Journal of Business & Technology Law

Volume 8 | Issue 1 Article 5

Dependence on Cyberscribes - issues in e-Security

Thomas R. McLean

Alexander B. McLean

Thomas R. McLean* and Alexander B. McLean**

Dependence on Cyberscribes — Issues in e-Security

From the Book of Thomas & Alexander: God said "01010110101111"
and there was e-security; and "Happy are the Cyberscribes
for they shall inherit the control of e-documents."

Abstract

A paucity of e-security exists in the world. The origins of this problem can be traced all the way back to Ancient Egypt, when literacy was held exclusively by a class of scribes. Although the Egyptians attempted to deter scribe corruption with harsh penalties, such corruption only ceased to be a problem when literacy became widespread in the Greek and Roman cultures.

The modern lack of e-security, which is a cause of medical identity theft (MIT), can be traced to the fact that computer and computer code literacy is held exclusively by a class of "cyberscribes." We, as a society, have attempted to deal with our illiteracy problem by enacting the HITECH Act, which contains harsh penalties for those individuals who gain unauthorized access to protected health information (PHI). So the question now becomes, will a strategy that failed in the 21st century B.C.E. work in the 21st century C.E.?

To answer this question, this Article begins with an overview of computer systems and the tools available to corrupt cyberscribes to defeat e-security systems. The Article next examines the motivation for hackers to commit MIT. MIT is so financially lucrative that the penalties under HIPAA/HITECH create no real disincentives for hackers. Accordingly, the subsequent part of this Article reviews the HITECH Act, the Federal Wiretap Act, and the Stored Communications Act. Collectively, these laws can potentially create harsh penalties for anyone who gains unauthorized access to PHI. Unfortunately, loopholes in these laws mean that they are unlikely to deter corrupt cyberscribes from hacking medical records. Moreover, modification of these laws to make it clear that a conviction for hacking an

* M.D., J.D., FACS, ESQ.; CEO, Third Millennium Consultants, LLC, Shawnee, KS; tmclean@isp.com.

** B.S.; Research Associate, Third Millennium Consultants, LLC, Shawnee, KS; first-year law student at University of Texas (Austin) School of Law; amclean89@gmail.com.

electronic medical record will result in a guaranteed ten-year prison sentence is still unlikely to deter hackers. The reason: the prosecution of hackers is difficult.

So, if we seek a solution to cyberscribe corruption in our time, we need to study the Greek and Roman times when a change in societal conditions minimized the opportunity for corrupt scribes to game the system. In our modern times, changing our healthcare system to one of universal access would destroy the obscene profit associated with MIT and thereby destroy the biggest incentive available to hackers to breach e-security systems to gain unauthorized access to PHI.

I. Introduction

A general lack of e-security exists in today's world, and this lack has real world consequences in the health care sphere.[1] For example, in 2011 the Department of Health and Human Services (DHHS) fined Cignet Health $4.3 million for violating the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule,[2] and settled with the Massachusetts General Hospital for $1 million after the latter lost a number of patients' personal electronic data.[3] Interestingly, these two healthcare providers may have gotten off easy. Depending on how breach of e-security damages are calculated,[4] a healthcare provider's average damages from an e-security breach have been reported to range from $5.5 million to $7.2 million in

1. This Article is being written for attorneys who have a minimal to a moderate understanding of computers and electronic devices. As used herein, "e-security" contemplates all human, hardware, and software techniques that secure transmitted or stored e-documents from unauthorized access.

2. Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996); *see* News Release, HHS Imposes a $4.3 Million Civil Money Penalty for Violations of the HIPAA Privacy Rule, Dep't of Health & Human Servs. (Feb. 22, 2011), *available at* www.hhs.gov/news/press/2011pres/02/20110222a.html.

3. *See* News Release, Massachusetts General Hospital Settles Potential HIPAA Violations, Dep't of Health & Human Servs. (Feb. 24, 2011), *available at* www.hhs.gov/news/press/2011pres/02/20110224b.html. *See generally* Arthur E. Peabody, Jr. & Lucy L. Thompson, *HITECH: The First Federal Data Breach Notification Law*, *in* Data Breach and Encryption Handbook 128–29 (Lucy Thompson ed., 2011) [hereinafter Data Breach Handbook] (describing the civil and criminal penalty allowances granted to DHHS under HIPAA); *HIPAA Compliance and Data Protection*, Intronis 1–2 (2011), http://www.intronis.com/resources/pdf/whitepapers/HIPAA-compliance-WP.pdf (laying out the HIPAA requirements and recommending methods for compliance).

4. Total calculated damages depend on whether the data includes losses from administrative penalties, lawsuits, or damage to the business organization's reputation. A detailed discussion on how damages arising from an e-security breach are calculated is beyond the scope of this Article. *See* Ponemon Inst., 2011 Cost Of Data Breach Study 3, 17 (Mar. 2012), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US (determining the cost of a data breach is based upon many different elements, including: the severity of the breach, legal costs, lost business, and industry); Arthur E. Peabody, Jr. & Renee A. Abbott, *The Aftermath of Data Breaches: Potential Liability and Damages*, *in* Data Breach Handbook, *supra* note 3, at 31–35 (describing growing financial risks of data breaches which businesses must prevent and the various ways data breaches have cost customer businesses).

recent years.[5] At the extreme high end, e-security breaches may ultimately cost healthcare business entities billions of dollars in damages.[6] As for patients, neither the rich nor the poor appear to be immune from e-security breaches that compromise personal health information.[7] While e-security breaches can be secondary to provider's negligence,[8] increasingly e-security breaches are the planned works of malicious cyberscribes.[9] For example, hackers gained control of 8.3 million medical records from the Commonwealth of Virginia's prescription drug database and then held these records for ransom.[10]

Thus, we find ourselves with a modern version of an ancient problem. During the time of the Ancient Egyptian pharaohs, literacy was held exclusively by a class of scribes.[11] These ancient scribes had a conflict of interest: from time to time, scribes gained personal advantages by corrupting written documents, a crime that was difficult to detect because only scribes were literate.[12] The problem of corrupt

5. PONEMON INST., *supra* note 4, at 6, fig. 2 (determining the cost of data breaches from 2005 to 2011); *cf. id.* at 7, fig.4 (showing per capita cost of breaches across industries, of which healthcare is one of the highest).

6. *See First-of-its-Kind Study Reveals the Reach and Severity of Medical Identity Theft in the United States*, BUS. WIRE (Mar. 3, 2010, 2:00 PM), *available at* http://www.businesswire.com [hereinafter *Medical Identity Theft Study*] (estimating that medical identity theft costs healthcare businesses approximately $20,000 per victim, for a combined industry cost of $28.6 billion). In medical identity theft cases plaintiffs are required to prove that damages arise from actual harm incurred, and not the possibility of future harm. *See* Paul v. Providence Health Sys.-Or., 240 P.3d 110, 110–14 (Or. Ct. App. 2010), *aff'd on other grounds*, 273 P.3d 106 (2012).

7. *See* Andrew Porter & James Kirkup, *My Son's Medical Records Were Hacked, Says Brown*, DAILY TELEGRAPH (UK), July 12, 2011, at 1 (describing British Prime Minister Brown's statement that his family medical records were hacked); *see also Medical Identity Theft Study*, *supra* note 6 (claiming almost 1.5 million Americans have had their medical identities stolen).

8. PONEMON INST., *supra* note 4, at 10 (describing that system breaches frequently occur after a mobile device storing this information is lost or stolen); *see, e.g.*, Joseph De Avila, *City News: Data are Stolen from Hospitals*, WALL ST. J., Feb. 12, 2011, at A21 (describing the theft of 1.7 million medical data records from a New York City hospital that occurred when the magnetic data tapes were left in an unlocked car); *see id.* at 8 (stating that negligent employees are most often to blame for the cause of these breaches).

9. JEROME P. BJELOPERA & KRISTIN M. FINKLEA, CONG. RESEARCH SERV., R41547, ORGANIZED CRIME: AN EVOLVING CHALLENGE FOR U.S. LAW ENFORCEMENT 10 (2012); *see* Lucy L. Thompson, *Cybercrime and Escalating Risks*, *in* DATA BREACH HANDBOOK, *supra* note 3, at 3–7 (identifying that the sophistication and scope of cyber-attacks indicates criminal organizations are organizing these attacks); *see also* PETER SOMMER & IAN BROWN, FUTURE GLOBAL SHOCKS: REDUCING SYSTEMIC CYBERSECURITY RISK 30–31 (Jan. 14, 2011), *available at* http://www.oecd.org/sti/futures/globalprospects/46889922.pdf (explaining that "criminal gangs" are responsible for the growing criminal activity on the Internet).

10. Brian Krebs & Anita Kumar, *Hackers Want Millions for Data on Prescriptions*, WASH. POST, May 8, 2009, at B1.

11. *See generally* JAMES GLEICK, THE INFORMATION: A HISTORY, A THEORY, A FLOOD 43 (2011) (stating that King Hammurabi "was probably the first literate king" of Mesopotamia).

12. *See Life in Ancient Egypt, Daily Life: Scribes*, CARNEGIE MUSEUM OF NATURAL HISTORY, http://www.carnegiemnh.org/online/egypt/scribes.html (last visited Sept. 30, 2012) (explaining that scribes created and controlled all the written documents in Ancient Egyptian Government); *see also* André Dollinger, *Law and Order: The Criminals and their Crimes*, RESHAFIM.ORG (Sept. 30, 2012, 8:32 PM), http://www.reshafim.org.il/ad/egypt/law_and_order/index.html (explaining that scribes acted as judges to read historical records, and often were susceptible for bribes or hesitant to punish other scribes); *cf.* Dan Ariely, *Why*

scribes was mitigated by ancient societies in two ways. First, harsh penalties (such as being buried alive) were given to any scribe caught keeping crooked books.[13] The second solution to scribe corruption was a change in societal conditions.[14] By the time the Greeks and Romans rose to power, literacy was widely disseminated.[15] Accordingly, during the Greek and Roman times the problem of the corrupt scribe faded away.[16] Indeed, literacy had become so pervasive that the Romans found it necessary to encrypt documents to protect state secrets.[17]

Yet, during the last generation of the 20th century C.E. the corrupt scribe problem was resurrected. During this period, the American society developed a dependence on computers.[18] Few individuals in modern America (and other developed countries) understand the basic principles of how computers operate; and still fewer individuals can read computer code.[19] Widespread computer use combined with computer code illiteracy means that our modern American society has become dependent on a class of cyberscribes[20] who can read

We Lie, Wall St. J., May 26, 2016, at C1 ("[W]e want to benefit from cheating and get as much money and glory as possible; on the other hand, we want to view ourselves as honest, honorable people.").

13. *See* Dollinger, *supra* note 12 (explaining the punishments for scribes caught for falsifying their writings were "savage"). Of course punishment of the crooked scribe must have raised evidentiary issues because an expert witness scribe — someone who was an economic competitor to the defendant scribe — would have been needed to provide testimony on the accuracy of the defendant's writings. *Cf. id.*

14. *See generally* Gleick, *supra* note 11, at 43 (describing that Hammurabi's promotion of literacy throughout Mesopotamia government created "a new method of civil direction").

15. William V. Harris, Ancient Literacy 9 (Harvard U. Press paperback ed. 1991) ("[R]eading and writing were learned by a great part of the population not only in Rome but in the whole Roman Empire.").

16. *See* Albert C. Leighton, *Secret Communication Among the Greeks and Romans*, 10 Tech. & Culture 139, 140–42 (1996) (describing how the dissemination of literacy in ancient Rome and Greece diminished the power of groups which formally had social power, which arose from the knowledge of the contents within the written articles). Additionally, for a brief period the monopoly on literacy reappeared in Europe around approximately 1000 C.E. During this time, the only written language in Europe was Latin and only members of the Roman Catholic Church's clergy understood written documents. *See* Rudi Volti, Society and Technological Change 214 (6th ed. 2009) (discussing the Liturgy's withholding written sources of Latin text up to the fifteenth century in order to maintain power and control).

17. *See* Leighton, *supra* note 16, at 148 (stating that the Roman Government developed methods of document encryption, including the Caesar Cypher, "because of the increased sophistication of the literate public it was no longer possible to trust in the security of letters alone, new methods had to be developed to insure secrecy").

18. *See* Misha Glenny, Dark Market: Cyberthieves, Cybercops and You 1 (Alfred A. Knopf ed., 2011) ("[Humanity] ha[s] developed a dangerous level of dependency on networked systems in a short space of time.").

19. *See* Dan L. Burk, *Patenting Speech*, 79 Tex. L. Rev. 99, 106–07 (2000) (citing Karn v. United States Dep't of State, 925 F.Supp. 1, 9 (D.D.C. 1996)) (noting that some courts accept the conclusion that "computer source code, even though incomprehensible to the majority of people, is comprehensible to other programmers").

20. *See* Dan Greer, Jr., *Cybersecurity and National Policy*, 1 Harv. Nat'l Sec. J. 203, 203 (2010) (describing that currently e-security is the "province of the 'The Few'" who understand the complex cyber code and describing the growing trend of "The Few" computer literate individuals who exploit the public's unawareness of security and not taking efforts to protect it).

and write in machine code,[21] produce programs[22] or manipulate the esoteric multilayer Internet Protocol (IP).[23]

In healthcare specifically, cyberscribe dependency is most clearly manifested in the lack of knowledge that patients and doctors have regarding the inner workings of Electronic Medical Record (EMR) systems[24] and of the workings of computerized Electronic Medical Devices (cEMDs).[25] The inner workings, especially with respect to e-security, of EMRs and cEMDs are so dependent on computer code that it would be a mistake not to realize that for all of our technology, we are still facing an ancient problem.[26] Just as ancient scribes used literacy to gain personal advantages, it is reasonable to anticipate that modern cyberscribes will attempt to use their

21. Machine code is a string of zeros and ones that provides the ultimate instructions to a computer. Even for cyberscribes, working in machine code is difficult. *See* Klaus M. Schmidt & Monika Schnitzer, *Public Subsidies for Open Source? Some Economic Policy Issues of the Software Market*, 16 HARV. J.L. & TECH. 473, 475 (2003) ("[M]achine code, which is just a sequence of zeros and ones. . . . [i]s very difficult to read for humans . . . and time-consuming to retranslate into source code."); *see also* Paul I. Kravetz, *Copyright Protection of Computer Programs*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 41, 45 (1998) (describing the three levels of computer language, in ascending difficulty: high level, assembly language, and machine language); *id.* ("Programs written in assembly language are usually more difficult for programmers to understand than high level languages"). Low order computer language codes like assembly language produce very efficient code that can be easily transmitted, but these lower-order languages require the cyberscribe to keep track of a large number of details. *See generally* DOUGLAS GRAER, THE INTRINSIC HOLE IN INFORMATION SECURITY 2 (Aug. 15, 2002), *available at* http://www.sans.org/reading_room/whitepapers/securecode/intrinsic-hole-information-security_25 (distinguishing types of computer languages, specifically "C Language," a midlevel language that does not require a high level of knowledge or skill and therefore "bridges the gap between hard to use assembly language and user friendly high level languages").

22. Programs are written in computer languages. *See* Kravetz, *supra* note 21, at 46 ("Programs written in either high level or assembly languages are referred to as written in source code."); *cf.* KEVIN MITNICK & WILLIAM L. SIMON, GHOST IN THE WIRES: MY ADVENTURES AS THE WORLD'S MOST WANTED HACKER 54 (2011) [hereinafter GHOST] (conveying a personal account of a hacker's preference for lower-level coding).

23. Currently, Internet Protocol is used to transmit much of the data that passes through the Internet by joining "tens of thousands of networks to communicate via IP." PATRICK CICCARELLI ET AL., NETWORKING BASICS 55 (2d ed. 2011). In the future, EMRs are likely to be electronically transmitted by the Nationwide Health Information Network's Direct Project, which uses a variation of the Simple Mail Transport Protocol, the standard protocol for sending email messages over Internet Protocol. THE DIRECT PROJECT, THE DIRECT PROJECT OVERVIEW 9–11 (Oct. 11, 2010), *available at* http://directproject.org/content.php?key=overview.

24. An EMR contains the information that is available to healthcare providers and patients. Additionally, "[l]ike any other computer record" an EMR "generates metadata" which "is an automatically generated computer record that certifies how an electronic document (e-document) has been manipulated." Thomas R. McLean, *EMR Metadata: Uses and Discovery*, 18 ANNALS HEALTH L. 75, 75 (2009). While a detailed discussion of metadata is beyond the scope of this Article, attorneys need to be aware that metadata is required for the formal authentication of an EMR. *Id.* at 86.

25. cEMDs refers to medical devices that use telemedicine or computer assisted devices that allow either physicians or surgeons to treat their patients. Thomas R. McLean, *Cybersurgery—An Argument for Enterprise Liability*, 23 J. LEGAL MED. 167, 168 (2002) (defining cEMDs and examining the legal issues these devices create, specifically liability, from emerging precedence). For the most part, these devices are beyond the scope of this Article.

26. *See* GLENNY, *supra* note 18, at 2 (describing the current social organization in which a "minuscule elite," commonly referred to as hackers, "has a profound understanding of technology that everyday directs our lives more intensively and extensively, while most of the rest of us understand absolutely zip"); *see also* sources cited *supra* note 21.

computer code literacy to gain personal advantages. Indeed, the growing number of security breaches within the healthcare industry may indicate that the percentage (as well as the actual number) of EMR e-security breaches will continue to increase in the next few years as techniques are developed to decrease the incidence of e-security breaches arising from negligence.[27]

So how will the United States solve the ancient problem of the corrupt cyberscribe? Will it be by severe punishment or by a change in societal conditions? To answer this question, this Article examines the economic and legal incentives given to hackers. However, given the ubiquitous nature of computers and the Internet in our private and commercial lives, the scope of this Article will have relevance to more than those individuals working in the healthcare field: any attorney who handles confidential e-documents should find the discussion herein of e-security interesting.[28] Part II of this Article provides an overview of the "physics" of e-security (i.e., the nature of computer systems, malware, and encryption).[29] Part III examines the economic factors that seem destined to substantially increase the incidence of unauthorized access to EMRs and cEMDs, and drive medical identity theft.[30] Part IV then examines the laws governing e-security to determine whether such laws are likely to deter corrupt cyberscribes.[31]

This Article reaches two conclusions. First, as we move towards a healthcare system based on the ubiquitous presence of EMRs, corrupt cyberscribe activity will increase because the existing laws create, at best, a mild deterrence to such activity.[32] Second, if we are truly interested in making EMRs secure, we need to change societal conditions that allow hackers to flourish.[33] In the case of healthcare, moving to a healthcare system that has universal access would minimize hacking because universal access is likely to destroy the black market value of personal health information.[34]

27. PONEMON INST., *supra* note 4, at 21 (demonstrating that in 2011 the healthcare industry comprised 10% of the total security breaches across all industries); *see also* Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, *in* DATA BREACH HANDBOOK, *supra* note 3, 20–21 (stating the number of stolen EMRs has increased from 2,741,101 in 2006 to 10,461,818 in 2009 due to "both the vast amount of personal data housed at hospitals and medical centers and the comparatively lax security employed by these organizations").

28. This Article contains material relevant to all attorneys, even those whose only electronic device is a smartphone. *See* Lucy L. Thompson, *Cybercrime and Escalating Risks*, *in* DATA BREACH HANDBOOK, *supra* note 3, at 10–11 (describing the rising trend of criminals hacking into law firm networks in order to steal confidential information about the firm's clients). Additionally, "e-message," "e-communication," and "e-document" are used frequently in this Article in an interchangeable manner.

29. *See infra* Part II.

30. *See infra* Part III.

31. *See infra* Part IV.

32. *See infra* Parts IV.B–C.

33. *See infra* Part V.

34. *See infra* Part V.

II. E-SECURITY OVERVIEW: SYSTEMS, MALWARE, AND ENCRYPTION

EMRs, like e-data and money, must be kept safe from loss, corruption, and unauthorized access.[35] For EMRs and cEMDs, the risk of an e-security breach depends on a number of factors, including the nature of the computer system, the presence of malware, the use of encryption and the social sophistication of the hacker.[36] This section will review the first three of these factors, while the social sophistication of hackers (which may be revealed through, for example, social engineering) will be addressed in Part III of this Article.[37]

A. Computer Systems

Three basic types of computer systems exist: closed, semi-closed, and open with other computer systems.[38] With a closed system, also known as a client-server (CS) system, the system's purchaser is the owner-operator of the system.[39] A CS system is considered closed to the outside world because the owner-operator controls all aspects of the system, including the system's hardware (i.e., the server and its terminals), software (including the e-security package[40]), and authorized access to the system.[41] With respect to EMRs, the principal advantage of the CS system is its security; of the three types of computer systems, closed systems are considered to be

35. *Cf.* Peabody & Thomson, *HITECH: The First Federal Data Breach Notification Law*, *in* DATA BREACH HANDBOOK, *supra* note 3, 128–29 (describing HIPAA's increased authority to impose penalties, both civil and criminal, upon an individual or business after a security breach results in the loss, corruption, or destruction of EMRs).

36. *See infra* Parts II.B–C, III; *see also* DAVID SALOMON, ELEMENTS OF COMPUTER SECURITY 2 (2010) (describing the numerous ways a hacker may breach a computer network's security, but concluding that "[a]n attacker has to find only one security weakness to compromise an entire [network]").

37. *See infra* Part III.

38. "Closed," "semi-closed," and "open" are descriptive terms, used here to explain whether a computer system interacts with other computer systems.

