determined that estimates of cybercrimes—the feared result of identity theft—may be exaggerated substantially by inexact methodologies of data collection.

Whatever the precise risk of an identity crime resulting from a data breach may be, the possibility is real and persists indefinitely. Perhaps the most frightening truth about this type of crime is that stolen personal information can be used maliciously years later. A substantive percentage of people reporting identity theft crimes did not recognize that fraud occurred until >2 years after the theft.[11] In fact, because credit monitoring is 1 of the few ways to discover when identity theft has occurred, identity thieves target knowingly children's information, knowing no credit check is likely to occur for years to come.