39. *See* Anita Jones, *Cyber Security in Open Systems*, COMPUTER SYSTEMS: THEORY, TECHNOLOGY, AND APPLICATIONS 133, 133–34 (Andrew Herbert & Karen Spärck Jones eds., 2004) (describing a closed computer system as a system in which each computer acts alone, and this single access reduces the need for comprehensive e-security); *see also* Steven Biggs & Stilianos Vidalis, *Cloud Computing Storms*, 1 INT'L J. INTELLIGENT COMPUTING RES. 3, 62 (describing the traditional, "closed," computing system in which the user has sole ownership of both the computing hardware and software).

40. As used here, an e-security package is to be viewed broadly to mean all aspects of a computer system's security that is controlled by digital code. Such security features would include, but are not limited to, the computer's firewall, the anti-virus protection, the type of encryption, and the nature of password protection.

41. *See* Biggs & Vidalis, *supra* note 39, at 62 (comparing CS systems to newer "cloud computing").

the most secure.[42] This is not to say that the security associated with a CS system is infallible, as all computer systems are vulnerable to e-security breaches.[43]

At the other extreme of computer systems are open systems, including the systems commonly known as cloud computing systems.[44] Compared with the closed system, cloud systems have the reverse trade-off, in that open systems are often cheaper to operate, but they are less secure.[45] Open systems are less expensive because their software programs are run over the Internet rather than on a dedicated local computer,[46] thereby lowering the per user software costs.[47] These differences allow vendors of cloud-based computer systems to sell their services according to a flat monthly subscription fee.[48] EMR subscription fees for cloud services might range from $175 per month[49] to $600 per month.[50]

---

42. *See* Jones, *supra* note 39, at 133 ("Cyber security has been a *casualty* of the transition from closed to open systems. In closed systems sufficient protection of one user from another could be assured . . . ."). *But see* Jonathan Loiterman, *Free as in Freedom: Open Source Software's Role in Remaking Healthcare in the Twenty-First Century*, 19 ANNALS HEALTH L. 259, 259–60 (explaining that "[c]losed, proprietary information systems and closed software licensing are a big problem in the healthcare industry" because these systems remove a doctor's ability to alter, update, or view a patient's EMR).

43. Benjamin G. Walker, *Protection of Data Privacy in Computer Systems*, 21 ISR. L. REV. 1, 9 (1986) ("There is no perfectly secure computer system."); *cf.* David Kushner, *Machine Politics: the Man who Started the Hacker Wars*, NEW YORKER, May 7, 2012, *available at* http://www.newyorker.com/reporting/2012/05/07/120507fa_fact_kushner?printable=true (describing a hacker's successful attempt to hack Sony's "impenetrable" system, after which the hacker stated "nothing is unhackable").

44. *See* Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. TECH L. & POL'Y 231, 232 (2011) (comparing the extreme differences from closed to open systems by explaining that open systems perform "computing practices on an outside vendor's machines somewhere in the cloud"). Other types of open computer systems are web-based servers or Application Service Provider (ASP) systems. S*ee* CICCARELLI, *supra* note 23, at 28 (describing ASPs as systems that provide access to specific software to be stored on the system).

45. *See* Lucy L. Thompson, *Cybercrime and Escalating Risks*, *in* DATA BREACH HANDBOOK, *supra* note 3, at 12 (demonstrating that the open nature of cloud systems reduces computing costs, but multiple security risks arise from the open nature of the programs as well as from third party operators' access to the data). *See generally* Harshbarger, *supra* note 44, at 233–37 (explaining the various advantages and disadvantages of cloud computing).

46. *See* Harshbarger, *supra* note 44, at 232–33 (explaining the specific features of cloud computing not permitted in closed systems that make cloud computing economical).

47. *See id.* at 232 (stating cloud computing reduces costs because "user transitions from operating on their own mainframe to operating on an Internet-based architecture in the 'cloud'"). *See generally* Lucy L. Thompson, *Cybercrime and Escalating Risks*, *in* DATA BREACH HANDBOOK, *supra* note 3, at 12–13 (describing the cost efficiency of shared computing services).

48. *See* Jack Newton, *Solo/Small Firm: Ten Reasons to Adopt Cloud Computing for Your Law Office*, 74 TEX. BAR J. 860, 861 (2011) (stating "[m]ost cloud computing solutions offer a simple month-to-month subscription" and because the user is not purchasing additional hardware the customer doesn't incur "upfront hardware purchases"). *But see* Sean Mortson et al., *Cloud Computing: The Business Perspective* 23 (Working Paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1413545 ("There are many different potential pricing policies available to providers, such as flat fee, pay-per-use fee, or a two-tier mix of flat and pay-per-usage fee.").

49. *See, e.g.*, ENCOUNTERWORKS, *EncounterWorks Patient Management / EMR Cloud Quote* (Oct. 5, 2012), http://encounterworks.com/docs/brocures/cloud-emr-price-comparrison.pdf.

In exchange for lower operating costs, cloud computing services often provide weaker e-security for several reasons.[51] First, e-documents in a cloud system are only as secure as the cloud-EMR vendor's e-security policy for that subscription rate.[52] Second, even if a client is willing to pay a cloud vendor a premium price for better e-security, it may be impossible to make a cloud system as safe as a CS system.[53] Cloud-based systems are subject to attacks that are mediated by malware that exploit "holes" in the Internet and the open system's software.[54] Finally, "[c]loud service providers typically work with numbers of third parties," so cloud users need to consider these third-parties as e-security risks.[55]

While this difference in security may sound subtle, the difference has real world implications. To illustrate, consider the recent attack on an Indiana hospital in which the hackers targeted the hospital's cloud-based computer system that

50. *See* Marianne Kolbasuk McGee, *Is that a Cloud on Healthcare's Horizon?*, INFORMATIONWEEK (June 16, 2009), http://www.informationweek.com/cloud-computing/is-that-a-cloud-on-healthcares-horizon/229206257 (reporting that eClinicalWorks brand software may have a monthly subscription fee as high as $600).

51. *See generally* William Jeffery Robinson, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1214–17 (2010) (describing the impact of the terms of service agreements within service contracts and the power the service provider may receive to access the customer's data based on the level of service agreed upon in the subscription). In addition to suboptimal security, cloud computing also suffers from a lack of oversight by regulators and a lack of interoperability with existing applications. *See* Harshbarger, *supra* note 44, at 235–36 (explaining a disadvantage of cloud computing includes the potential that the cloud provider may not comply with cyber security regulations and there may be increased vulnerabilities).

52. *See* Simon Bradshaw et al., *Contracts for Clouds: Comparison and Analysis of the Terms & Conditions of Cloud Computing Services* 21–34 (Queen Mary Sch. of L. Legal Stud. Res. Paper No. 63/2010, 2010), *available at* http://ssrn.com/abstract=1662374 (analyzing the terms and conditions in numerous cloud providers' service agreements and determining that cloud providers supply minimal security under standard service agreements); *see also* WAYNE JANSEN & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T COMMERCE, PUB. NO. 800-144, GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING 40–43 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf (stating that customers should subscribe to cloud providers that use negotiable service agreements which provide the customer with the ability to negotiate the terms of the service to emphasize security). Thus, it is a wise decision to review the service agreement and select the provider that offers additional data protection measures. *See generally* Mayer Brown LLP, *Managing the Risks of Cloud Computing, reprinted in* MONDAQ BUS. BRIEFING, Dec. 10, 2010 (advising a potential cloud subscriber that one of the essential tasks before subscribing to a cloud service is to establish clear terms in the service contract for liability on breaches and general security).

53. *See* Jones, *supra* note 39, at 134 (explaining that hackers normally breach open systems through "holes" that must be patched in order to make the software more secure). *See generally* Michael J.G. van Eeten & Johannes M. Bauer, *Economics of Malware: Security Decisions, Incentives and Externalities* (Org. for Econ. Co-Operation & Dev., Working Paper No. 2008/1, 2008) (describing that before third party vendors patch a hole they balance the cost to patch the hole against the ongoing vulnerability to hackers this open hole provides).

54. *See supra* note 53.

55. Manisha Malhorta, *"EIGAMAL Signature Scheme" - Approach to Ensuring the Security of Cloud Computing Environment*, INT'L J. ENTER. COMPUTING & BUS. SYS. (2010), www.ijecbs.com/January2012/7.pdf; *see also* Lucy L. Thompson, *Cybercrime and Escalating Risks*, *in* DATA BREACH HANDBOOK, *supra* note 3, at 12 (stating the increased risks of cloud computing that arise from users relying on "third-party service providers to process or analyze [the users'] confidential information").

contained employee health data.[56] This e-security breach resulted in the hackers obtaining personal information, including Social Security numbers, of more than 12,000 people who applied for jobs at the hospital.[57] Yet, the same hacker attack left the hospital's records that were stored in the hospital's more secure closed EMR system untouched.[58] Given the street value of patients' health and insurance data, it is plausible that hackers went after the hospital's employees' records because the cloud-based record system was less secure than the CS-based patient record system.[59]

Increasingly, smartphones employ cloud computing systems.[60] Given that there are a number of medical application programs for smartphones,[61] physicians[62] and patients[63] are increasingly using smartphones as cEMD.[64] Yet, as the World News smartphone hacking scandal has demonstrated, hackers have identified a number of ways to breach the e-security of smartphones.[65] Although the details of just how hackers were able to compromise the smartphones of the United Kingdom's Royal

56. *See IU Health Goshen Data Hit by Virus*, S. BEND TRIB., Feb. 1, 2012, at C1 (describing a computer virus, planted by hackers, that successfully breached an Indiana Hospital's cloud computing system and attempted to steal the hospital records on this system).

57. *Id.*; *IU Health Goshen Suffers Web Security Breach; Personal Information of More than 12,000 People Compromised*, GOSHEN NEWS (Jan. 31, 2012), http://goshennews.com/local/x647581516/IU-Health-Goshen-suffers-web-security-breach-personal-information-for-more-than-12-000-people-compromised (describing a breach that gave hackers access to the personal information for more than 12,000 people who applied for jobs at the hospital).

58. *See IU Health Goshen Data Hit by Virus*, *supra* note 56.

59. *See infra* Part III.

60. *See* Mikael Ricknäs, *HTC Launches Entry-Level Android Smartphone with Dropbox*, COMPUTERWORLD (Aug. 30, 2012), http://www.computerworld.com/s/article/9230762/HTC_launches_entry_level_Android_smartphone_with_Drobox ("Smartphone integration with cloud storage is starting to become common place."). *See generally* Lucy L. Thompson, *Cybercrime and Escalating Risks*, DATA BREACH HANDBOOK, *supra* note 3, at 13 (describing that the increase in mobile device use presents a major vulnerability, specifically for the theft of personal identities, such that experts predict that hacking mobile devices will be a major criminal activity).

61. *See* Dina ElBoghdady, *Feeling Sick? There's an App for that*, WASH. POST, June 24, 2012, at G01 (describing that more than 13,000 mobile medical applications are available and "medical applications have flooded onto millions of smartphones").

62. Olga Khazan, *Summit: Medical Devices Going Mobile*, WASH. POST, Dec. 12, 2011, at A31 (describing the recent innovations of mobile applications specifically created to enable doctors to monitor their patients over mobile devices).

63. Steven Overly, *Mobile Health Apps Navigate Privacy, Safety Concerns*, WASH. POST, Apr. 30, 2012, at A8.

64. *See* David Daw, *FDA Plans to Regulate Smartphone Apps.*, PCWORLD (July 19, 2011, 1:30 PM), www.pcworld.com/. . ./fda_plans_to_regulate_smartphone_apps.html (reporting an increase in the use of medical smartphone "app" programs in recent years).

65. *See, e.g.*, *Timeline of Britain's Phone-Hacking Scandal*, AGENCE FRANCE PRESSE, July 20, 2011, http://www.thenational.ae/news/world/europe/timeline-of-britains-phone-hacking-scandal; *see* Katherine Rushton, *Murdoch Stepping Down Doesn't Mean Clear Skies for Sky*, DAILY TELEGRAPH (UK), Apr. 4, 2012, at B4; *see also* LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID (2012) (discussing the overall loss of privacy that users experience as a result of the use of social networks).

Family (and others) have not officially been released, it seems likely that the smartphones of the Royals were the victims of a malware attack.[66]

B. Malware

Regardless of which type of computer system a hacker seeks to compromise, among the favorite tools of hackers for gaining unauthorized access to the targeted computer system are malware and social engineering.[67] Malware is classically defined as "a computer program designed specifically to damage or disrupt a system, such as a virus."[68] When hackers write malware programs, a higher-order computer language is generally used. Higher-order computer languages are more elaborate then the zeros and ones of machine code as they have word-like commands and use syntax.[69] Unless you are both trained and experienced in higher-order computer languages, these languages can be as foreign as Latin or Chinese to a native English speaker.[70]

66. *See* Andy Bloxham, *Prince and Duchess Warned of Phone Hacking*, DAILY TELEGRAPH (UK), July 15, 2012, at 5 (noting that there are at least 10 members of the Royal Family whose mobile phones might have been hacked); *see also* 45 C.F.R. § 164.304 (2011) (defining "malicious software," also known as "malware"); Robert W. Ludwig, Jr., Salvatore Scanio & Joseph S. Szary, *Malware and Fraudulent Electronic Fund Transfers*, XVI FIDELITY L. J. 101, 103–04 (2010).

67. *See* Sean B. Hoar, *Trends in Cybercrime: The Dark Side of the Internet*, 20 CRIM. JUST. 4, 4–5 (2005) (describing social engineering and malware as "two common methods used to commit cybercrime").

68. *Malware*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 753 (11th ed. 2008).

69. *See supra* note 19.

70. *See, e.g.*, *infra* Table I.

Table I: Example of a Program Written in "C" that Creates an Array[71]

```
#include <stdio.h>
main()
{
   int array[100], n, c;
   printf("Enter the number of elements in array\n");
   scanf("%d", &n);
   printf("Enter %d elements\n", n);
   for ( c = 0 ; c < n ; c++ )
   scanf("%d", &array[c]);
   printf("Array elements entered by you are:\n");
   for ( c = 0 ; c < n ; c++ )
   printf("array[%d] = %d\n", c, array[c]);
   return 0;
}
```

Still, it is not typically possible to classify malware based on its intended use. The same computer code that can have legitimate beneficial use can sometimes also be used to achieve a malevolent or destructive goal.[72] Accordingly, herein, we define malware broadly to include any computer program that can be used to compromise e-security, regardless of whether that computer program may also have a legitimate use or a beneficial intent.[73]

1. First Generation Malware

Viruses, Trojan horses, and worms are paradigmatic forms of first generation malware. A computer virus is a program or piece of code that is capable of self-replication and may perform tasks on a computer system without the operator's knowledge or consent. Viruses almost always require the victim to open a file in order to cause damage.[74] Trojan horses are typically passed through downloads

71. *C Program Examples*, Programming Simplified, http://www.programmingsimplified.com/c-program-examples (last visited Oct. 13, 2012).

72. *See* Andrews, *supra* note 65, at 73; *see also* Peter Beaumont, *Stuxnet Worm Heralds New Era of Global Cyberwar*, Guardian (UK), Sept. 30, 2010, *available at* 2010 WLNR 19416018.

73. A computer code is ultimately nothing more than a string of zeros and ones, accordingly, computer code is incapable of the mental process required to create intent. *See* Black's Law Dictionary 881 (9th ed. 2009) (defining "intent" as "the state of mind accompanying an act, especially a forbidden act").

74. *See* Michael Edmund O'Neil, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 Geo. Mason L. Rev. 237, 247 (2000) (noting that a virus commonly requires some sort of action on the user's part before it can be activated such as the opening of a file).

disguised as legitimate files, while viruses are more often passed by email.[75] The main difference is that Trojans, unlike viruses, neither infect other files nor self-replicate; they typically create backdoors into users' systems.[76] Worms are similar to both viruses and Trojan horses with the key distinction that worms can spread without human action and they self-replicate.[77] Regardless of whether a hacker uses a virus, a Trojan horse, a worm, or some other malware, the goal of the hacker is usually to render the targeted computer system inoperable, to hijack a computer, or to spy on a computer.[78] In short, the characteristic feature of first generation malware was destruction and defacement.

2. Current Generation Malware

Current generation malware and hackers, by way of contrast, often have broader objectives than rendering a computer system inoperable or causing harm *per se*. Rather, current generation malware often concerns itself with the hijacking of, or the spying on, a targeted computer(s).[79] To hijack a computer, a hacker may use malware that takes control of a computer such that control of the device is transferred to a remote computer.[80] For example, the Mariposa botnet hijacked 12.7 million computers to facilitate the theft of login and password information from financial institutions.[81] Alternatively, botnet attacks may be launched to take down a financial services' or an economic competitor's server.[82] Hackers could potentially also use current generation malware programs for spying (also known as spyware)[83] to gain unauthorized access to protected health information (PHI).[84] As Professor

75. *See* GLENNY, *supra* note 18, at 122 ("Zip files were some of the most notorious carriers of trojan infections.").

76. *See* Benjamin R. Jones, Comment, *Virtual Neighborhood Watch: Open Source Software and Community Policing Against Cybercrime,* 97 J. CRIM. L. & CRIMINOLOGY 601, 608 (2007) (explaining that Trojan horse programs contain "backdoor" functions that allow remote access to the computer).

77. *See* O'Neil, *supra* note 74, at 247 (worm replicates itself and relies solely upon computer networks to duplicate itself, thus it is not dependent on a user's action for transmission); *see also* Sharon D. Nelson & John W. Simek, *Electronic Security in Your Law Office*, 38 TENN. B.J. 12, 13 (2002) ("A worm is a program or algorithm that replicates itself over a computer network and usually performs malicious actions.").

78. *Cf.* Susan W. Brenner, *Nanocrime?*, 2011 U. ILL. J.L. TECH. & POL'Y 39, 58, 78 (2011) (noting that malware can be used to siphon valuable information from a victim computer system).

79. *See* Kaspersky Lab Zao, *Patent Issued for System and Method for Dynamically Allocating Computing Resources for Processing Security Information*, INFO. TECH. NEWSWEEKLY, July 17, 2012, at 2 (discussing cybercriminals and the current generation of malware).

80. *See* Mark Bassingthwaighte, Esq., *Ten Technology Traps and How to Avoid Them*, W. VA. LAW. 34, 39 (Oct. 2006) (noting that other types of malware programs enable a remote computer to monitor your machine or scan your computer network).

81. *Summary Box: 3 Nabbed for Huge Computer Infection*, ASSOCIATED PRESS FIN. WIRE, Mar. 2, 2010.

82. *Report: 'Kneber' Botnet Attacked 75,000 Systems*, SAN JOSE BUS. J., Feb. 18, 2010, at 1.

83. *See FinFisher Surveillance Malware Spreads to Smart Phones*, TORONTO STAR, Aug. 30, 2012, at B1.

84. *See* Mike Paquette, *An Ounce of Prevention for the Healthcare IT Network*, HEALTH MGMT. TECH., Dec. 2006, at 18 (defining spyware as a type of "malicious content").

Andrews has recently and comprehensively reviewed spyware programs, no attempt will be made here to replicate her work.[85]

A hacker can attack computer systems using either a front door or backdoor strategy. During a front door attack on a computer system, the hacker gains unauthorized access to a computer system by using a pirated password or other login information in the same way a legitimate user would use this information to access the computer system.[86] Pirated authentication can be obtained directly or indirectly through the use of malware.[87] In a direct attack, the hacker connects directly to the compromised computer.[88] For example, a hacker may use a Trojan to install a keystroke logger program to obtain login authentication information.[89] Another example is when a hacker sends a virus to a user via a phishing email and the virus opens the computer to the hacker once the user opens the email.[90] In an indirect attack, the hacker uses third party computers to conduct an attack.[91]

Understanding how a hacker attacks a computer system through the backdoor is more complicated, but basically this strategy takes advantages of vulnerabilities in the software.[92] Therefore, for simplicity's sake, herein, unless otherwise indicated, a "backdoor" refers only to holes in the source code of legitimate software regardless of whether the backdoor was intentionally left by the original programmer for debugging or subsequently inserted by a hacker via software vulnerabilities in order to facilitate subsequent unauthorized entry.[93]

85. Lori Andrews, I Know Who You Are and I Saw What You Did (2012).

86. *See This Winter, Protect Computers from Viruses Too*, U.S. St. News, Dec. 12, 2005, *available at* 2005 WLNR 20005955 (describing tools that can be used to prevent front- and back-door attacks).

87. *See B3: Authentication, Authorization, and Encryption Systems*, Practical IT Auditing (Warren Gorham & Lamont eds., 2012), *available at* 2003 WL 21375197. Direct attacks set up a direct link from the hacker to the compromised machine. *Id.* Indirect attacks use third party computers to conduct an attack. *Id.* However, sophisticated hackers commonly use indirect approaches. *See, e.g.*, Nicole Perlroth, *Hackers in China Attacked The Times for Last 4 Months*, N.Y. Times, Jan. 31, 2013, at A1 ("The hackers tried to cloak the source of the attacks on The Times by first penetrating computers at United States universities and routing the attacks through them, said computer security experts at Mandiant, the company hired by The Times.")

88. *See supra* note 87.

89. *See* Jonathan Sidener, *LOG-ON LARCENY: Keystroke Loggers Can Steal Sensitive Data, Commit Fraud*, San Diego Union-Trib., Oct. 25, 2004, at E1 (discussing that keystroke logger software logs the strokes typed on computer keyboards so that others can remotely read and steal personal information).

90. *See* Jeremy Feigelson & Camille Calman, *Liability for the Costs of Phishing and Information Theft*, 13 J. Internet L. 15, 16 (2010) (describing the concept of email phishing).

91. *See Newest Digital Tech Aids Hackers*, Cap. Times (Madison, Wis.), Feb. 28, 2000, at 5A ("Indirect hacking can occur through e-mail . . . . [so t]o discourage hacking, [it is advisable] to turn off file- and print-sharing options in Windows-based systems.").

92. *See New Linux Trojan Horse*, Info. Sys. Auditor (Int'l Newsl.), Mar. 1, 2002, at 5 (describing a "backdoor" Trojan software attack).

93. *See* Ghost, *supra* note 22, at 31 (explaining a system "backdoor" as "software code that sets [a hacker] up so [he would] be able to gain access whenever [he] want[s] to get back in").

While this review of computer hacking 101 lacks the detail to train a true malicious cyberscribe,[94] for many readers this review provides insight into a level of stealth that they could not have previously imagined. Just as the scribes of Ancient Egypt could commit crimes that were almost inconceivable to the illiterate masses,[95] today's cyberscribes, who are fluent in computer languages and e-security architecture, can commit crimes that are almost inconceivable to the computer illiterate 21st century man. Worse, hacker stealth is reaching even new heights in the era of designer, so-called "zero day" malware.[96]

3. Next Generation Malware

The computer virus Stuxnet is the prototype of next generation designer malware.[97] Designer malware like Stuxnet is highly discriminating with respect to the computer it impacts: while it may still be able to spread from computer to computer, the manifestations of the malware will only become apparent when the malware encounters a specific type of computer (or electronic device).[98]

Stuxnet, which the United States military almost certainly had a hand in developing,[99] was designed to seek out and disable a specific brand of control system located in an Iranian nuclear facility.[100] On any other computer or device, Stuxnet has no effect.[101] Stuxnet was wildly successful as it substantially impaired Iran's

94. Indeed, any reader who thinks that based on this primer on computer language and technology that they can breach a computer's e-security system has not read the majority of the footnotes. *Cf.* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1401, 1539 (2010) (noting that the Department of Defense ordered all troops and officials involved in protecting computer networks to undergo training in computer hacking under the premise that "to beat a hacker, you must think like one").

95. If the Ancient Egyptians could imagine the power of the scribes to steal from the contents of the pharaohs' warehouse, it is likely that literacy in general population would have appeared long before the Greeks in the fifth century B.C.E. *See generally supra* notes 11–17 and accompanying text.

96. *See* Sharon D. Nelson, Esq. & John W. Simek, *Preventing Law Firm Data Breaches*, 75 TEX. B.J. 364 (2011) (describing a "zero day exploit" as an instance in which the user "got the mal-ware [sic] before the security companies have had a chance to muster a defense against it").

97. *See* Richard Brust, *CYBERATTACKS: Computer Warfare Looms as the Next Big Conflict in International Law*, 98 A.B.A. J. 40, 41 (2012) (noting that the future is likely to see more viruses like Stuxnet, which represents the so-called high end of cyberware"); *see also Stuxnet: Computer Worm Opens New Era of Warfare*, CBS NEWS (July 1, 2012, 7:03 PM), http://www.cbsnews.com/8301-18560_162-57460009/stuxnet-computer-worm-opens-new-era-of-warfare/ (noting that Stuxnet is unlike the millions of worms and viruses that turn up on the Internet each year).

98. *See Stuxnet: Computer Worm Opens New Era of Warfare*, CBS NEWS (July 1, 2012, 7:03 PM), http://www.cbsnews.com/8301-18560_162-57460009/stuxnet-computer-worm-opens-new-era-of-warfare/ (explaining that Stuxnet was designed to only hit one target and it goes through a sequence of checks to actually determine if it is the right target).

99. *See* Hayley Tsukayama, *Malware is Linked to Stuxnet, Flame*, WASH. POST, Aug. 10, 2012, at A03 (asserting that Stuxnet was jointly developed by the United States and Israeli defense programs).

100. *See Stuxnet: Computer Worm Opens New Era of Warfare*, CBS NEWS (July 1, 2012, 7:03 PM), http://www.cbsnews.com/8301-18560_162-57460009/stuxnet-computer-worm-opens-new-era-of-warfare/ (reporting that "someone sabotaged a top secret nuclear installation in Iran" using only computer code).

101. *Id.* The Stuxnet virus was spread through contact with an infected thumb drive. *Id.*

ability to develop nuclear weapons for a number of years.[102] Yet, the broader security-related price of the Stuxnet attack on the Iranian nuclear plant may be high because the virus was reverse engineered after being identified.[103] This means that computer code used to create target specificity has been cracked by hackers and Stuxnet's coding tricks are now known to a wider audience than just the military.[104]

In the future, could a hacker launch a Stuxnet-type attack on a specific hospital's EMR system or a specific patient's cEMD? The short answer seems to be "yes." One example might be found in a hypothetical attack on a hospital's heating, ventilation, and air conditioning (HVAC) system.[105]

Infrastructural support of a client-server EMR (or any large-scale computer) system is critical for the system's normal operation. For an EMR system, the infrastructure support required includes a reliable power source, an operating data network, and a functioning HVAC system.[106] An excessive amount of heat can destroy a computer system and its data.[107] Yet, given the importance we are placing on EMRs in our healthcare system, it is surprising that hospitals "often don't have guidelines for securing . . . the HVAC systems that maintain the strict environmental controls over operating rooms and surgical wards,"[108] let alone to securely provide for temperature control support for their EMR systems. This lack of concern for the operational details of a hospital's HVAC systems thus creates an e-security risk that can compromise a hospital's EMR system. In fact, at least one hospital has had its HVAC hacked without apparent harm.[109]

EMR hostage-taking is not new. In 2009, the Washington Post reported on how hackers broke into a Virginia State website and compromised eight million patients' medical records.[110] These thieves then threatened to delete all the records if a ransom of $10 million was not paid.[111] Unfortunately these hackers overlooked one

102. *See* Dominic Basulto, *Stuxnet, Flame and Fulfilling the Dream of Sun Tzu*, Wash. Post (June 1, 2012, 10:38 AM), http://www.washingtonpost.com/blogs/innovations/post-stuxnet-flame-and-fulfilling-the-dream-of-sun-tzu/2012/06/01/gJQA61Jv6U_blog.html ("It appears the line between 'covert action' and 'act of war' is blurring like at no time in history in one of the world's most volatile regions.").

103. *See* Nicole Perlroth, *Computer Is Stealing Data Across Middle East, Report Says*, N.Y. Times, May 29, 2012, at B4 (reporting that the "Flame" virus, unlike the "Duqu" virus, was likely developed by a group of programmers unaffiliated with the production of Stuxnet).

104. *See* Misha Glenny, *A Weapon We Can't Control*, N.Y. Times, June 25, 2012, at A19 (describing Stuxnet's widespread availability as an "escap[e] into the cyberwild").

105. *See, e.g.*, Ajay Gupta, *Hackers, Breaches and Other Threats to Electronic Records*, 19 Health Data Mgmt., Sept. 2011, at 54 (recounting an incident in Texas of an HVAC system being hacked).

106. *See* Steven Levy, In The Plex 191 (2011) (describing the utilities needed to operate a Google data center).

107. *Antenna Type Can Affect Picture*, Atlanta J.-Const., May 30, 2012, at E15.

108. Gupta, *supra* note 105, at 55.

109. *Id.*

110. *Hackers Break into Virginia Health Professions Database, Demand Ransom*, Wash. Post (May 4, 2009), http://voices.washingtonpost.com/securityfix/2009/05/hackers_break_into_virginia_he.html.

111. *Id.*

detail: Virginia had a backup system for its EMRs, so the State was able to avoid having to meet the hackers' ransom demand.[112] Given the ability of certain viruses to hone in on a specific target, in the future individual cEMDs may be targeted. In the 21st century, many cEMD have computers. Two such devices are insulin pumps and heart rhythm regulatory devices (pacemakers and defibrillators).[113]

Insulin pumps are medical devices worn by diabetics to regulate their blood sugar.[114] Insulin pumps have two basic components: a wireless sensor that detects blood sugar levels and a pump for insulin administration. The sensor's function is to monitor the patient's blood sugar and then send this information to the pump via a radio frequency (RF) signal.[115] The pump, which houses the system's computer, takes the patient's blood glucose as input and then calculates and administers an appropriate dose of insulin to the patient.[116]

Recently, a hacker reverse engineered an insulin pump to learn its secrets.[117] One of the key findings of this reverse engineering process was the discovery that the RF signal between the sensor and the pump was unencrypted.[118] The hacker then demonstrated how a $10 radio frequency circuit board could be used to reprogram and corrupt the pump's algorithm for insulin delivery.[119] Had this not been a planned demonstration, but rather a direct attack on an insulin pump attached to a patient, the outcome might have been fatal.

A similar demonstration has also been carried out on an implantable cardiac defibrillator. Unlike the insulin pump, heart rhythm regulatory devices are self-contained units in that their sensory and output leads are directly connected to the device's computer.[120] In other words, there is no RF signal. However, all heart rhythm regulatory devices are programmable. The device's settings are modified by an electromagnetic signal. Thus, heart rhythm regulatory devices are analogous to a

112. *Id.*

113. For non-cardiac specialists, the key difference between a pacemaker and a defibrillator is the latter's ability to deliver an electric shock when the device detects certain potentially fatal heart rhythms. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 326 (11th ed. 2008) (defining defibrillator as "an electronic device that applies an electronic shock to restore the rhythm of a fibrillating heart"); *id.* at 833 (defining pacemaker as "an electronic device for stimulating or steadying the heartbeat or reestablishing the rhythm of an arrested heart").

114. *See* Howard Simmons, *Insulin Pumps Give Diabetics Flexibility*, SPRINGFIELD NEWS-LEADER (Missouri), Feb. 12, 2007, at 10E (explaining benefits of insulin pumps over other types of pancreatic function modification).

115. *See* Dean Takahashi, *Insulin Pump Hacker Says Vendor Medtronic is Ignoring Security Risk*, VENTURE BEAT (Aug. 25, 2011), http://venturebeat.com/2011/08/25/insulin-pump-hacker-says-vendor-medtronic-is-ignoring-security-risk/ (revealing that a hacker found a weakness in the devices that was created by their wireless connectivity).

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

120. *See* Janet Moore, *Timing of Defibrillator News is No Shock; On the Eve of a Major Meeting of Doctors, Medtronic and Boston Scientific Hoped to Garner Attention for their New Heart Devices*, STAR TRIB. (Minneapolis), May 14, 2008, at 1D.

semi-open computer system.[121] When the defibrillator demonstration was carried out on a non-implanted defibrillator,[122] the hackers were able to "reprogram [the device] to shut down and to deliver jolts of electricity that would potentially be fatal if the device had been in a person."[123] Accordingly, this demonstration project, like the insulin pump demonstration project, suggests hackers could convert cEMD from life-saving devices into murder weapons.

C. Encryption

Few doubt that encryption enhances e-security. Yet, the statistics on EMR e-security breaches suggest that healthcare providers rarely use encryption.[124] For the encryption process to be effective, therefore, both the sender and the receiver must have access to the cypher's key. If the two parties know each other well, a symmetric-key encryption system, which uses a single cypher key, can be used.[125] A single key encryption system is predicated on both the sender and the receiver sharing a single secure encryption key.[126] A single key cypher system worked well more than 100 years-ago when remote newspaper reporters telegraphed their reports to the home office, as both parties had a copy of the same code book.[127]

Unfortunately, there are three principle drawbacks to using single key encryption in the healthcare sector. First, single key encryption is at the mercy of human fallibility (e.g., one party may lose a copy of the code book or inappropriately disclose the code to a third-party).[128] Second, single key encryption systems do not work well in hospitals (or large law firms) because the encryption key must be

121. As a self-contained computer system, it is tempting to analogize a heart rhythm regulatory device to a closed CS system. But this would be wrong. From time to time it is clinically necessary to change the settings of heart rhythm regulatory device with an externally applied electromagnetic signal. *See generally* Gabriel Gregoratas et al., *ACC/AHA Guidelines for Implantation of Pacemakers and Antiarrhythmia Devices*, 31 J. Am. C. Cardiology 1175 (1998). Thus the computer system of a heart rhythm regulatory device is more analogous to a semi-open computer system. *See supra* Part II.A.

122. Barnaby J. Feder, *Computer Security Team to Report Hacking Into Defibrillator-Pacemaker*, N.Y. Times, Mar. 12, 2008, at C4.

123. *Id.*

124. Diane Bartz, *Electronic Medical Records Rarely Encrypted: Expert*, Reuters, Nov. 9, 2011, *available at* http://www.reutersreprints.com; *cf.* Daniel R. Levinson, Office of Inspector Gen., Dep't of Health & Human Servs., A-18-09-30160, Audit of Info. Tech. Sec. Included in the Health Info. Tech. Standards 5 (2011) (observing that many serious EMR e-security breaches occur because laptop computers are not encrypted).

125. CGI Group Inc., Public Key Encryption and Digital Signature: How do they work? 3 (2004), *available at* http://www.cgi.com/cgi/pdf/cgi_whpr_35_pki_e.pdf.

126. *Id.*

127. Gleick, *supra* note 11, at 154. To a degree, a single cypher key system was used to keep a news story under wraps. But a more important reason was money. Telegraph operators charged the sender ¼ cent per word. *Id.* at 152. To keep number of words down, reporters used a code that was only known to them and the home office. *Id.* at 153.

128. *See* Eric A. Hibbard, *Encryption: The Basics*, *in* Data Breach and Encryption Handbook 180 (Lucy Thomson ed., 2011).

shared with too many individuals.[129] Third, single key encryption does not work well when two healthcare providers who have never met each other must exchange PHI for a patient they have in common.[130]

To work around the limitations of single key encryption, asymmetric key or public-key infrastructure (PKI) encryption was developed.[131] In PKI encryption both parties have a pair of keys: one key is personal and private and one key is stored in the public domain.[132] In practice, PKI works in a manner that is analogous to a safety deposit box type security system.[133] That is, a key from both the sender and the receiver must be used to decipher a PKI encrypted message. In the real world, each PKI key is a large prime number and the two keys are multiplied together to obtain the ultimate key for encryption. So when the sender uses their private key to encrypt a message it is combined (multiplied) with the receiver's public key to produce the ultimate cypher key.[134] The resulting encrypted message may then only be decoded by using the receiver's private key and the sender's public key.[135]

So, why do EMR systems not make better use of PKI encryption? The answer is that the devil is in the details for generating the encryption keys. First, performing PKI encryption requires a lot of computational power.[136] Large hardware computing capacity requirements mean that the price tag for EMR systems with encryption will be larger than EMR systems without encryption. Thus, from the perspective of healthcare providers, the higher cost of EMR systems with PKI encryption may make the system less desirable.

---

129. *Cf.* CGI Group, *supra* note 125 (explaining that single key cryptography requires that all users be given the same key by sophisticated mechanisms, which are difficult to coordinate among a greater number of individuals).

130. David L. Gripman, *Electronic Document Certification: A Primer on the Technology Behind Digital Signatures*, 17 J. Marshall J. Computer & Info. L. 769, 775 (1998); *see also* CGI Group, *supra* note 125 (describing a secure single key distribution mechanism as necessarily very "sophisticated").

131. Of course, PKI is not infallible. John Markoff, *Flaw Found in Online Encryption Method*, N.Y. Times, Feb. 15, 2012, at B4 (observing that method for generating PKI prime numbers is flawed); *see also* Gleick, *supra* note 11, at 370 (quantum computing theoretically can factor large numbers for their prime factors).

132. Gripman, *supra* note 130, at 776.

133. Hibbard, *supra* note 128, at180. The public key is no more a security risk then a bank's key to a safety deposit box. The reason has to do with the astronomical number of public keys that could be combined with single key to open an encrypted message. *See id.*

134. For those interested in a little more detail, the key to PKI encryption is its use of large prime number. Assume the ultimate encryption key is a very large number that is the product of two large prime numbers. Because of the rarity of prime numbers and astronomical size of the ultimate encryption key, the latter is almost impossible to hack. Although identifying two large prime numbers and multiplying them is relatively easy; running this operation in reverse is very difficult. Gleick, *supra* note 11, at 370.

135. CGI Group, *supra* note 125, at 3.

136. *See* Junzuo Lai et al., *Self-Generated Certificate Public Key Encryption Without Pairing and its Application*, 181 Info. Sci. 2422, 2422 (2011) (arguing that PKI faces a number of challenges, including storage limitations on computer systems).

Second, encryption makes interoperability among the various EMR systems in the market more difficult.[137] The computer code that generates and stores pairs of PKI keys, as well as the actual encryption process, is often vendor-dependent.[138] So, if two EMR systems are running different vendors' PKI encryption programs, sharing PHI may be impossible. Given that there are a number of encryption vendors in the market,[139] until some healthcare authority articulates a universally accepted standard for EMR PKI encryption, it is likely that encryption and interoperability will maintain their adversarial relationship.[140]

III. Hackers: A New Public Health Risk

To paraphrase F. Scott Fitzgerald, cyberscribes "are different from you and me."[141] Cyberscribes not only have a unique understanding of computers and computer languages, but many of the better cyberscribes may understand human behavior better than the rest of us.[142] This part of the Article examines what motivates hackers and how hackers use social engineering.

In times past, hacker activity was almost exclusively driven by ego.[143] Today, money is increasingly supplanting ego as the prime motivator of hackers.[144] This trend appears to be applicable to EMR e-security where hackers carefully identify

137. Interoperability is the ability of one computer system to interact and exchange information with another computer system. James C. Dechene, *The Challenge of Implementing Interoperable Electronic Medical Records*, 19 Annals Health L. 195, 195 (2009). Without interoperability of EMR systems, patients would be locked into a particular provider because they would not be able to transfer their EMR to new provider. *See id.* at 199 (stating that in order to be useful, "[a]ny EMR from any system should be readily available and integrated into any other EMR system in use by any other provider"). *Cf.* Arash Anoshiravani et al., *Implementing an Interoperable Personal Health Record in Pediatrics: Lessons Learned at an Academic Children's Hospital*, 3 J. Participatory Med. 3 (2011) (explaining that the need for interoperability is greater in pediatric populations because patients change providers more frequently than adults).

138. *See* Joint Interoperability Test Command, Department of Defense, PKI Interagency/Partner Interoperability Testing (2012), *available at* http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html (stating that "vendor selection" has contributed to difficulties in PKI interoperability).

139. *Cf. id.* (testing interoperability of several PKIs produced by different vendors). Currently there are numerous encryption standards, but encryption software is becoming increasingly standardized and may enable widespread interoperability between encrypted PHI in the future. *Id.*

140. The HITECH Act does not mandate the use of encryption, but does provide an administrative safe harbor when an e-security breach only compromises encrypted PHI. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740 (effective Sept. 23, 2009) (to be codified at 45 C.F.R. pts. 160, 164). Specifically, when an e-security breach results in only encrypted PHI being accessed, the HITECH Act's e-breach reporting requirements can be avoided. *Id.*

141. F. Scott Fitzgerald, Rich Boy (1926), *reprinted in* The Diamond as Big as the Ritz and Other Stories 171 (Stuart Hutchinson ed., Wordsworth Eds. Ltd. ed. 2006) ("[The rich] are different from you and me.").

142. Kevin D. Mitnick & William L. Simon, The Art of Deception 8 (Wiley & Co. eds., 2002) [hereinafter "Deception"].

143. *Cf.* Ghost, *supra* note 22, at 6, 38, 43 (describing the thrill and encouragement that hackers sometimes receive through their illegal activity).

144. Glenny, *supra* note 18; *see also* Deception, *supra* note 142, at 7 (differentiating hackers "motivated by financial gain" from earlier, ego-driven hackers).

well-defined targets for their potential pecuniary gain.[145] Indeed, hackers view medical identity theft (MIT), which is a "twist" on personal identity theft (PIT),[146] as a very lucrative field.[147]

The street value of MIT information is fifty times that of PIT information.[148] These divergent street values for medical and personal identities arise from two factors: the potential demand for medical identities is greater than that for personal identities; and the time to detect MIT is much longer than that for PIT.[149] In part, the demand for person-specific medical insurance information, the *sine quo non* of MIT, arises from the masses of Americans who are either un- or underinsured.[150] Given that more than 50 million individuals in the United States are uninsured, the potential market for MIT is staggering.[151] In addition, because the perpetration of MIT requires the pairing of medical insurance information and personal identity information, the supply of medical identities is much less than the supply of personal identities.[152] As hackers sell both personal and medical identities in

145. DECEPTION, *supra* note 142, at 7.

146. FED. TRADE COMM'N, FTC FACTS FOR CONSUMERS: MEDICAL IDENTITY THEFT 1 (2010), http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.shtm.

147. Latour "LT" Lafferty, *Medical Identity Theft: The Future Threat of Health Care Fraud is Now*, J. HEALTH CARE COMPLIANCE, Jan.–Feb. 2007, at 11, 15. Careful readers may notice that this Article, in essence, conflates the unauthorized access of protected health information (PHI) with MIT. To a degree this is true and we are well aware that the unauthorized access of PHI and MIT are not synonymous. However, as used in this Article, MIT is viewed primary from the vantage point of the hacker who gains the unauthorized access to an EMR system in order to obtain access to PHI and insurance information. After all, hacking an EMR system provides cyberscribes with one-stop shopping for both components of medical identities. One-stop shopping is a more efficient method for obtaining medical identities than independently obtaining (stealing) an individual's personal identity and their insurance information. *See id.* at 12–13 (describing MIT as a subset of PIT). Accordingly, as used herein, the conflation of the unauthorized access of PHI and MIT is reasonable. *See, e.g.*, Ansh Patnaik, *HITECH, Medical Data Privacy and Fraud*, EXEC. INSIGHT (Nov. 16, 2010), http://healthcare-executive-insight.advanceweb.com/Features/Articles/
HITECH-Medical-Data-Privacy-and-Fraud.aspx (cybercriminals "target general PII [personally identifying information] to execute identity theft").

148. Press Release, Nationwide Mut. Ins. Co., Study: Few Aware of Risk of Medical ID Theft (June 13, 2012), *available at* http://www.nationwide.com/newsroom/061312-MedicalIDTheft.jsp. In general, PHI without insurance information is worthless, unless it is celebrity PHI. Jim Rutenberg, *The Gossip Machine, Churning Out Cash*, N.Y. TIMES, May 21, 2011, at A1.

149. *See* Joseph Conn, *A Real Steal*, 36 MODERN HEALTHCARE 26 (2006).

150. FED. TRADE COMM'N, MEDICAL IDENTITY THEFT: HOW TO MINIMIZE YOUR RISK (2010), http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt179.pdf. In contrast, PIT can be accomplished with as little as a Social Security number. *See* SOCIAL SECURITY ADMINISTRATION, IDENTITY THEFT AND YOUR SOCIAL SECURITY NUMBER 2 (July 2012), *available at* www.ssa.gov/pubs/10064.html (describing what types of identity theft may be accomplished with a Social Security number).

151. Amy Lee, *Number of Uninsured Americans Soars to Over 50 Million*, HUFFINGTON POST (Dec. 27, 2010, 11:39 PM), http://www.huffingtonpost.com/2010/12/27/uninsured-americans-50-million_n_801695.html.

152. The specific need for a real patients' medical insurance information, as opposed to a simple Social Security number, is the likely reason that MIT accounts for only 3% of all identity thefts. *See* FED. TRADE COMM'N, FTC RELEASES SURVEY OF IDENTITY THEFT IN THE U.S. STUDY SHOWS 8.3 MILLION VICTIMS IN 2005 (2007), *available at* www.ftc.gov/opa/2007/11/idtheft.shtm (stating that three percent of MIT victims reported their personal information was used to obtain medical treatment).

underground commodity-like black markets located on the Internet, end users have the opportunity to bid up the price of MIT.[153] However, the degree to which such bidding drives up the price of MIT is unknown.[154]

Yet, in part, the premium paid for medical identities is driven up by the presence of institutional end users in this black market.[155] Institutional end users of medical identities are in a position to submit multiple fraudulent claims to an insurer, whereas individual users of medical identities are only in a position to make one large purchase.[156] Hence, healthcare professionals and bogus healthcare institutions are much more willing to pay a premium for medical identities because these institutional end users are in a position to leverage health insurance information.[157]

To illustrate, consider how an individual and an institutional provider utilize a single medical identity. Assume an individual patient, who lacks health insurance coverage, has coronary artery disease and is in need of a coronary artery bypass grafting (CABG) operation. With a purchase of a medical identity from a black market Internet site, the patient acquires a CABG operation. From the individual patient's perspective, this one-time fraud is worth approximately $20,000, i.e., the dollar-value of CABG operation.[158] Now suppose a crooked (or fake) hospital obtains the same medical identity information. To leverage this medical identity, the hospital first files a claim with an insurer for providing a fictitious $20,000 CABG operation.[159] Then the hospital has this fictitious patient develop a number of billable complications such as postoperative pneumonia ($5,500) and an abnormal heart beat that requires a pacemaker ($12,000).[160] Thus from the hospital's perspective the total value of this fraud is approximately $37,500. As the value of the leveraged medical identity to the hospital is worth almost twice the amount that the medical identity is worth to the individual patient, then all other factors being

153. *The Cyber-Crime Black Market: Uncovered*, PANDA SEC. 13 (2010), http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf ("These types of markets operate in line with the normal laws of supply and demand."); *see also* GLENNY, *supra* note 18.

154. *See generally The Cyber-Crime Black Market: Uncovered*, PANDA SEC. 13 (2010), http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf.

155. Pam Dixon, *Medical Identity Theft: The Information Crime that Can Kill You*, 1 WORLD PRIVACY F. REP. 37, 37 (2006) (explaining how organized crime schemes have begun to engage in medical identity theft).

156. *Id.* at 38.

157. Jonathan Ginsberg, *Medical Identity Theft a Growing Problem*, BANKR. L. NETWORK (Apr. 21, 2012), http://www.bankruptcylawnetwork.com/medical-identity-theft-a-growing-problem. As used in this section, "healthcare professionals" are viewed as any legitimate healthcare provider who may occasionally launder some MIT through their organization's collection system. Ginsberg's use of "bogus clinics" suggests that he views the leveraging of MIT in a narrower, more criminal context.

158. Thomas R. McLean & Valerie Lawson, *Heart Hospitals, Medicare, and Cross-Subsidization*, 7AM. HEART HOSP. J. 94, 96 tbl. 3 (2009) (this figure has been rounded-off and represents the approximate Medicare Allowable Reimbursement figure for Coronary Artery Bypass Grafting).

159. *See, e.g.*, Latour "LT" Lafferty, *Medical Identity Theft: The Future Threat of Health Care Fraud is Now*, J. HEALTH CARE COMPLIANCE, Jan.–Feb. 2007, at 11, 14 (describing an incident of leverage resulting in submission of $2.8 million in false claims).

160. McLean & Lawson, *supra* note 158, at 96.

equal, one would expect a crooked hospital to pay about twice as much money as the individual patient would pay for a medical identity.

The ability of an institutional provider to leverage MIT is related to long latency period between the actual commission of MIT and its detection. When a personal identity is stolen its street value is relatively low because the time between the theft of the personal identity information and the detection of the crime is relatively limited — perhaps to as little as 30 days.[161] After a stolen personal identity has been in circulation for more than 30 days, the individual whose identity was stolen often notices unauthorized charges on credit card bills or starts to receive bills from companies that they have no prior relationship.[162] Additionally, financial institutions that are involved in credit lending are highly adept at spotting financial fraud.[163]

MIT, on the other hand, which is predicated on the theft of insurance information, is in a different situation.[164] Unlike VISA and American Express, health insurers do not routinely send out monthly statements.[165] In general, insurers only send out a statement of benefits after a claim for services has been made.[166] Even then an insurer may not send the statement to the patient's attention for one or two billing cycles.[167] This delay in sending a patient-policy holder information regarding care that was allegedly rendered to the patient is a key reason that institutional healthcare providers are able to leverage MIT.[168]

For the victims of MIT, the long latency period between the commission of an act and its detection can have devastating consequences.[169] These consequences may be psychological, financial, or both. The psychological damages associated with

161. Katherine M. Sullivan, *But Doctor, I Still Have Both Feet! Remedial Problems Faced by Victims of Medical Identity Theft*, 35 AM. J. LAW & MED. 647, 655 (2009) (indicating that person will generally discover a stolen identity within a month, when they receive a credit statement).

162. *Id.* at 31 (finding that "52 percent of victims of financial identity theft discovered the misuse of their personal information 'by monitoring the activity in their accounts'").

163. *Id.* at 39. Moreover, with online banking, personal identity theft can theoretically be detected within hours. Assume John Doe, living in Austin, TX, goes to dinner on Friday night. On Saturday morning, he wakes up and checks his transactions online to make sure he was charged the correct amount for his dinner. Upon logging on he discovers that 2 minutes after he authorized the transaction for his dinner, a $25 charge occurred for 2 beers at Wrigley Field in Chicago. It would be fair for John Doe to assume that someone had his credit card information and was using his identity to be a bleacher bum in Chicago.

164. *Id.* at 5 (defining MIT).

165. *Id.* at 31 (observing that the mechanisms banks and credit card companies use to detect fraudulent activity are not feasible solutions in detecting MIT).

166. *See* Sullivan, *supra* note 161, at 656 (describing the administrative process following a claim for benefits).

167. *Id.* at 656. This statement is especially true if the healthcare provider has not filed a timely claim for reimbursement with the insurer.

168. *Id.* at 656 (attributing late notification of MIT victims to lags in healthcare billing and processing).

169. *Medical ID Theft is Latest Twist on Identity Theft*, CBS NEWS 4 DENVER (May 1, 2012, 10:53 AM), http://denver.cbslocal.com/2012/05/01/medical-identity-theft-is-latest-twist-on-identity-theft (moreover, MIT can be "almost impossible for a victim to fix").

MIT arise because the imposter's medical information often becomes comingled with the victim's medical information.[170] This comingling of the imposter-legitimate patient information can trigger fears in the legitimate patient that they will receive the wrong treatment.[171] For example, one non-diabetic victim of MIT worried about being erroneously treated with insulin after a diabetic impostor stole her medical information.[172] Worse, the victims of MIT are often saddled with significant financial damages. On average, victims of MIT spend $20,000 to clean up their medical records.[173] The loss of insurance coverage must often be added to this figure. Although several reasons have been articulated for why insurers cancel a health insurance policy after it has been stolen, the bottom line for the victims of MIT is that 48% of these individuals lose their healthcare insurance coverage.[174]

The flip side of the victims' losses are the hackers' net gains, which are potentially substantial, especially in aggregate.[175] To illustrate the net profits that can flow from a hackers' attack on an EMR system, assume that four hackers form an equal partnership to engage in MIT.[176] The partnership targets the EMR system at Man's Best Friend (MBF), a large, well-endowed hospital, located in the fictional city of Megopolis, with a population of 17 million people.

The partnership's first step is to identify hospital insiders who can facilitate the MIT. To this end the partnership purchases a report for $120[177] from a data aggregator that contains a profile of everyone living in Megopolis.[178] From this report, the partnership identifies all individuals in Megopolis employed by MBF, and from these individuals the partnership identifies three hospital insiders who work in the hospital's IT department and are highly likely to have a drinking

170. BOOZ ALLEN HAMILTON, OFF. NAT'L COORDINATOR HEALTH INFO. TECH., U.S. DEP'T OF HEALTH & HUMAN SERVS., MEDICAL IDENTITY THEFT ENVIRONMENTAL SCAN 9 (Oct. 2008).

171. *See Diagnosis: Medical Identity Theft*, BLOOMBERG BUS. WK., Jan. 7, 2007, *available at* http://www.businessweek.com/magazine/content/07_02/b4016041.htm (accounting for one woman's worry about being treated according to inaccurate medical records).

172. *Id.* Theoretically, HIPAA directs that patients are to have access to their EMR so that they can make corrections when necessary. *See* 45 C.F.R. §§ 164.524, 164.528 (2011) (giving patients the right of access to their protected health information and the right to an accounting of disclosures of protected health information). As this vignette demonstrates, laws are often more Platonic ideals and less like the bureaucratic real world. *See generally* Plato, THE REPUBLIC (Project Gutenberg ed., Benjamin Jowett trans. 2008).

173. PONEMON INST., *supra* note 4, at 13.

174. *Id.* at 10; *see* Dixon, *supra* note 155, at 29 ("Victims of identity theft can be denied insurance due to imposter activity.").

175. PONEMON INST., *supra* note 4, at 1, 14 (finding that the average value of stolen services, products and pharmaceuticals was $29,464 and, as there were an estimated 1.85 million people affected, this could come out to $54.5 billion per annum).

176. While this is a hypothetical, the stratagems employed herein are modeled on the real life adventures of ex-hacker Kevin Mitnick. *See generally* GHOST, *supra* note 22.

177. Marc Porcelli, *ISP Targeting Ad Company Phorm Gets Targeted* (Mar. 23, 2008), http://www.marcporcelli.com/2008/03/23/isp-targeting-ad-company-phorm-gets-targeted (data aggregators charge advertisers $4 to $12 per million individuals for a focused audience).

178. For a more detailed discussion of data aggregators, see *infra* note 197 and accompanying text.

problem.[179] The partnership then spends $21,000 on these three employees by purchasing them a weekend trip to Las Vegas, where the employees are wined, dined, and compromised.[180] For their trouble, the partnership learns the MBF's EMR is cloud-based system that has an e-security risk in the form of an unpatched backdoor.

The partnership then purchases a computer system for $35,000[181] and spends $48,000 to develop targeted malware.[182] The malware is coded so as to locate the MBF's EMR system's backdoor and then attach itself to MBF's EMR system. The attack enables the hacker to copy and email different patients medical records — including PHI and insurance information — to the partnership. This process continues until the partnership has possession of 8 million medical identities,[183] at which point the partnership elects to shut down its attack.

The partnership now has to launder these 8 million medical identities. Assume here that the partnership is able to sell only half of these medical identities because it fears that by selling all 8 million simultaneously, it will flood the black market thereby driving down the price per medical identity. Indeed, during the course of four cyber auctions held during the next year,[184] the partnership is able to sell 2 million medical identities for $50 each on average, but is only able to sell an

179. This would not be hard to do. For example, consider an individual who makes credit card purchases from a liquor store for $20,000 per year but who makes no other purchase consistent with throwing parties. Such an individual is likely to be either an alcoholic or a serious sommelier. Data aggregators may also find other information indicating excessive drinking habits.

180. This figure is based on the average cost to wine and dine government workers at a recent scandalous lobbying event. Courtney Subramanian, *GSA Scandal: So What Does $823,000 Buy You in Las Vegas?*, TIME NEWSFEED (Apr. 18, 2012), http://newsfeed.time.com/2012/04/18/gsa-scandal-so-what-does-823000-buy-you-in-las-vegas; *see also* GLENNY, *supra* note 18, at 32 (perpetrators of Internet fraud "invest considerable effort in trying to find disgruntled or distressed" employees who have the type of knowledge that will facilitate the planned crime).

181. Michelle Stephenson, *EHR Computing: In-House or in the Cloud?*, REV. OPHTHALMOLOGY (Jan. 10, 2012), http://www.revophth.com/content/c/31831 (noting that "[f]or the client-server option, the up-front fee is typically $35,000").

182. This figure is a rough estimate based on the cost of launching a botnet attack, which is a different type of an attack than described here. *See* Pierluigi Paganini, *How Much Does Malware Production Cost? Which Are the Processes for the Production of Virus? (Part.2)*, SEC. AFFAIRS (Dec. 6, 2011), http://securityaffairs.co/wordpress/430/cyber-crime/how-much-cost-malware-production-which-are-the-processes-for-the-production-of-virus-part-2.html. *See generally* GHOST, *supra* note 22, (costs could be less for the attack described here if the hacker knew of specific vulnerabilities and how to attack them). *But see generally* GLENNY, *supra* note 18.

183. This figure is based on the MIT from a Virginia hospital. *See* Brian Krebs & Anita Kumar, *Hackers Want Millions for Data on Prescriptions*, WASH. POST, May 8, 2009, at B01.

184. *See* Erin Kenneally & Jon Stanley, *Beyond Whiffle-Ball Bats: Addressing Identity Crime In An Information Economy*, 26 J. MARSHALL J. COMPUTER & INFO. L. 47, 88 (2008) (citing DEAN TURNER ET AL., SYMANTEC INTERNET SECURITY REPORT: TRENDS FOR JANUARY-JUNE 2007 (2007), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf) (describing an online underground economy for selling stolen identities); s*ee also* GLENNY, *supra* note 18.

additional 2 million medical identities for $25 each on average.[185] Of course, because the cyber platform that runs the auction is dealing in stolen goods, the partnership has to pay the cyber platform a 20% commission.[186] The partnership is now ready to unwind and distribute the millions of dollars of net proceeds of the enterprise. Table II summarizes the partnership's finances. The approximately $100,000 to fund this operation could be a real entry barrier for those individuals who are not seriously interested in a life of MIT. Still, these expenses are little more than round off error when the size of the net revenue to the partnership is considered. The bottom line is that the four individual partners would each pocket about $30 million.

Table II: Hypothetical MIT Enterprise Financials

Expenses:		Revenue:	
Data Aggregator Report	$ 120	2 M identities at $50	$100 million
Cost of Information	$ 21,000	2 M identities at $25	$ 50 million
Computer	$ 35,000		
Software development	$ 48,000	Less Commission	($ 30 million)
Net expense	$104,120	Net revenue	$ 120 million

Based on these figures, MIT is likely to be profitable at volumes much lower than those used in this hypothetical. This fact alone suggests that as more and more healthcare providers purchase EMRs during the next three years,[187] the incidence of MIT is likely to continue to rise, unless hackers' incentives are changed.[188] Second, the primary barrier to committing MIT (after software development) appears to be the ability to distribute medical identities to end users.[189] As more hackers enter the

185. The disparate prices for medical identities used herein are an attempt to reflect real world situations. Cyberscribes do fear that flooding the market with MIT may drive the per unit price down. *See* Kenneally & Stanley, *supra* note 184 at 49–50 (citing *Free Market*, INVESTORWORDS.COM (last visited Oct. 9, 2012), http://www.investorwords.com/2086/free_market.html); *see also* GLENNY, *supra* note 18; FED. TRADE COMM'N, FTC FACTS FOR CONSUMERS: MEDICAL IDENTITY THEFT (2010) (adopting the view that the commission of MIT is analogous to the commission of PIT). In the real world, not every patient has health insurance. So, given our premises, it would be illogical for us to assert that cyberscribes could obtain a medical identify from every record they hacked.

186. *See* GLENNY, *supra* note 18 (cyber auction houses get a cut of the gross proceeds); *see also* Sean Rocha, *How Does a Sotheby's Auction Work*, SLATE (May 7, 2004), *available at* http://www.slate.com/articles/news_and_politics/explainer/2004/05/how_does_a_sothebys_auction_work.html. Although establishing the average commission rate for illegal cyber auctions is difficult for obvious reasons, it is not unreasonable to assume that many such transactions have maintained the 20% figure for commissions of legitimate transactions.

187. *See infra* Part IV.

188. *See infra* Part IV.

189. *See* DEAN TURNER ET AL., SYMANTEC INTERNET SECURITY REPORT: TRENDS FOR JANUARY-JUNE 2007 41 (2007) *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_

MIT market, the need to distribute stolen medical identities will tend to limit market growth.[190] In part, hackers who subsequently enter the market will stifle market growth by flooding the market with medical identities thereby driving down the price per medical identity.[191] And in part, just as the credit lending financial institutions have become adept at detecting financial fraud, as more bogus medical identities circulate in the healthcare market, health insurers are likely to become more knowledgeable about how MIT is perpetrated[192] and are hence likely to become more efficient in detecting MIT.[193]

In the above hypothetical, the hacker enterprise wines and dines insiders to get information. In the world of hackers, this type of information gathering is referred to as social engineering. Broadly speaking, social engineering encompasses the techniques used by one individual to gain the trust of another individual such that the second individual reveals confidential information to the former.[194] In their book, *The Art of Deception*, Mitnick and Simon chronicle the various social engineering techniques that are used by hackers to gain confidential information about their targeted computer systems.[195] For the most part, the trust building techniques of social engineering, which require a modicum of patience, allow the hacker to obtain valuable information like passwords, authentication procedures, and information about the nature of a computer system.[196]

---

security_threat_report_xii_09_2007.en-us.pdf (showing that criminals use underground economy servers to sell stolen information).

190. The market for MIT data will follow the diminishing returns law. *See* DONALD RUTHERFORD, ROUTLEDGE DICTIONARY OF ECONOMICS 105 (Taylor & Francis ed. 2005).

191. *See* sources cited *supra* note 185.

192. *Cf.* GLENNY, *supra* note 18. Credit lending agencies are disinterested in identifying or disclosing PIT and other cyber frauds. In part, this is because credit-lending agencies do not want the public and their competitors to know that they have been hacked; and in part this is because such agencies have a moral hazard. *Id*. As credit lending agencies have PIT insurance, these agencies are all too willing to write off losses to PIT and cyber fraud, which are covered by insurers. Of course, the insurers will then raise the credit lending agencies premiums, but these agencies then pass the premium costs off to debtors in the form of higher fees. *Id*.

193. For example, EMR administrators should be looking for medical information that is transferred during the dead of night, in unusual volumes, or to unusual destinations. *E.g.,* MCAFEE, SECURITY AND PRIVACY OF ELECTRONIC MEDICAL RECORDS 4 (2012) *available at* http://www.mcafee.com/us/resources/white-papers/wp-security-privacy-medical-records.pdf. However, a detailed discussion of the standard of care for an EMR administrator is beyond the scope of this Article. *See generally Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, REP. BRIEF (Inst. Med., Wash., D.C.), Feb. 2009, at 1 *available at* http://www.iom.edu/~/media/Files/Report%20Files/2009/Beyond-the-HIPAA-Privacy-Rule-Enhancing-Privacy-Improving-Health-Through-Research/HIPAA%20report%20brief%20FINAL.ashx (detailing problems with protecting patient privacy under HIPAA regulations).

194. *See* DECEPTION, *supra* note 142, at iv (describing social engineering); *see also* GLENNY, *supra* note 18, at 24 ("[I]t is a little-appreciated fact the very best computer managers are as talented in managing the social and psychological expectations as they are fixing widgets.").

195. DECEPTION, *supra* note 142.

196. *See* Daniel E. Geer, Jr., *Cybersecurity and National Policy*, 1 HARV. NAT'L SECURITY J. 203, 208 (2010) ("[W]ithout universal strong authentication, tomorrow's cybercriminal will not need the fuss and bother of maintaining a botnet when, with a few hundred stolen credit cards, he will be able to buy all the virtual machines he needs from cloud computing operators.").

Certain cyberscribes — or more exactly, organizations of cyberscribes — known as data aggregators specialize in such data collection.[197] For example, using multiple online sources, data aggregators like Spokeo[198] have compiled as many as 1,500 data points for every Internet user.[199] Based on these profiles, data aggregators will develop composite profiles ("second selves") for each Internet user; and these profiles can then be purchased by advertisers to develop individual-specific marketing strategies.[200]

Our second selves' composites are not cyber doppelgangers of our real world selves. Still, the second selves are not unreasonable facsimiles of our real world selves.[201] These second selves offer insight into our strengths and weaknesses. Second selves can suggest to advertisers which of us are religious, enjoy alcohol, or take risks. In addition, these second selves can suggest to hackers how best to social engineer us.[202] After all, social engineering is nothing more than "human hacking" in that it involves the profiling of an individual by piecing together all the little bits of the person's identity specific data, including: name, age, birthday, and personal preferences.[203] In the hypothetical of the hacker criminal enterprise, the partnership purchased a data aggregator's report to streamline their social engineering attack.

This is not to say that aggregator-based social engineering will replace all human mediated social engineering. In our hypothetical, once the partnership had identified the three IT employees who had a potential drinking problem, the partnership still had to have some of their members personally socialize with these employees to gain their trust. But, group personality profiles from data aggregators will almost certainly act as a catalyst for human mediated social engineering. So, if the MIT market does expand in parallel with our use of EMRs, it is likely that data aggregators will see a rising demand for the profiles of current and former healthcare providers, hospital administrators, and hospital maintenance workers, since these individual might have valuable insider information.[204]

---

197. *E.g.*, Joseph Nocera, *Data Theft: How to Fix The Mess*, N.Y. TIMES, July 9, 2005, at C1 (describing the activities of a data aggregator).

198. *See* ANDREWS, *supra* note 85, at 9 (describing the creation of Spokeo); *see also* LEVY, *supra* note 106, at 46 (As Google uses personal data when composing its online advertisements, Google is almost certainly the largest data aggregator).

199. ANDREWS, *supra* note 85, at 35.

200. *Id.* at 35.

201. *Id.* at 35; *see also* GLENNY, *supra* note 18.

202. *See* DECEPTION, *supra* note 142, at iv (observing that by posing as another individual, "the social engineer is able to take advantage of people to obtain information"). For example, if a cyberscribe knows that members of the targeted organization are religious (think of the right to life movement), the cyberscribe may use a religion-based phishing attack to gain insider's trust.

203. *See generally* CHRISTOPHER HADNAGY, SOCIAL ENGINEERING: THE ART OF HUMAN HACKING (2010).

204. *See, e.g.*, Press Release, U.S. Att'y Off. N.D. Ga., Atlanta Man Sentenced on Computer Hacking Charge (Jan. 10, 2012), *available at* http://www.justice.gov/usao/gan/press/2012/01-10-12.html (reporting the prosecution of a man charged with specifically targeting computers in a medical practice to aggregate personal information on patients of that practice).

Moreover, with sufficient social engineering, current employees may be enticed into participating in a medical information embezzlement scheme.[205] To cope with health information technology employees who are susceptible to, or who are actively being compromised by hackers, hospital risk managers should consider stepping up their counter-intelligence programs. Given the value of medical identities, hospitals need to identify and help health information technology employees who are at risk of social engineering tactics.[206]

Indeed, an MIT epidemic seems to be just around the corner. During a recent three-year period one report found that the incidence of MIT had doubled;[207] while other reports document more modest growth in MIT (in the range of 32%[208] to 47%[209] per year). Similar to the existing epidemic in PIT,[210] which is predicated on the ability of criminal organizations to exploit jurisdictional and legal loopholes in overseas countries,[211] the coming epidemic of MIT will also be driven by social engineering and favorable economics that promote organized criminal activity.[212] The Obama administration's $29 billion stimulus for the conversion of paper medical records to EMR by 2015[213] could be

205. *See* Assoc. Press, *California: U.C.L.A. Reports Theft of Patient Data*, N.Y. TIMES, Nov. 5, 2011, at A11 (citing statistics and an example of hospital employees illegally accessing medical records). The potential for using MIT to defraud healthcare providers has already been discussed. Such a fraud scheme does not necessarily have to involve the business owners and could easily be perpetrated by a financial manager with access to billing and accounts receivable. *See also infra* Part IV (describing HIPAA criminal litigation).

206. *See* Chris Apgar et al., *Mitigating Medical Identity Theft*, 79 J. AHIMA 63, 66 (2008) (recommending that healthcare employers "[e]nsure appropriate background checks of employees and business associates, both prior to hiring and in high-risk areas, as well as periodically after hiring. Consider minimizing the use of noncredentialed or nonlicensed individuals in temporary positions if they are not bound by professional codes of conduct or ethics").

207. N. Nedim Halicioglu, *The Rise of Medical Identity Theft*, VALLEY BUS. J. 1, http://www.valleybusinessjournal.com/archived-front-page-articles/420-the-rise-of-medical-identity-theft- (last visited Oct. 15, 2012).

208. PONEMON INST., *supra* note 4, at 5 (showing a 32% increase in per capita cost of data breach from 2005 to 2006).

209. *Patient Medical Records Hacking: The Unintended Consequences of Health Care Reform*, LWG CONSULTING, http://www.lwgconsulting.com/casestudy/default.aspx?CaseStudyId=156 (last visited Sept. 22, 2012) (citing *2008 Data Breach Total Soars: ITRC Reports 47% Increase Over 2007*, IDENTITY THEFT RESOURCE CENTER (2009) *available at* http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml).

210. *See* Brian Krebs, *Organized Crime behind a Majority of Data Breaches*, WASHINGTONPOST.COM (Apr. 15, 2009, 10:22 AM) http://www.washingtonpost.com/wp-dyn/content/article/2009/04/15/AR2009041501196.html (citing VERIZON BUSINESS, 2009 DATA BREACH INVESTIGATIONS REPORT 6 (2009), *available at* www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf (reporting that data breaches in 2008 affected "roughly 285 million consumer records")).

211. GLENNY, *supra* note 18.

212. *See* VERIZON BUS., 2010 DATA BREACH INVESTIGATIONS REPORT 2 (2010), *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf (showing a recent 16% increase in the use of social tactics in data breaches).

213. *See* HITECH Act, Pub. L. No. 111–5, § 13001, 123 Stat. 226 (2009) (requiring utilization of EHRs for all patients by 2014); *see also* David Blumenthal, *Wiring the Health System – Origins and Provisions of a New Federal Program*, 365 NEW ENG. J. MED. 2323, 2323 (2011) (observing that even though this technology stimulus

like throwing gasoline on a fire.[214] Currently, only 40% of healthcare providers are using EMR.[215] So, a shift to nationally-sponsored EMR adoption is likely to more than double the number of EMR systems in use during the next five years.[216]

For many cash strapped healthcare providers,[217] monies from the Obama stimulus package are unlikely to cover the full cost of conversion to an EMR system.[218] Consequently, it is possible that the majority of EMR systems that become operational in the next few years are likely to be the less secure, but more economical, cloud-based systems.[219] Less secure EMR systems and the lucrative returns associated with MIT will invite criminal organizations into the MIT market. A similar evolution from individual hackers seeking thrills to organized criminal activity occurred in the PIT market. Where PIT was once a crime of opportunity,[220] it is increasingly a planned gang related activity.[221]

---

package is to be paid out over ten years, such funding of technology by the United States government is virtually unprecedented).

214. "The widespread, accelerated diffusion of [IT] technology resulting from recent legislation [the HITECH Act] may engender unintended consequences manifested in various ways throughout those organizations under pressure to accommodate the changes." Meryl Bloomrosen et al., *Anticipating and Addressing the Unintended Consequences of Health IT and Policy: A Report from the AMIA 2009 Health Policy Meeting*, 18 J. Am. Med. Inform. Assoc. 82, 87 (2011).

215. Eric Jamoom et al., Dep't Health & Human Servs., NHCS Data Brief No. 98, Physician Adoption of Electronic Health Record Systems: United States, 2011 (July 2012), *available at* http://www.cdc.gov/nchs/data/databriefs/db98.pdf.

216. This assumes that number of healthcare providers remains constant; an assumption that is unlikely to be true. *See* Barry Liss, *The Current Wave of Hospital Consolidation: Cause and Effect*, Metro. Corp. Couns. 8 (Feb. 22, 2012) http://www.metrocorpcounsel.com/articles/17931/current-wave-hospital-consolidation-cause-and-effect (the nation's economy and economic incentives under the Patient Protection and Affordable Care Act [Pub. L. 111–148 (2010)] will result in hospital closures and overall market consolidation); *see also* Merritt Hawkins, Health Reform and the Decline of Physician Private Practice: A White Paper Examining the Effects of the Patient Protection and Affordable Care Act on Physician Practices in the United States 4 (2010) (same with respect to physicians); Thomas R. McLean, *The 80-Hour Work Week: Why Safer Patient Care Will Mean More Health Care Is Provided By Physician Extenders*, 26 J. Legal Med. 339, 341 (2005) (the impact of patient safety and economics will mean fewer physicians will be needed in the market).

217. *See supra* note 216.

218. *See infra* Part IV.

219. *See supra* Part II.A. If EMR systems do evolve to become less secure, one of Congress' intended outcomes for the HITECH Act will be defeated. "Congress recognized that expanding the use of health IT would be futile if patients and providers came to feel that their information was safer in a paper chart than in electronic format. Therefore, HITECH was seen as the right time to update and strengthen" HIPAA's privacy and security rules. Pete Stark, *Congressional Intent for the HITECH Act*, 16 Am. J. Manag. Care SP24, SP26 (Supp. 2010).

220. From 2004 to 2007 large scale cyberscribe activity was historically opportunistic in that the computer systems targeted by cyberscribes where selected because of known e-security flaws rather than the identity of the user. In more recent years, 90% of the computer systems targeted by cyberscribes were selected after the cyberscribes had "carefully picked their targets first and then figured out a way to exploit them." *See* Krebs, *supra* note 210 (citing Verizon Bus., 2009 Data Breach Investigations Report (2009), http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf).

221. *E.g.*, Charles Arthur, *Court Papers Reveal Hacker Worked for FBI*, Australian Fin. Rev., Mar. 7, 2012, http://afr.com/p/technology/court_papers_reveal_hacker_worked_WXtfHK9KoyWcqa5ZAil8cL (reporting that a particular hacking crew of ten people undertook several concentrated attacks against specific institutional targets). *See also* Glenny, *supra* note 18.

For many, the more evolutionary view of cybercrime may appear strange. This is because our societal images of cybercrime are rooted in the motion picture industry, which views hackers as college-aged kids on a misadventure[222] or correcting a social injustice.[223] This antiquated view, however, is no longer valid. Today, 85% of PIT is committed by gangs with organized goals.[224] The complexity of code writing, coupled with the importance of social engineering to cybercrime,[225] means that these gangs have had to develop divisions of labors amongst their members.[226] And, according to the Obama administration, many of these gangs are "tied to traditional Asian and Eastern European organized crime organizations."[227]

As MIT is every bit as complex, sophisticated, and organized as PIT, organized criminal gangs seem destined to enter the MIT market. Already, the size and scope of many healthcare e-security breaches suggest the extent to which MIT is becoming increasingly organized.[228] As one commentator has observed, MIT is frequently "carried out by organized crime rings — often with the help of corrupt health care workers."[229] This observation raises an interesting question: Will MIT gangs be dominated by foreign hackers to the extent that PIT is dominated by foreign hackers?[230]

As of today, this question remains hypothetical. Our review of healthcare e-security breaches failed to identify a single hacker attack of an EMR system that involved foreign nationals. Still, from a legal point of view, if MIT is committed by overseas gangs of hackers, obtaining effective jurisdiction over these hackers is likely to become a substantial issue in curtailing MIT.[231] Under the Constitution, Congress has the power to punish felonies "committed on the high Seas and Offense against

222. *E.g.*, SNEAKERS (Universal Pictures 1992).

223. *E.g.*, THE ITALIAN JOB (Paramount Pictures 2003).

224. GLENNY, *supra* note 18.

225. *See* VERIZON BUS., 2010 DATA BREACH INVESTIGATIONS REPORT 2 (2010), *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf (showing a recent 16% increase in the use of social tactics in data breaches).

226. *See* Kenendra Srivastava, *Obama Says Hacks Are Organized Crime, Wants Stiffer Penalties*, MOBILE MEDIA (Sept. 9, 2011, 11:35 AM), http://www.mobiledia.com/news/107373.html (reporting that PITs are "complex and sophisticated electronic crimes are rarely perpetrated by a lone individual"); *see also* GLENNY, *supra* note 18.

227. Srivastava, *supra* note 226.

228. Krebs, *supra* note 210 (citing VERIZON BUS., 2009 DATA BREACH INVESTIGATIONS REPORT 6 (2009), *available at* www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf).

229. Dale Dixon, *The Biggest Threat in Medicine: Medical ID Theft*, IDAHO PRESS-TRIB. BLOG (Apr. 11, 2011, 12:52 PM) http://www.idahopress.com/blogs/business_to_business/dale_dixon_-_better_business_bureau/the-biggest-threat-in-medicine-medical-id-theft/article_0d7c6f8a-c2b9-11e0-8302-001cc4c03286.html.

230. Most PIT is perpetrated by Chinese, Russian, and other Eastern Europeans on Americans, the British, and Canadians. There are many reasons for this pattern of criminal activity, including culture and legal systems. *See generally* GLENNY, *supra* note 18.

231. *See* Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet*, 50 FED. COMM. L.J. 117, 120 (1997) (observing that "[j]urisdictional questions have become increasingly complex with the explosion in Internet usage and technology").

the Law of Nations"[232] and to "regulate Commerce with foreign Nations."[233] Thus, under Article I of the Constitution, the United States does have extraterritorial jurisdiction for criminal acts that occur here. Unfortunately, the scope of this extraterritorial jurisdiction is not unlimited and a number of obstacles (both practical and diplomatic) to the enforcement of extraterritorial jurisdiction exist.[234]

IV. Cyberlaw as a Deterrent to EMR e-Security Breaches

So, if during the next five years healthcare providers uniformly adopt cloud-based EMRs and organized gangs of hackers are formed, which have the tools, know-how, and economic incentives to commit MIT, what is there to deter them? Conceptually, a deterrence to hacker attacks could be created by enacting laws with harsh penalties that impose sufficient economic disincentives to dissuade hackers from committing MIT; or alternatively, the conditions under which our healthcare payment system operates could be changed so that the street value of PHI plummets to zero. We begin with an examination of the relevant laws.

There are numerous federal anti-hacker laws, including: HIPAA,[235] as modified by the Health Information Technology for Economic and Clinical Health (HITECH) Act[236] (which is part of the American Recovery and Reinvestment Act of 2009);[237] the Electronic Communications Privacy Act (ECPA),[238] with its two principle components the Federal Wiretap Act (FTWA)[239] and Stored Communication Act (SCA);[240] and the Computer Fraud and Abuse Act (CFAA).[241] As HIPAA has been a federal law for almost two decades, basic knowledge of this law is assumed.[242] In addition, because the scope of the CFAA is limited to situations

232. U.S. Const. art. I, § 8, cl. 10.

233. U.S. Const. art. I, § 8, cl. 3.

234. *See generally* Charles Doyle, Cong. Research Serv., No. 94-166, Extraterritorial Application of American Criminal Law (Feb. 15, 2012).

235. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, § 1, 110 Stat. 1936 (1996).

236. HITECH Act, Pub. L. No. 111–5, § 13001, 123 Stat. 226 (2009).

237. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111–5, § 1, 123 Stat. 115 (2009). The dollar value of the "Stimulus Act," *id.*, is fantastic. If you had spent a million dollars a day, every day since the year 0 C.E., the total money available under this Act would still be more.

238. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, § 101, 100 Stat. 1848 (1986).

239. 18 U.S.C. §§ 2510–22 (2006).

240. 18 U.S.C. §§ 2701–12.

241. 18 U.S.C. § 1030 (2006).

242. However, the key concepts relevant to understanding this Article with respect to HIPAA and the HITECH Act (Privacy & Security Rule, covered entity, and business associates) are briefly reviewed. In the healthcare context, hackers seek to obtain Protected Health Information (PHI), and not control of, or the ability to take down a computer. If an e-document contains PHI, then covered entities, 45 C.F.R. §164.530 (2011), and business associates, 42 U.S.C.A. § 17921(2) (2012), have certain obligations to protect the confidentiality of the document. *See infra* notes 243–97 and accompanying text.

of unauthorized access to the federal government's computers,[243] this Act will also not be discussed further.[244]

A. HITECH Act

The HITECH Act is a dual purpose act. The Act's first purpose is to stimulate the use of EMR such that virtually all healthcare providers will be using an EMR system by the end of 2014.[245] Based on the Obama administration's calculations, the HITECH Act's liberal distribution of $20 billion for EMR conversion startup money[246] would ultimately return to the government $80 billion in annual savings.[247]

The second purpose of the HITECH Act is to regulate the transmission of EMRs and cEMD e-data.[248] Under HITECH, HIPAA's regulations regarding the handling and transmission of EMRs are modified by two mechanisms: the creation of a new

243. 18 U.S.C. § 1030(a) (2006). CFAA's scope reaches to the extent of the Act's jurisdiction so the Act covers computers with "information of the federal government, consumer credit or other kinds of financial information, and information acquired from a protected computer." CHARLES DOYLE, CONG. RESEARCH SERV., 97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 16 (2010). *Cf.* United States v. Nosal, 642 F.3d 781 (9th Cir. 2011) (noting the scope of CFAA does not extend to cover employees who merely misappropriate government files in violation of employer's work policy).

244. Most of the principles articulated in the CFAA are similar to those found in the HITECH Act and ECPA. Perhaps one key difference between the CFAA and the other acts discussed herein is that under the CFAA the criminal penalties for violating the Act (up to 20 years (18 U.S.C. § 1030(c)(1)(B) (2006))) are substantially harsher than the penalties for violation of the HITECH Act or ECPA. *See infra* Parts IV.A–B. However, the CFAA should be kept in mind by attorneys involved in litigation that concerns e-security breaches involving the Department of Veterans Affairs' EMR system.

245. Robert Steinbrook, *Health Care and the American Recovery and Reinvestment Act*, 360 NEW ENG. J. MED. 1057, 1059 (2009) (the Congressional Budget Office projects the incentives will result in the adoption of comprehensive EHRs by 90% of physicians and 70% of hospitals by 2019).

246. *See* Helen Christophi, *EHRs Fuel Controversy in Healthcare Industry*, HC+O NEWS (Jan. 25, 2011), http://www.hconews.com/articles/2011/01/25/ehrs-fuel-controversy-in-healthcare-industry (beginning in 2015 providers who have not adapted EMR technology will be penalized). The amount of stimulus dollars provided by the HITECH Act for EMR adoption ranges from $20 to $29 billion, a spread of roughly 30%. *Compare id.* (Federal government appropriated $20 billion for the computerization of patients health records), *with* PATIENT MEDICAL RECORDS HACKING: THE UNINTENDED CONSEQUENCES OF HEALTH CARE REFORM, http://www.lwgconsulting.com/casestudy/default.aspx?CaseStudyId=156 (last visited Apr. 1, 2012) (Federal government appropriated $29 billion for the computerization of health records). As HITECH's stimulus dollars are to be released over a decade and depend on the degree to which providers embrace meaningful use, *see* Part IV.A, the literature values for the HITECH stimulus package are not necessarily incompatible (depending on the assumptions the authors made). Herein we used the figures found in our source material, but recognize that from paragraph to paragraph the dollar-value of the HITECH stimulus package shifts.

247. Christophi, *supra* note 246. *But see* Danny McCormick et al., *Giving Office-Based Physicians Electronic Access to Patients' Prior Imaging and Lab Results Did Not Deter Ordering of Tests*, 31 HEALTH AFF. 488, 491 (2012) (demonstrating that doctors who have access to EMRs are 40% more likely to order imaging studies than those using paper medical records); *see* Steve Lohr, *Digital Records May Not Cut Health Costs, Study Cautions*, N.Y. TIMES, Mar. 5, 2012, at B1.

248. *See generally HITECH Act Expands HIPAA Privacy and Security Rules*, COPPERSMITH, GORDON, SCHERMER & BROCKELMAN PLC, http://www.azhha.org/member_and_media_resources/documents/HITECH Act.pdf (last visited Apr. 14, 2012).

reporting requirement for major e-security breaches and the expansion of enforcement actions through both the enlargement of the scope of the Privacy and Security Rules[249] and through the creation of heightened penalties for non-compliance.[250]

The HITECH Act modifies HIPAA's personal notification requirements for e-security breaches and creates a new public notification requirement.[251] Under HIPAA, covered entities (CEs) are required to maintain an audit trail.[252] If this audit trail (technically metadata)[253] reveals that a patient's PHI[254] has been compromised, the CE has an obligation to provide private notification of the e-security breach to patient-owner(s) of the PHI. Under the HITECH Act, in the event of an e-security breach,[255] both CEs[256] and Business Associates (BAs)[257] are required to notify the patient-owners that their PHI has been compromised. Importantly, CEs and BAs are required to give such notification within sixty days of the security breach.[258]

HITECH then goes further than HIPAA to create a public reporting requirement in the event of a major EMR security breach.[259] There can be little doubt that a key reason behind the public reporting requirement for e-security breaches involving

249. A comprehensive discussion of HITECH's expansion of the Privacy Rule is beyond the scope of this Article. However, topics not covered in detail here with respect to the expansion of the Privacy Rule include: under the HITECH Act, if the patient has paid for the service out of pocket, covered entities (CEs) must now honor a patient's request to restrict disclosure of their PHI. 42 U.S.C.A. § 17935(a)(2) (2012); *see also HITECH Act Expands HIPAA Privacy and Security Rules*, *supra* note 248, at 5–6. In addition, when a CE does make a disclosure, it alone must make the determination of the minimally necessary amount of PHI to disclose. 42 U.S.C.A. § 17935(b)(2) (2012). CEs may not receive any remuneration for the disclosure (without the patient's approval). 42 U.S.C.A. § 17935(d)(1) (2012). Several exceptions (e.g., disclosures for public purpose or research) to this rule exist. 42 U.S.C.A. § 17935(d)(2) (2012); *see also* 42 U.S.C.A. § 17936(a) (2012) (limiting the remuneration a covered entity can receive for HIPAA permitted marketing).

250. *See HITECH Act Expands HIPAA Privacy and Security Rules*, *supra* note 248, at 8.

251. *See* 42 U.S.C.A. § 17932(e)(2) (2012) (outlining public reporting requirement).

252. *See id.* § 17932(f) (outlining the content of notification).

253. An automatically generated computer record that certifies how an electronic document has been manipulated. Thomas R. McLean, *EMR Metadata Uses and E-Discovery*, 18 Annals Health L. 75, 75 (2009).

254. "[I]ndividually identifiable health information . . . that is transmitted by electronic media, maintained in electronic media, or transmitted/maintained in any other form or medium." 45 C.F.R. § 160.103 (2011).

255. Under the HITECH Act a "breach" occurs when there has been "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information." 42 U.S.C.A. § 17921(1)(A) (2012). Accordingly, HITECH's definition for breach is broader than the concept of an e-security breach as it is used herein (which contemplates that a security breach occurs only when a cyberscribe gains unauthorized access to PHI).

256. A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transmission of information between two parties to carry out financial or administrative activities related to health care. 45 C.F.R. § 160.103 (2011). Under the HITECH Act, for the most recent three-year period, patients can demand an accounting of all individuals who have accessed their PHI. 42 U.S.C.A. § 17935(c)(1)(B) (2012).

257. 45 C.F.R. § 160.103 (2011).

258. 42 U.S.C.A. § 17932(d)(1) (2012). However, when state law has stricter reporting requirements, that state law is not preempted by the HITECH Act's reporting requirements. *See* 42 U.S.C.A. § 17951(a) (2012); 42 U.S.C. § 1320d-7(a)(2)(B) (2012).

259. 42 U.S.C.A. § 17932(e) (2012).

EMRs is to decrease the long latency period between the time of commission and the time of detection of MIT.[260] Under the HITECH Act, when the unsecured PHI of more than 500 patients (who are located in one state) has been compromised, the data custodian must notify "prominent media outlets" and the federal government.[261] Failure to report a major e-security breach exposes the EMR data custodian to significant administrative fines.[262] Since HITECH's public notification requirement went into effect, more than 385 PHI e-security breaches have been reported to the government.[263] Impressively, these EMR security breaches have involved the records of 19 million individuals (roughly 6% of the United States' population).[264] Of these EMR breaches, the largest occurred at Tricare in October 2011 when 4.9 million EMRs were compromised.[265] Consistent with other reports in the literature, the most common form of e-security breach (accounting for 39% of e-breaches) that has been reported to the federal government is the loss of a portable e-device (e.g., laptop computers and memory sticks) containing PHI.[266]

Under the HITECH Act, the scope of HIPAA's regulations has been extended to cEMD including: insulin pumps, defibrillators, and even email.[267] We were unable

260. *See supra* Part III.

261. 42 U.S.C.A. § 17932(e)(2) (2012). The term "unsecured PHI" should be read as PHI that is not secured through the use of a technology or methodology certified by the U.S. Department of Health and Human Services or an ANSI-accredited organization. 42 U.S.C.A. § 17932(h)(1)(A) (2012); *see HITECH Act Expands HIPAA Privacy and Security Rules*, *supra* note 248, at 3.

262. *See* Press Release, U.S. Department of Health and Human Services, HHS Settles HIPAA Case with BCBST for $1.5 Million (Mar. 13, 2012). Given that the average cost to notify patients of an e-security breach is $200 per patient, when millions of EMRs have been compromised, a healthcare provider has an incentive to want to keep knowledge of the breach in house. *See* Pamela Lewis Dolan, *Thinking of Buying Data Breach Insurance? Here Are Some Things to Consider*, AMEDNEWS.COM (Jan. 31, 2011), www.ama-assn.org/amednews/2011/01/31/bica0131.htm (last visited May 24, 2012).

263. Nicole Lewis, *Health Data Breaches Up 97% in 2011*, INFORMATIONWEEK (Feb. 13, 2012), http://www.informationweek.com/healthcare/security-privacy/health-data-breaches-up-97-in-2011/232600746 (last visited Oct. 2, 2012) (reporting 385 breaches between October 2009 and November 2011).

264. Robin Erb, *Data Breaches Put Patients at Risk for Identity Theft*, USA TODAY (Feb. 12, 2012, 10:03 PM), http://usatoday30.usatoday.com/news/health/story/health/story/2012-02-12/Data-breaches-put-patients-at-risk-for-identity-theft/53065576/1 (last visited Oct. 2, 2012); *see* USA QuickFacts, U.S. CENSUS BUREAU (2011), http://quickfacts.census.gov/qfd/states/00000.html (last visited Oct. 2, 2012) (reporting a population of 313,914,040 in 2012).

265. Joseph Conn, *Tricare Reports Data Breach Affecting 4.9 million Patients*, MODERNHEALTHCARE.COM (Sept. 29, 2011, 5:45 PM), http://www.modernhealthcare.com/article/20110929/NEWS/110929951 (last visited Oct. 2, 2012).

266. Lewis, *supra* note 263 (reporting that 39% of the 385 breaches between October 2009 and November 2011 occurred on a laptop or other portable device). Sadly, 81% of healthcare entities use such devices; and 49% do not make attempts to protect them. Pamela Lewis Dolan, *Smartphones Blamed for Increasing Risk of Health Data Breaches*, AMEDNEWS.COM (Dec. 19, 2011), http://www.ama-assn.org/amednews/2011/12/19/bil21219.htm (last visited Oct. 2, 2012).

267. *See* 42 U.S.C.A. § 17921(5) (2012) (defining "electronic health record" as an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff); *see also* Benjamin Wright, *Health-care Data Tracking | Electronic Health Record (EHR)*, ELECTRONIC DATA RECORDS LAW | HOW TO WIN E-DISCOVERY (Aug. 17, 2009), http://legal-beagle.typepad.com/wrights_legal_beagle/electronic-medical-records/ (last visited May 25, 2012) (reporting

to find documentation on the monetary impact of the HITECH Act's regulations on medical device manufacturers. However, the cost of HITECH compliance is unlikely to be as onerous for cEMD manufacturers as it is for healthcare providers. The reason is that a cEMD already has a computer; so the cost of HITECH compliance to device manufacturers is limited primarily to software modification. On the other hand, it is likely that an e-security breach that was facilitated by a non-compliance with HITECH would be especially damaging to a cEMD manufacturer's reputation.[268]

Indeed, an unintended, or perhaps intended,[269] outcome of HITECH's public reporting on healthcare providers and cEMD manufacturers may be the financial losses that flow from a major e-security breach. After such a breach, healthcare providers and cEMD manufacturers will be exposed to financial losses from administrative penalties,[270] business losses,[271] and the potential losses associated with defending a class action lawsuit.[272] Deloitte has reported that nationally, EMR e-

that the HITECH Act's accounting requirement applies to emails and e-records in medical devices and equipment).

268. Dolan, *supra* note 262 ("The biggest challenge is calculating the monetary loss from the damage to a practice's reputation.").

269. It is not hard to imagine that the framers of the HITECH Act anticipated that public reporting would trigger civil litigation. Just the same, the potential for such litigation gives the EMR and cEMD record custodians an incentive to ramp up their security systems.

270. Civil monetary penalties will be discussed in more detail, see *infra* this section. However, such penalties may be substantial. *See Office of Civil Rights: Resolution Agreement*, Blue Cross Blue Shield of Tennessee, www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/resolution_agreement_and_cap.pdf (last visited Apr. 23, 2012) (noting an insurer was fined $1.5 million after failing to report a major e-security breach in a timely manner).

271. *See* Ajay Gupta, *Hackers, Breaches and Other Threats to Electronic Records*, HealthData Mgmt. (Sept. 1, 2011), http://www.healthdatamanagement.com/issues/19_9/hackers-breaches-and-other-threats-to-electronic-records-43068-1.html (last visited Apr. 2, 2012); *see also* Chris Silva, *Blue Cross Tenn. Pays $1.5 million for HIPAA Violation*, Nashville Bus. J. (Mar. 13, 2012, 4:28 PM), http://www.bizjournals.com/nashville/news/2012/03/13/blue-cross-tenn-pays-15-million-for.html (last visited Oct. 2, 2012) (reporting that after a major e-security breach, an insurer spent $17 million to cover the cost of the investigation and attorneys' fees).

272. Neither HIPAA nor the HITECH Act creates a private right of action for healthcare e-security breaches. Still, class action lawsuits worth "millions and billions" were filed in 2011 for e-security breaches that occurred at Stanford University, Tricare, and Sutter Health System. Amy Catapano, *Data Breaches: A Growing and Alarming Trend and a Potential Safe Harbor*, HealthReformWatch (Feb. 7, 2012), http://www.healthreformwatch.com/2012/02/07/data-breaches-a-growing-and-alarming-trend-and-a-potential-safe-harbor/ (last visited Apr. 5, 2012); *see also* Howard Anderson, *SAIC Explains Insurance for Breach*, GovInfoSecurity (Apr. 9, 2012), www.govinfosecurity.com/latest-news/p-8 (last visited Apr. 23, 2012) (reporting that seven class action lawsuits were filed as a result of the e-security breach that occurred at Tricare). Unfortunately, such class action litigation over e-security breaches typically falters for inability to prove recoverable damages. *See First Line Of Defense In Privacy Class Actions – Damages*, Law360 (Sept. 22, 2011, 12:57 PM) ("[A]s demonstrated by recent court decisions in California and New York, the inability to allege damages continues to pose significant obstacles for would-be class plaintiffs."); *see also* Paul v. Providence Health System-Oregon, 273 P.3d 106 (Or. 2012) (dismissing a case where the plaintiffs sustained no actual damages after a provider lost physical control of unencrypted PHI).

security breaches have resulted in total losses of $6 billion dollars.[273] For healthcare providers' organizations' balance sheets, over the course of the two-years following an e-security breach, the cumulative business losses are approximately $2 million, which represents a loss of approximately $100,000 over the lifetime of the patient.[274] Others have calculated the business losses to healthcare providers for an e-security breach to be approximately $200 per compromised record.[275]

The business losses associated with the public reporting of a major e-security breach are thus on an order of magnitude that can destroy a healthcare provider's business. Given such risk exposure, it is not surprising that insurers have already entered the market. A detailed discussion of EMR e-security breach insurance is beyond the scope of this Article. However, it is worth noting that EMR e-security breach insurance policies are not all alike,[276] and the coverage of many of these policies is severely limited, to the point where the policies may not mitigate the business losses associated with a major e-security breach.[277]

Another aspect of the HITECH Act is its expansion of the scope of the Privacy and Security Rules with respect to so-called "business associates" and the creation of enhanced penalties for non-compliance with these rules by either CEs or BAs.[278]

Under the HITECH Act, HIPAA's definition of a BA remains unchanged,[279] but enforcement shifts from contractual mechanisms to statutory mechanisms. Under HIPAA, CEs were mandated to enter into BA agreements whereby the BAs were contractually bound to comply with the Privacy[280] and Security[281] Rules. When a CE detects that a BA is non-compliant with HIPAA's regulations, the CE is required to

273. *See* PONEMON INST., *Benchmark Study on Patient Privacy and Security* 1 (Nov. 9, 2010), http://www.dgshealthlaw.com/uploads/file/Ponemon_Benchmark_Study_on_Patient_Privacy_and_Data_Security%5B1%5D%281%29.pdf (last visited Oct. 2, 2012) (reporting that the total economic burden created by data breaches on U.S. hospitals as almost $12 billion over a period of two years).

274. *Id.* at 9 ("The extrapolated average lifetime value of one lost patient (customer) is $107,580.").

275. *See* PONEMON INST., *2010 Annual Study: U.S. Cost of a Data Breach*, 5 (Mar. 2011), http://msisac.cisecurity.org/resources/reports/documents/symantec_ponemon_data_breach_costs_report2010.pdf (last visited Oct. 2, 2012) ("Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from last year.").

276. *See* Drew Becker, *Implementing Electronic Medical Records (EMR): Mitigate Security Risks and Create Peace of Mind*, Clarity: White Paper 1, 3–4 (2011), http://www.claritygrp.com/media/13028/hipaa_hitech_whitepaper_6.7.11_final.pdf (last visited Apr. 23, 2012) (explaining different types of cyber liability insurance products and their features).

277. *See CyberGuard*, THE DOCTORS CO., http://www.thedoctors.com/Coverages/ID_010509?refId=CYBERGUARD (last visited Oct. 2, 2012) (CyberGuard insurance only covers up to $50,000); *see also* Dolan, *supra* note 262 (reporting that small physicians' groups can purchase $1 million of e-security breach insurance for $5,000 per year, but that the coverage purchased is limited to patient notification and does not cover fines).

278. *See generally HITECH Act Expands HIPAA Privacy and Security Rules*, *supra* note 248.

279. *See* 42 U.S.C.A. § 17921(2) (2012) (defining "business associate" as it has been defined at 45 C.F.R. § 160.103 thereby leaving the definition unchanged).

280. *See* 45 C.F.R. § 164.504(e) (2011) (privacy rules).

281. *See* 45 C.F.R. § 160.308 (2011) (administrative safeguards); § 160.310 (physical safeguards); § 160.312 (technical safeguards); § 160.316 (2011) (policies and procedures and documentation requirements).

bring a lawsuit against the BA.[282] This is a weak enforcement mechanism. As the CE and BA are business partners, compelling one of these parties to bring litigation against the other is likely to drive a wedge between the two parties. Such litigation would not be good for either party's balance sheet. Moreover, during such litigation the BA agreements were often found to be defective because they were inelegantly drafted.[283]

The HITECH Act obviates this awkward business situation. By statute, BAs are now directly accountable for their compliance with the Privacy and Security rules.[284] From a practical point of view, this means that BAs must now comply with all the Security Rules' administrative safeguards,[285] physical safeguards,[286] technical safeguards,[287] and policy and documentation requirements.[288] In the event that a CE or BA is noncompliant with these rules, the HITECH Act authorizes the Office of Civil Rights (OCR) to bring an enforcement action and seek civil and criminal penalties.[289]

Given the OCR's new statutory authorities over CEs and BAs, BA agreements may appear as a thing of the past. However, this would not be correct. BA agreements are still required under the HITECH Act, and those in existence are to be updated.[290] BA agreements are needed to define the "steps a CE or BA must take

282. *See* Lora Bentley, *HITECH Act Ramps up HIPAA Compliance Requirements*, ITBusinessEdge (Apr. 3, 2009), http://www.itbusinessedge.com/cm/community/features/articles/blog/hitech-act-ramps-up-hipaa-compliance-requirements/?cs=31575 (last visited Oct. 2, 2012) ("Before HITECH came into force . . . business associates that failed to properly protect patient information were liable to the covered entities via their service contracts, but they did not face governmental penalties.").

283. *See HITECH Act Expands HIPAA Privacy and Security Rules*, *supra* note 248, at 2 ("[M]ost of those business associate contracts did not impose specific security requirements and did not require business associates to have written policies and documentation of security safeguards in place.").

284. *See* 42 U.S.C.A. § 17934(a) (2012) (applying Privacy Rules to business associates); *id.* § 17931(a) (2012) (applying Security Rules to business associates).

285. *See* 45 C.F.R. § 160.308 (2011) (outlining administrative safeguards).

286. *See id.* § 164.310 (outlining physical safeguards).

287. *See id.* § 164.312 (outlining technical safeguards).

288. *See id.* § 160.316 (outlining policies and procedures and documentation requirements).

289. *See HITECH Act Expands HIPAA Privacy and Security Rules*, *supra* note 248, at 8. Under certain conditions the States' Attorneys General are authorized to bring HIPAA enforcement actions. 42 U.S.C.A. § 17939(e) (2012). While a detailed discussion of this HITECH Act enforcement mechanism is beyond the scope of this Article, this enforcement mechanism is being utilized. *See* Stacy Chubak Hinners, *HIPAA Compliance: Why the Stakes Are Higher Now Than Ever Before*, CorporateComplianceInsights.com (Mar. 2, 2012), http://www.corporatecomplianceinsights.com/hipaa-compliance-why-stakes-higher-now-than-ever-before/ (last visited Apr. 22, 2012) (reporting that the Attorneys General for Indiana, Connecticut, and Vermont have brought successful HITECH enforcement actions).

290. 42 U.S.C.A. § 17931(a) (2012) ("The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity."); *see also* Mark S. Hedberg, *Practical Considerations: Business Associate Agreements Under the Proposed HITECH Rules*, ABA Health eSource (Aug. 4, 2010), https://www.americanbar.org/newsletter/publications/aba_health_esource_home/Volume6_12_hedberg.html (last visited May 24, 2012) (reporting that the HITECH Act requires business associate agreements to incorporate the new privacy and security provisions).

if it learns of a pattern or practice that constitutes a material breach of the agreement."[291] As ambiguity exists in the HIPAA and HITECH regulations, it is also recommended that the BA agreement should more clearly define the "BA's obligations with respect to the minimum necessary standard, the prohibition on the sale of PHI, fundraising activities, marketing activities or research activities," as well as to define reporting responsibilities in the event of e-security breach.[292]

As an incentive for CEs and BAs to comply with the Privacy and Security Rules, the HITECH Act ramps up the civil monetary penalties (CMP) for e-security breaches and makes no distinction with regard to CE and BA liability.[293] Under HIPAA, the CMP for non-compliance with the Privacy Rule started at $100 per violation and topped off at $25,000 for all violations in a single year.[294] The HITECH Act, on the other hand, creates a four-tier scheme for assessing civil penalties.[295] At the most venial level, acts of HIPAA non-compliance are still subject to a fine of $100.[296] But more egregious acts of non-compliance are subjected to more severe CMP. At the top level, when the OCR finds that a CE or BA is non-compliant with HIPAA regulations and their non-compliance occurred because of "willful neglect," the OCR may fine that business entity up to $50,000 per violation, but no more than $1.5 million per calendar year.[297] (Parenthetically, under HITECH the failure to take remedial action within thirty days after an e-security breach is viewed as a willful violation of the regulations.[298])

Interestingly, HITECH's tiered CMP scheme creates a conflict of interest for the OCR. Under the Act, the civil penalties that are collected by the OCR are to be funneled back to the OCR to fund its enforcement budget.[299] So, the fact that OCR has become proactive with respect to its enforcement efforts is not surprising. In 2012, the OCR awarded a $9 million contract to KPMG to audit 150 CEs for

291. Hedberg, *supra* note 290.

292. *Id.*

293. *See* Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111–5, § 13409, 123 Stat. 115, 271 (2009); *see also* 42 U.S.C. 1320d-6(a) (2006) (attaching liability generally rather than specifically to a business associate or covered entity).

294. *See HITECH Act Expands HIPAA Privacy and Security Rules*, *supra* note 248, at 8 ("The Act also increases the amount of civil penalties from the present $100 per violation (up to $25,000 per identical violation). . .").

295. *See* HITECH Act, Pub. L. No. 111–5, §13410(d)(3), 123 Stat. 115, 273 (2009) (outlining four-tier scheme for assessing civil penalties).

296. *Id.* §13410(d)(3)(A).

297. *Id.* §13410(d)(3)(D).

298. *See id.* §13410(d)(3)(D) (amending 42 U.S.C. § 1320d-5(b)(3)(A) (2006)); *see* 42 U.S.C. § 1320d-5(b)(3)(A)(ii) (2006) ("[T]he failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.").

299. 42 U.S.C.A. § 17939(c)(1) (2012). *But see* 42 U.S.C.A. § 17939(c)(3) (2012) (noting under certain conditions, victims of Privacy Rule violations may receive a share of the penalties collected).

HIPAA compliance.[300] Under this program, CEs will be given little advance notice of the audit and CEs are expected to produce the requested documents within ten days.[301] Should a CE not cooperate with the audit, the CE could face significant penalties.[302] In the eyes of the OCR, non-cooperation with the audit process is willful neglect, which triggers the top tier for CMPs.[303] In the case of Cignet Health, its two years of non-cooperation with an OCR's investigation ultimately cost the organization $3 million in fines.[304]

Criminal liability under the HITECH Act also has been increased for BAs. Under HIPAA, individuals who gained unauthorized access to PHI with the intent to sell, transfer, or use the PHI for personal or commercial gain were subject to a fine of up to $250,000, ten years imprisonment, or both.[305] But because of the language used in HIPAA, only CEs were considered to have exposure for criminal liability.[306] But the real issue with HIPAA's criminal penalties was that they were mostly theoretical; prior to 2009, HIPAA violations were rarely subject to criminal prosecution.[307]

Under HITECH, the government has retained its authority to enforce HIPAA violations criminally,[308] and the maximum criminal penalty remains unchanged. However, the HITECH Act makes it clear that employees of CEs and "other individuals" can be held criminally liable for the unauthorized disclosure of PHI.[309] As used in § 13409, "other individuals" is an individual, regardless of CE employee status, who "without authorization, obtains or discloses such information

300. Hinners, *supra* note 289. OCR has also indicated that in subsequent years such random audits will be extended to BAs. *Id.*

301. *Id.*

302. *See, e.g.*, *HHS Office of Civil Rights Issues First Monetary Penalty for HIPAA Privacy Violation*, SIDLEY AUSTIN LLP (Feb. 25, 2011), www.sidley.com/sidleyupdates/Detail.aspx?news=4736.

303. *Id.*

304. *Id.*

305. 42 U.S.C. § 1320d-6(b)(3) (2006 & Supp. IV 2011).

306. Memorandum Opinion from Steven G. Bradbury, Principal Deputy Assistant Attorney General, U.S. Dep't of Justice, for the General Counsel Dep't of Health and Human Serv's and the Senior Counsel to the Deputy Att'y Gen. on Scope of Criminal Enforcement under 42 U.S.C. § 1320d-6 (June 1, 2005), *available at* www.justice.gov/olc/hipaa_final.htm.

307. Ian C. Smith DeWaal, *HIPAA Post-"HITECH": Health Information Privacy Enforcement*, DEP'T OF JUSTICE (Nov. 4, 2009), www.aoami.org/omed09_dewaal1104_hipaa.ppt; *see also* Doreen Z. McQuarrie, *HIPAA Criminal Prosecutions: Few and Far Between* (Feb. 2007), http://www.law.uh.edu/healthlaw/perspectives/2007/(DM)HIPAACrimCharges.pdf.

308. Technically a criminal action is not brought by the OCR, but rather by the Department of Justice upon a referral from the OCR. Nor does the OCR perform criminal investigations. *See* GLENNY, *supra* note 18, at 60 (noting the principal cybercrime investigating agencies are the FBI, Secret Service, and the United States Postal Inspection Service).

309. 42 U.S.C. § 1320d-6(a) (2006 & Supp. IV 2011) (stating a person "shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization").

maintained by a covered entity."[310] Given that HITECH § 13409 "makes HIPAA's criminal and civil penalties (42 U.S.C. § 1320d-5 and § 1320d-6) applicable to business associates,"[311] there is an argument that Congress did not intend hackers to be considered as other individuals. After all, Congress could have specifically stated that hackers were to be included as "other individuals" under the statute.

It will be interesting to see if courts do construe hackers to be "other individuals" within the meaning of the HITECH Act,[312] and whether the courts construe the HITECH Act as an anti-hacking statute.[313] Of the HIPAA criminal cases that have been publically reported in detail, all have involved CEs (healthcare providers or their employees) and in none of these cases was the unauthorized access to PHI obtained by a hacker hacking an EMR system.[314] Thus far only two HITECH criminal actions have been brought.[315] In one case, the government took action against a psychiatrist who had been disciplined by the State of Virginia for having

310. Teresa K. Culver et al., *Health Information & Technology for Economic and Clinical Health Act ("HITECH")*, MARTINDALE (Apr. 3, 2009), *available at* http://www.martindale.com/health-care-law/article_Miller-Martin-PLLC_662398.htm; *see also* Lisa J. Acevedo & Jennifer L. Rathburn, *Medical Privacy Enforcement and Penalties: HIPAA Gets Teeth*, *in* HEALTH CARE LAW ENFORCEMENT AND COMPLIANCE: LEADING LAWYERS ON UNDERSTANDING RECENT TRENDS IN HEALTH CARE ENFORCEMENT, UPDATING COMPLIANCE PROGRAMS, AND DEVELOPING CLIENT STRATEGIES (INSIDE THE MINDS) (2011), *available at* http://www.quarles.com/files/FileControl/c0df14d7-6e02-44e6-8b71-c6080df99f71/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Medical_Privacy_Enforcement.pdf.

311. *HITECH Act Expands HIPAA Privacy and Security Rules*, *supra* note 248, at 2.

312. *See infra* Part IV.B (discussing that under the EPCA, gaining unauthorized access to a computer that is privately owned, without more, does not trigger criminal liability).

313. We suspect that the courts will ultimately rule that using hacking techniques to gain access to PHI in an EMR system is a criminal act. But even if courts do not so hold, an individual who does use hacking techniques to gain access to PHI in an EMR system still faces HITECH criminal liability when they attempt to use the PHI. *See* 42 U.S.C. § 1320d-6(b) (2006 & Supp. IV 2011).

314. *See* United States v. Zhou, 678 F.3d 1110 (9th Cir. 2012) (Zhou was a physician and CE employee who exceeded his level of authorization when he obtained the prohibited PHI); United States v. Ferrer and Machado, 06-60761 CR (S.D. Fla. Sept. 11, 2006) (similar issue as *Ramirez*); United States v. Williams, 1:06-CR00129-UNA (D. Del. Nov. 16, 2006) (non-CE employee pled guilty to illegally obtaining PHI and grand theft for exceeding her authorized access to a hospital computer, but hacking was not an issue); Plea Agreement, United States v. Gibson, No. CR04-0374RSM, 2004 WL 2237585 (W.D. Wash. Aug. 19, 2004) (while the phlebotomist defendant engaged in criminal conduct, it is not clear that HIPAA was used to determine his liability); Ian C. Smith DeWaal, *Successfully Prosecuting Health Insurance Portability and Accountability Act Medical Privacy Violations Against Noncovered Entities*, U.S. Att'ys Bulletin, July 2007, at 10, 14–15 (discussing United States v. Ramirez, No. 7:05-CR-00708 (S.D. Tex. Aug. 30, 2006), where employee pled guilty to selling PHI, but computer hacking was not an issue); *see also Memorandum Opinion for the General Counsel Dep't of Health and Human Servs. and the Senior Counsel to the Deputy Att'y Gen. on Scope of Criminal Enforcement under 42 U.S.C. § 1320d-6*, U.S. DEP'T OF JUSTICE (June 1, 2005), www.justice.gov/olc/hipaa_final.htm (the Office of Legal Counsel opined that the scope of HIPAA's criminal enforcement extends only to CEs; but non-CEs may accrue criminal liability according to the principles of conspiracy and aiding and abetting); *cf.* United States v. Abdallah, No. H-07-155, 2007 WL 4570189 (S.D. Tex. July 1, 2009) (holding that because an ambulance driver is not a CE, there was no HIPAA criminal liability).

315. *DOJ Steps Up Enforcement With Indictment of 'Loose Lips' Doctor, Hospital Visitor*, HEALTH BUS. DAILY (July 15, 2011), http://aishealth.com/archive/hipaa0711-01; *Atlanta Man Sentenced on Computer Hacking Charge*, U.S. ATTY'S OFFICE (Jan. 10, 2012), http://www.justice.gov/usao/gan/press/2012/01-10-12.html.

"spoke[n] out of turn to an 'agent' of an employer of a former patient."[316] In the second case, the defendant was a healthcare provider who was incidentally found to be in the unauthorized possession of PHI when a search warrant was executed for other reasons.[317] In both of these cases,[318] the defendant was a CE and neither defendant was accused of engaging in hacker activities. So, the answer as to whether a hacker is an "other individual" under the HITECH Act will have to wait until a more appropriate case arises.

Perhaps the most interesting aspect of HIPAA criminal enforcement actions may be the low threshold for the demonstration of criminal intent. In the *United States v. Zhou*, defendant Zhou gained unauthorized access to PHI after he was terminated by his hospital employer.[319] For this, Zhou was charged with a misdemeanor violation of HIPAA.[320] Zhou sought to have the criminal case dismissed by arguing that HIPAA criminal liability arises when a "person who knowingly *and* in violation of this part" of the HIPAA gained unauthorized access to PHI.[321] Zhou did not argue that he had knowingly gained unauthorized access, but argued that a "defendant is guilty only if he knew that obtaining the personal healthcare information was illegal."[322] The Ninth Circuit responded by observing that:

> *The word "and" unambiguously indicates that there are two elements of a Section 1320d-6(a)(2) violation: 1) knowingly obtaining individually identifiable health information relating to an individual; and 2) obtaining that information in violation of Title 42 United States Code Chapter 7, Subchapter XI, Part C. Thus, the term "knowingly" applies only to the act of obtaining the health information.*[323]

Accordingly, under HIPAA criminal liability is applicable if the defendant knew that he was accessing PHI without authorization.[324]

Stepping back, the HITECH Act's stimulus money was to encourage providers to adopt EMR systems and its amendment of HIPAA's civil and criminal enforcement mechanisms are clearly intended to motivate CEs and BAs to provide the best e-security they could afford. Whether healthcare providers can finance the conversion

316. *DOJ Steps Up*, *supra* note 315.

317. *Atlanta Man Sentenced*, *supra* note 315.

318. *See supra* note 315.

319. United States v. Zhou, 678 F.3d 1110, 1112 (9th Cir. 2012).

320. *Id.* at 1112 (the hospital's culpability for failing to terminate Zhou's computer access to PHI after he was terminated was not discussed).

321. *Id.* (citing 42 U.S.C.A. § 1320d-6(a)) (emphasis added).

322. *Id.* at 1113.

323. *Id.*

324. *Id.* at 1115; *see also* Horne v. State, 445 N.E.2d 976, 979 (Ind. 1983) (a person "knowingly" commits an act if the act is a product of a conscious design, intent or plan), *abrogated by* Jackson v. State, 728 N.E.2d 147 (Ind. 2000).

to a secure EMR system is an open question.[325] Financial considerations will likely drive many healthcare providers to select the less secure cloud based EMR systems; thereby offering hackers the opportunity to exploit Internet holes and perpetuate MIT.[326] And therein is the problem: nothing in the HITECH Act is specifically aimed at hackers.[327]

The question then becomes does HITECH's civil and criminal penalties combined create a deterrence for hackers? Perhaps. The economics of MIT mean that it is unlikely that HITECH's CMP will deter a hacker.[328] As we have seen, MIT is wildly profitable.[329] If a hacker anticipates earning $20-30 million from MIT, the hacker is likely to view a fine of $3 million dollars as the price of doing business. Still, HITECH's prescribed jail time for the unauthorized access of PHI might make a hacker think twice. Ten years in jail for perpetrating an e-security breach of an EMR system is a long time.[330]

Still, while a ten-year jail term may cause a hacker to think twice, the deterrent value of jail time depends on the certainty it will be applied.[331] Assume here that a hacker is an "other individual" within the meaning of the HITECH Act § 13409.[332] Under this statute:

> *[A] person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation[ )] . . . and the individual obtained or disclosed such information without authorization.*[333]

325. Marla Durben Hirsh, *Can Providers Afford the Changes Government Is Implementing?* FIERCE EMR (Mar. 29, 2012), http://www.fierceemr.com/story/can-providers-afford-changes-government-implementing/2012-03-29.

326. *See supra* Part II.A.

327. *See generally* 45 C.F.R § 160.103 (2011) (noting although HIPAA protects PHI, the scope of the Act's Privacy Rule is limited to CEs and BAs). *See also* James G. Hodge, Assoc. Professor, Johns Hopkins Sch. of Pub. Health, Exec. Dir., Center for Law and the Public's Health at Georgetown and Johns Hopkins University, The HIPAA Privacy Rule: Scope, Structure, and Implementation (Nov. 4, 2009), *available at* www.slidefinder.net/t/the_hipaa_privacy_rule_scope/6645112.

328. *See supra* Table II and accompanying text.

329. *See supra* Table II and accompanying text.

330. *See* 42 U.S.C. § 1320d-6(a) (2006 & Supp. IV 2011) ("[A] person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization.").

331. Raymond Paternoster, *How Much Do We Really Know About Criminal Deterrence?*, 100 J. CRIM. L. & CRIMINOLOGY 765, 769–71, 821 (2010) (discussing different theories on criminal deterrence, their strengths and weaknesses, and the limits of deterrence theory in general).

332. HITECH Act § 13409, 42 U.S.C. § 1320d-6(a) (2006 & Supp. IV 2011).

333. *Id.* (emphasis added).

Therefore, for hackers to be punished under § 13409, they must both hack into an EMR and obtain or disclose the information.

Hackers are likely to understand the first element of § 13409. But what does it mean to obtain and disclose e-information? According to Black's Law Dictionary, "to obtain" is "to get hold of by effort, to get possession of, to procure, to acquire in any way;" and "to disclose" is "to bring into view by uncovering, to expose, to make known, to lay bare, to reveal to knowledge, to free from secrecy or ignorance, or make known."[334] These are words grounded in the physical world; not cyberspace where holding a stream of electronic zeros and ones is a metaphysical concept. Interestingly, the cases reviewed for this Article failed to identify any hacker criminal cases where "to obtain" or "to disclose" were distinguished or used in a way different from their physical world meaning.[335]

This suggests that certainty of a criminal conviction under the HITECH Act should be approximately the same as the certainty of a criminal conviction under other cybercrime statutes. Accordingly, to better understand the potential of jail time to deter hackers from gaining unauthorized access to PHI, a look at the ability of the Electronic Communications Privacy Act (ECPA) is appropriate.[336] In addition, a review of the ECPA is appropriate here because, unless unauthorized access to PHI is obtained from the federal government's EMR system, the ECPA is the only other federal statute for which a hacker could potentially be criminally tried.[337]

B. ECPA

The ECPA is composed principally of two parts: the Federal Wiretap Act (FWTA)[338] and Stored Communication Act (SCA).[339] Historically, the FWTA is older. A rudimentary Wiretap Act[340] was enacted in 1968 in response to the Supreme Court's opinion in *Katz v. United States*.[341] Technological advances soon required this first iteration of the Wiretap Act to be clarified.[342] Accordingly, in 1986, the ECPA was passed, amending the 1968 Wiretap Act to produce the FWTA and creating the

334. Black's Law Dictionary 320, 743 (6th ed. 1991).

335. *See infra* Part IV.B (discussing that under the EPCA, gaining unauthorized access to a computer that is privately owned, without more, does not trigger criminal liability).

336. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (1986).

337. *See supra* Part III.

338. *See supra* note 334.

339. 18 U.S.C. §§ 2701–2712 (2006 & Supp. IV 2011).

340. Omnibus Crime Control and Safe Street Act of 1968, Pub. L. 90–351, 32 Stat. 197 (1968); *see also* Andrew R. Schulman, *What Civil Practitioners Should Know about the Federal Wiretap and Stored Communications Acts*, Getman, Tamposi, Schulthess and Steere, P.A., http://www.andrewschulman.com/Briefs/cle%20wiretap.PDF (discussing the origins of the Federal Wiretap Act).

341. Katz v. United States, 389 U.S. 347 (1967) (extending Fourth Amendment protection to non-consensual interceptions of private telephone conversations by the government).

342. Fraser v. Nationwide, 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001).

SCA.[343] Under the ECPA, the "amended Wiretap Act prohibits the unauthorized 'interception' of oral, wire, and electronic communications, while the SCA prohibits "unauthorized 'access' to wire and electronic communications in temporary and back up storage."[344] Although both Acts have civil and criminal enforcement mechanisms[345] and are often bundled together in ECPA, each Act is distinct and enforceable independent of the other.[346]

1. FWTA

A priori, the FWTA may appear to have limited application in the healthcare sector because its focus is on the privacy of communications and the punishment of e-communication interception.[347] But, this would not be correct because of telemedicine. Virtually every medical specialty has an analogue specialty in telemedicine.[348] As the telemedicine market has matured, telecommunication vendors have similarly matured their attitude towards e-security. Prior to the enactment of the HITECH Act, one of us (TRM) interviewed a representative of Tandberg, a leader in telepresence technology (room-sized high-definition video conferencing).[349] This representative disclosed that the company, at the time, did not encrypt its Video-over IP transmissions. In contrast, at the 2012 American Association of Thoracic Surgeons' meeting, a representative of the In Touch Health Corporation found the concept of non-encryption of telemedicine imagery to be unimaginable in light of the HITECH Act.[350]

Conceptually, telemedicine streamed over the Internet or sent via Video-over-IP could be intercepted thereby raising the potential of a wiretap. But for two practical reasons, the FWTA is unlikely to play a significant role in regulating the transmission of PHI or deterring hacker activity.[351] First, intercepting PHI one record at a time is inefficient. Any hacker with the time or capital to invest in a telemedicine interception operation would be better served if that time and capital

343. *See supra* note 341.

344. Schulman, *supra* note 340.

345. 18 U.S.C. § 2511 (2006 & Supp. IV 2011) (stating the civil and criminal penalties under the ECPA); *id.* § 2701(b) (stating the criminal penalties under the SCA); *id.* § 2707 (stating the civil remedies under the SCA).

346. United States v. Councilman, 418 F.3d 67, 82 (1st Cir. 2005) (en banc).

347. 18 U.S.C.A. § 2510(15) (2006).

348. Thomas R. McLean, *The Offshoring of American Medicine: Scope, Economic Issues and Legal Liabilities*, 14 ANNALS HEALTH L. 205, 228–46 (2005) (describing several different areas of the Healthcare Industry that have already begun using telemedicine to a significant degree and the potential for its use to spread).

349. Tandberg is now owned by Cisco Systems, Inc. *See* CISCO, http://www.cisco.com/en/US/solutions/ns669/ttg.html (last visited Dec. 4, 2012).

350. Olivier Salat, Manager, International Markets, In Touch Health, in Santa Barbara, Cal. (In Touch Health streams its video through IP rather than over IP. For the discussion here these differences are not material, still the comparison of telemedicine products made here is not exactly apples to apples).

351. The same skill set that facilitates computer hacking also facilitates wiretapping. *See* GHOST, *supra* note 22.

were directed at breaching the e-security of EMR system to gain access to a treasure trove of PHI.

Second, transmission of e-data no longer occurs over a dedicated hardwire circuit that is susceptible to wiretapping. In the modern telecommunication world e-information is transmitted in packets.[352] Packet switching according to the TCP/IP and other technologic innovations (including encryption and peer-to-peer networks) mean that electronic communications no longer travel in a linear fashion over a single wire.[353] Rather e-communications are broken up into packets of information by the first Internet service provider's (ISP) router that receives the document.[354] Next, this router sends the packets to different routers according to an algorithm that is designed to maximize transmission speed but minimize Internet congestion.[355] Not all packets go to the same intermediate routers.[356] When the packets arrive at the destination router the e-message is then reassembled before it is sent on to the end user.[357]

Packet switching's non-linear transmission of e-messages makes hacker interception of e-messages very difficult.[358] In the modern packet switching world, when e-messages are intercepted, the interception usually does not occur within the telephone system's network, but rather when the e-message is transmitted over airways (i.e., when the e-message passes between a sender/receiver and a router via cellular telephony).[359] Cellular telephony interception is relatively easy and can be achieved with a device that mimics a transmission tower.[360] Conversely, the physical difficulties of intercepting a packet-wired e-message have caused one commentator

352. Paul Rosenzweig, *The Evolution of Wiretapping*, Red Branch (Aug. 3, 2011), http://www.redbranchconsulting.com/index.php?option=com_content&view=article&id=13:the-evolution-of-wiretapping&catid=3:publications-and-presentaions&Itemid=7.

353. *Id.*; *see also Third Generation Partnership Project Z: Packet Switched Video Telephony Services (PSVT/MCS)* (June 2008), http://www.3gpp2.org/public_html/specs/C.S0055-A_v1.0_080623.pdf.

354. ISPs operate their own network of routers. Steven M. Bellovin, *Wiretapping the Net*, The Bridge, Summer 2000, at 21, 22 (ISPs operate their own network of routers, but communicate with each other via private links and through public exchange points).

355. *Id.*

356. *Id.*

357. *Id.* at 24.

358. Paul Rosenzweig, *The Evolution of Wiretapping*, 12 Engage: J. Federalist Soc'y Prac. Groups 83 (2011). On the other hand, if a telephone company or ISP cooperates "wiretapping" is still possible. Andy Greenberg, *These Are the Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps*, Forbes (Apr. 3, 2012, 3:01 PM), http://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps/. This is because packet switching produces e-copies of e-message that are stored on routers. *See infra* Part IV.A.1. However, such stored e-copies are better addressed under the SCA than the FWTA. *See infra* Part IV.A.1.

359. Kurt Marko, *The Potential for Cell Phone Interception*, 32 Processor 34 (2010), *available at* http://www.processor.com/editorial/article.asp?article=articles%2Fp3223%2F36p23%2F36p23.asp.

360. Dean Takahashi, *Hacker Shows how He Can Intercept Cell Phone Calls with $1,500 Device*, VentureBeat (July 31, 2010, 1:31 PM), http://venturebeat.com/2010/07/31/hacker-shows-how-he-can-intercept-cell-phone-calls-for-1500/ (noting an investment of $1,500 in equipment can provide access to approximately 80% of the global mobile communication system); *see also* Greenberg, *supra* note 358.

to observe that "the laws and policies for authorized wiretapping have, effectively, become obsolete."[361]

In short, the reality of wiretapping in the 21st century and the inefficiency of stealing PHI one record at a time make it unlikely that hackers will make use of wiretaps. So the FWTA will not be discussed further here.[362]

On the other hand, because packet switching results in e-messages[363] being stored on routers, the SCA comes into play.[364] Not only does the last router involved in an e-transmission make a copy of the message, so does the first router. Before sending the quantized message, the first router stores a copy of the e-message for reference in case a transmission error occurs.[365] Similarly, when the quantized message is received at the destination router, a copy of the e-message is stored in case a transmission error occurs when the message is sent to the receiver.[366] These e-copies, which are stored on an ISP's routers, can be accessed by sophisticated hackers.[367]

2. SCA

The SCA is a federal statute that provides relief for victims of a hacker attack. Under the Act, unauthorized access to stored electronic communications is prohibited.[368] A number of caveats, however, modify the scope of the SCA. First, authorization can be provided by a number of individuals besides the sender or receiver of an e-message.[369] Individuals who can grant authorization to access e-messages stored in an ISP's system include: the electronic communication provider, the record user, and the government (for lawful purposes).[370] Consent to access stored e-messages

361. Rosenzweig, *supra* note 358, at 84.

362. This is all the more reasonable because the incentives created by the FWTA are the same as those created by the SCA.

363. As an e-message and an e-copy of an e-message are physically indistinguishable, they will not be distinguished here.

364. The discussion of how the SCA regulates the government's access to e-messages stored on ISP routers is to be contrasted to how Russia regulates such e-storage. All e-messages stored on Russian ISPs routers are forwarded to the FSB (the successor agency to the KGB). GLENNY, *supra* note 18, at 169–71. The FSB in turn reads everything and looks for encryption of e-messages, since encryption is a criminal act in Russia. *Id.* This fact explains why a substantial volume of identity theft is perpetrated by cyberscribes in Russia (and Eastern Europe). The FSB takes the position that only spies against the Russian State need encryption, but it could care less if a Russian cyberscribe commits an act that undermines the United States' economic welfare. *Id.*

365. Rosenzweig, *supra* note 358, at 85.

366. *Id.*

367. STEVEN LEVY, IN THE PLEX: HOW GOOGLE THINKS, WORKS, AND SHAPES OUR LIVES 308–09 (2011).

368. 18 U.S.C. § 2701(a) (2006).

369. *Id.* § 2701(c).

370. *Id.* Law enforcement agencies at local, state, and federal level make use of this provision to conduct wireless e-surveillance operation. *Cf.* Andy Greenberg, *These Are the Prices AT&T, Verizon and Sprint Charge for Cellphone Wiretaps*, FORBES (Apr. 3, 2012, 3:01 PM), http://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps/. The procedures used and merits of such e-surveillance operations are beyond the scope of this Article.

can even be authorized inadvertently by third-parties.[371] Second, under the SCA, the fact that a record custodian facilitated unauthorized record access does not bar recovery under the Act.[372] So for example, a record custodian-owner was allowed to recover damages against a former employee for unauthorized access to his email account even though the record custodian-owner took months to disable the account.[373] Finally, the SCA does not punish the subsequent use or disclosure of the unauthorized information obtained.[374]

To have standing to bring an SCA action, the aggrieved party must show that the unauthorized access to the electronic documents was obtained with a "knowing or intentional state of mind."[375] Neither the statute nor case law precisely defines the meaning of "knowing."[376] Many courts, however, have taken the view that, within the context of the SCA, knowing is conduct that "includes willful blindness, but not recklessness or negligence;"[377] and "a reckless defendant is one who merely knows of a substantial and unjustified risk of such wrongdoing."[378] A party with standing may file a lawsuit to seek recovery of actual damages or at a minimum $1000 of damages.[379] Finally, under certain conditions, the SCA allows an aggrieved party to recover punitive damages and attorneys' fees.[380]

371. *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 500, 510–11 (S.D.N.Y. 2001). Without this case, behavioral advertising would have never developed to its current level and Professor Andrews would not have a best-selling book. *See supra* note 65. Today DoubleClick is owned by Google. LEVY, *supra* note 367, at 330–36.

372. 18 U.S.C. § 2702(a) (prohibiting providers of electronic communication services from knowingly divulging the contents of stored e-documents).

373. Cardinal Health v. Adams, Case No 3:07:00691 (M.D. Tenn. 2008). *See generally* 18 U.S.C. § 2702(a)(1)–(2).

374. Sherman & Co. v. Salton Maximum Housewares, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000); *see also In re* Am. Airlines Privacy Litig., 370 F. Supp. 2d 552, 558–59 (N.D. Tex. 2005).

375. 18 U.S.C. § 2707(a) (2006).

376. Worix v. MedAssets, Inc., No. 11 C 8088, 2012 WL 787210, at *2–3 (N.D. Ill. Mar. 8, 2012) (citing Freedman v. Am. Online, 329 F. Supp. 2d 745, 749 (E.D. Va. 2004)). *But see id.* at *3 (citing H.R. REP. NO. 647, 99th Cong., 2d Sess. at 64 (1986)) (providing insight to the meaning of knowing in the SCA through its legislative history: "The term knowingly means that the defendant was aware of the nature of the conduct, aware of or possessing a firm belief in the existence of the requisite circumstances and an awareness of or a firm belief about the substantial certainty of the result . . . . The concept of 'knowingly' does not include, however, 'reckless' or 'negligent' conduct").

377. *See, e.g.*, *Worix*, 2012 WL787210, at *3.

378. *Id.* at *4. The *Worix* court distinguished reckless conduct from willful blindness, which is conduct that "takes deliberate actions to avoid confirming a high probability of wrongdoing and who almost can be said to have actually known the critical facts." *Id.* (citing Global-Tech Appliances v. SEB S.A., 131 S. Ct. 2060, 2070–71 (2011)).

379. 18 U.S.C. § 2707(c) (2006); *see also* Cedar Hill Ass'n. v. Paget, 2005 WL 3430562, at *3 (N.D. Ill. Dec. 9, 2005). The ability to recover damages for use or dissemination of hacked electronic data arises under other theories of law (e.g., intellectual property or trade secret law), which are beyond the scope of this Article.

380. 18 U.S.C. § 2707(c) (2006).

Like "knowing," a "violation" of the SCA is not defined.[381] Some courts have taken the view that an SCA violation occurs each time a hacker gains unauthorized access to an e-document system,[382] while other courts have the view that an SCA violation occurs each time a specific e-document is accessed.[383] For civil litigation this distinction is of little importance, because an aggrieved party must prove their actual damages.[384] However, under the criminal enforcement statute, a violation of the SCA carries a penalty of up to five years in prison per violation.[385] So for a hacker who is caught and then criminally charged under the SCA, it makes a significant difference whether a violation occurs every time the record room is entered or whether a violation occurs every time a unique record is viewed.

Yet, we could not find any cases where a hacker was criminally charged under the SCA for gaining unauthorized access to either a record room or a record.[386] This is not an oversight on our part. Rather, it reflects how the SCA views temporary and permanent e-storage.

Under the SCA electronic storage occurs when an e-communication is temporarily stored or archived on an ISP's router.[387] ISPs, therefore, provide two distinct services: electronic communication service (ECS) and remote computing service (RCS). ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[388] An ISP provides ECS when it actually transmits an e-communication; e-copies of e-communication generated during the transmissions are considered to be part of ECS.[389] On the other hand, an ISP provides RCS when it provides "the public [with a] computer storage or processing services by means of an electronic communications system."[390] ISPs often archive e-communications that pass through their routers for "backup protection."[391] E-communications that have been archived by an ISP are not

381. Jeffery G. Weil & Robert A. Chu, *Email Theft: What Are Your Damages*, METRO. CORP. COUNSEL, Dec. 2009, at 36, *available at* http://www.metrocorpcounsel.com/articles/12001/email-theft-what-are-your-damages.

382. *Cedar Hill Ass'n.*, 2005 WL 3430562 at *3; Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 2009); *see also* Weil & Chu, *supra* note 381.

383. Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199 (4th Cir. 2009); *see also In re* Hawaiian Airlines, 355 B.R. 225 (D. Haw. 2006) (multiple logins are treated as if only one login had occurred); Weil & Chu, *supra* note 381.

384. 18 U.S.C. § 2707(c) (2006).

385. *Id.* § 2701(b).

386. Indeed, at issue in SCA criminal litigation is whether the government lawfully obtained access to electronic communications stored on an ISP's servers. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

387. 18 U.S.C. § 2510(17) (2006).

388. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004) (citation omitted).

389. *Id.* at 1216.

390. *Id.* at 1214–16.

391. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 984 (C.D. Cal. May 26, 2010).

necessarily in permanent storage.[392] But, an ISP provides RCS when it allows its clients to access documents that are stored long term on its servers.[393]

The distinction between the temporary ECS storage and the permanent storage of RCS matters. Under the SCA:

> *It is not enough for the electronic communication data to have been accessed in any format on any computer, in order to run afoul of the SCA, the data must have been accessed or obtained while it was within the electronic storage of the electronic communications service itself.*[394]

Accordingly, once an e-communication has been archived and transferred into a permanent storage media, it is no longer covered under the scope of the SCA.[395]

Now consider an EMR. When a healthcare provider enters data into an EMR system (or any computer), the e-document exists in Random Access Memory (RAM).[396] One distinguishing characteristic of RAM is that it is volatile memory, meaning it loses all the content it is currently storing once the power is cut.[397] (This is the reason word processing software prompts the user to save their work when the computer user attempts to close the program.) This volatile RAM storage corresponds to the temporary ECS. On the other hand, once the provider saves the data into a permanent storage medium (i.e., a hard drives or flash drive) the PHI continues to exist in the absence of electrical power.[398] Permanent EMR storage corresponds with archived RCS storage.

Accordingly, when hackers use their advanced knowledge to gain unauthorized access to an EMR system (e.g., when the Virginia State medical record system was hacked)[399] access is gained to PHI in permanent RCS-type storage. This means that when hackers hack into EMR systems their conduct falls outside the scope of the SCA.[400] More generally, the reason for paucity of SCA criminal prosecutions for hacking an EMR (or any computer) system is because the hackers only gain access

392. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 902–03 (9th Cir. 2008), *rev'd* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010).

393. *Crispin*, 717 F. Supp. 2d at 978.

394. Thompson v. Ross, 2:10-CV-479, 2010 WL 3896533, at *3 (W.D. Pa. Sept. 30, 2010).

395. *Id.* at *4.

396. Rene B. DeLaup, *Inside the Personal Computer*, 43 La. B.J. 87, 88 (1995).

397. *Id.*

398. *Id.*

399. Brian Krebs & Anita Kumar, *Hackers Want Millions For Data on Prescriptions; Theft of Va. Patient Records Claimed*, Wash. Post, May 8, 2009, at B01.

400. This is because only temporary and backup storage are protected by the SCA. *See* Thompson v. Ross, 2:10-CV-479, 2010 WL 3896533, at *4 (W.D. Pa. Sept. 30, 2010); *see also* United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010), as amended (Nov. 29, 2010); Baily v. Baily, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008); Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2003).

to permanent e-records, and not the temporary ECS e-records that are covered by the SCA.

The truth is that the SCA is not an anti-hacking statute. Rather, the "SCA regulates retrospective surveillance, specifically content that is in storage with an ISP."[401] As such:

> *[T]he SCA imposes strict rules on when the government may* compel *service providers to disclose information they are storing on their subscribers. The SCA creates similar limits on* voluntary *disclosures to the government by ISPs in section 2702, heightening the protection provided by the private search doctrine of the Fourth Amendment. According to the United States Department of Justice, the SCA serves "to protect and regulate the privacy interests of network users with respect to government . . . and the world at large."*[402]

President Obama's administration is promoting anti-cybercrime legislation to combat increasing hacker activity in organized crime.[403] The current administration has recently opined that "computers are now 'a key tool of organized crime,' with many hackers 'tied to traditional Asian and Eastern European organized crime organizations.'"[404] This statement was made after the cybercrime organization LulzSec broke into websites of the FBI, the CIA, and the Senate and the Obama administration was seeking to strengthen the penalties under the Computer Fraud and Abuse Act.[405] Still, with an epidemic in PIT and likely coming epidemic of MIT,[406] the Obama administration's comments are equally true to private computers and EMRs.

Erecting harsh penalties to deter scribes from using their specialized knowledge to further a criminal enterprise dates back to the earliest times of Ancient Egypt.[407] Unfortunately for healthcare providers, strengthening the criminal penalties under HITECH Act or the SCA, without more, is unlikely to deter hackers from hacking into private-sector EMR systems. Until an appropriate case is handed down, it is an open question whether the HITECH Act or the SCA covers hackers' attacks on

401. Casey Perry, Recent Development, U.S. v. Warshak*: Will Fourth Amendment Protection be Delivered to Your Inbox?*, 12 N.C. J.L. & TECH. 345, 350 (2011).

402. *Id.* at 350–51 (citations omitted).

403. *See generally* Mathew J. Schwartz, *Treat Hackers As Organized Criminals, Says Government*, INFORMATIONWEEK (Sept. 9, 2011), http://www.informationweek.com/security/government/treat-hackers-as-organized-criminals-say/231601078; Kenendra Srivastava, *Obama Says Hacks Are Organized Crime, Wants Stiffer Penalties*, MOBILEDIA (Sept. 9, 2011, 11:35 AM), http://www.mobiledia.com/news/107373.html.

404. Kenendra Srivastava, *Obama Says Hacks Are Organized Crime, Wants Stiffer Penalties*, MOBILEDIA (Sept. 9, 2011, 11:35 AM), http://www.mobiledia.com/news/107373.html.

405. *Id.*

406. *See supra* Part III.

407. *See supra* note 15 and accompanying text.

EMRs.[408] Nor, as the following hypothetical illustrates, is it likely that using the HITECH Act in tandem with the SCA's civil enforcement mechanism will deter hacker activity.

Suppose a healthcare provider's EMR system is attacked by a hacker and one million individual EMRs are compromised. In this case, however, none of the patients whose PHI was compromised sustained any damages as the hacker's momentary lack of focus resulted in him being arrested before the PHI could be auctioned off on the Internet. As direct consequence of having to publicly report the attack on its EMR system, the hospital ultimately sustains actual damages of $10 million in the form of a loss of business due to its damaged reputation. The healthcare provider then brings an SCA civil action against the hacker to recover the $10 million in actual losses.[409] Assuming that healthcare provider prevails in this litigation,[410] the potential judgment for $10 million is unlikely to deter the hacker who can earn $50 million by selling medical identities.[411] As the only unauthorized access to PHI occurred in a permanent storage media, the SCA's criminal sanctions do not come into play.[412]

C. Deterrence

Nor is it likely that the HITECH Act's criminal penalties will deter the hacker in this hypothetical. Even if a hacker is an "other individual" within the meaning of § 13409,[413] legal ambiguities (duration of sentences according to a per record room or a per record entered standard) and practical considerations of prosecuting cybercrime (the physical evidence that creates a nexus between the defendant and the crime) are likely to make convictions under the HITECH Act far from certain.[414]

Recall that controversy exists under the SCA with respect to whether criminal liability turns on the number of times a record room is entered or on the number of records entered.[415] Such controversy may develop under the HITECH Act. Under

408. We strongly believe, however, that courts will ultimately find that cyberscribes are "other individual[s]" within the meaning of the HITECH Act § 13409, unless our healthcare system evolves into one that has universal access.

409. Interestingly, SCA civil litigation does not often concern whether unauthorized access was obtained to e-documents in temporary or permanent storage. *See, e.g.*, Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199 (4th Cir. 2009) (unauthorized access e-documents appear to have been in permanent storage); Konop v. Hawaiian Airlines, 302 F. 3d 868 (9th Cir. 2002) (same).

410. In this hypothetical, we also assume that because the cyberscribe is easily caught, he is locally based, and a court will have jurisdiction to hear the case. This is not necessarily true if our cyberscribe is sophisticated and working outside of the U.S.

411. *See supra* Table II.

412. *See supra* note 400.

413. Health Information Technology for Economic and Clinical Health Act (HITECH Act) § 13409, 42 U.S.C. § 1320d-6 (2006 & Supp. IV 2011).

414. *See supra* notes 305–18 and accompanying text; *supra* notes 381–383 and accompanying text; *infra* notes 431–33 and accompanying text.

415. *See supra* notes 380–84 and accompanying text.

the HITECH Act, a person who knowingly violates the Act by obtaining unauthorized access to PHI "relating to an individual" and acts with "intent to sell, transfer, or use individually identifiable health information for commercial advantage" may be "imprisoned not more than ten years."[416] The use of the term "an individual" suggests that when a court sentences a hacker for the unauthorized access of an EMR, the court should interpret HITECH's punishment to be applied on a per record compromised basis. Yet, such a plain meaning interpretation is unlikely to stand. Consider the hacker(s) who stole 8 million medical records from the Commonwealth of Virginia.[417] Now consider the outcome of a trial where the hacker was convicted of gaining unauthorized access to all 8 million records and the court used a per record entered standard for sentencing. Under these conditions the judge should hand down a sentence of 80 million years in prison. Such a judge would look foolish and the sentence would invite ridicule of the legal system.

In addition, the HITECH Act also uses the language that unauthorized access to PHI is to be punished by "not more than 10 years" of imprisonment.[418] In contemplating how to interpret this rule, courts might look to the structure of the HITECH Act's CMP. Regardless of the tier used to assess a civil penalty, it is clear that the penalty to be applied is capped.[419] For example, although the most severe penalty carries a fine of up to $50,000 per violation, this penalty is capped at $1.5 million per year.[420] Having made this observation, a court may conclude that it is reasonable to apply a similar interpretation of the statute to HITECH's criminal penalties. So even if a court were to adopt a per record entered standard for criminal convictions, a hacker might only receive a ten-year sentence for compromising the PHI of millions of patients.

Still, shouldn't a ten-year prison sentence deter hackers from committing MIT? *A priori*, imprisonment is a weak deterrence. Of those individuals who are released from prison, 51.8% were back in jail within three years of release.[421] This statistic suggests that prison is only an effective deterrence to one-third of the individuals

416. Health Information Technology for Economic and Clinical Health Act (HITECH Act), 42 U.S.C. §§ 1320d-6(a)–(b) (2006 & Supp. IV 2011). HITECH's tiered criminal penalties punish non-commercial use of unauthorized PHI less severely than commercial use. *Id.* § 1320d-6(b).

417. *See supra* note 10 and accompanying text.

418. 42 U.S.C. § 1320d-6(b)(3) (2006); *see also* Meridith Levinson, *Why Law Enforcement Can't Stop Hackers*, COMPUTERWORLD UK (July 9, 2011, 5:01 PM), http://www.computerworlduk.com/advice/security/3318744/why-law-enforcement-cant-stop-hackers/ (finding that "hackers rarely serve maximum sentences").

419. *Id.* §§ 1320d-6(a)–(b) (2006 & Supp. IV 2011).

420. *Id.*

421. PATRICK A. LANGAN & DAVID J. LEVIN, BUREAU OF JUSTICE STATISTICS, OFFICE OF JUST. PROGRAM, U.S. DEP'T. OF JUST., SPECIAL REPORT NCJ 193427, RECIDIVISM OF PRISONERS RELEASED IN 1994 (2002), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/rpr94.pdf (finding that within three years of release, 51.8% of prisoners were back in prison, serving time for a new prison sentence or for a technical violation of their release, like failing a drug test, missing an appointment with their parole officer, or being arrested for a new crime).

who pass through a prison's gates.[422] Nor does criminal activity fall when a criminal becomes an adult and faces substantially longer jail time.[423] Moreover, for cybercrime, jail time is a particularly weak deterrent because hackers realize "if they get caught, they might get five to 10 years, but when they get out, they'll have a book deal, make a TV movie or become a consultant."[424]

More generally, whether imprisonment deters cyber criminals depends on the certainty and severity that a particular punishment will be imposed.[425] Even if we assume a ten-year jail sentence strikes fear in the hearts of hackers, the deterrent value of jail time is substantially mitigated for hackers because they have to be caught and successfully prosecuted; neither of which are slam-dunk propositions.[426]

The social engineering aspect of criminal hacking means that these individuals are skilled in the art of deception. Hackers believe that there is only "a small chance of getting arrested"[427] because of their ability to disguise their identity[428] and reside overseas,[429] and because the resources needed to track down hackers are often limited.[430] Once caught, the successful prosecution of a hacker depends on the demonstration that a tight nexus exists between the physical evidence and the alleged perpetrator.[431] Such a nexus between the evidence and perpetrator can be difficult to demonstrate because merely having "thousands of credit-card details . . .

422. PEW Ctr. on the States, State of Recidivism: The Revolving Door of America's Prisons 2, 9 (2011), *available at* http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/sentencing_and_corrections/State_Recidivism_Revolving_Door_America_Prisons%20.pdf (concluding that recidivism rates suggest that the prison system falls short in deterring future criminal behavior).

423. *See* Joel Waldfogel, *The Irrational 18-Year-Old Criminal*, Slate (Jan. 30, 2007, 4:54 PM), http://www.slate.com/articles/business/the_dismal_science/2007/01/the_irrational_18yearold_criminal.html (finding that while the probability of being sentenced rises from 3 to 17% at age 18, there is no significant measured decrease in the arrest rate). The study found that the only significance to turning 18 in terms of re-arrest was that 18-year old offenders were slightly less likely to be re-arrested because they remained in prison for longer periods of time, serving on average longer sentences. *Id.*

424. Levinson, *supra* note 418 (finding that the deterrent effect for hackers is weakened by plea bargaining, reduced sentencing due to young age, or expectations of book deals, TV movie roles, or consulting jobs after release from prison); *see* Elinor Mills, *Crime and Punishment: Harsh Fate for Accused*, CNET News (May 27, 2012, 11:30 AM), http://news.cnet.com/8301-1009_3-57417442-83/crime-and-punishment-harsh-fate-for-accused-lulzsec-hackers/ (finding that hackers are unlikely to be deterred from cybercrime where they know that the anonymity of the Internet makes it is unlikely that they will be caught).

425. Valerie Wright, The Sentencing Project, Deterrence in Criminal Justice: Evaluating Certainty vs. Severity of Punishment 1–2 (2010); *see also supra* note 329 and accompanying text.

426. *See supra* note 425.

427. *See* Levinson, *supra* note at 418.

428. Glenny, *supra* note 18 at 5–6, 94.

429. Leigh Goessl, *The Problems Catching Hackers*, *Internet Security & Safety: Hacking*, Helium (Feb. 4, 2008), http://www.helium.com/items/840369-the-problems-with-catching-hackers.

430. Levinson, *supra* note 418 ("[L]aw enforcement officials lack the manpower, training, technical resources and political support necessary to crack down on these crimes.").

431. *See generally* Deb Shinder, *Preserving Digital Evidence to Bring Hackers and Attackers to Justice*, ComputerWorld (June 1, 2005), http://www.computerworld.com/s/article/print/102157/Preserving_Digital_Evidence_to_Bring_Hackers_and_Attackers_to_Justice?taxonomyName=Security&taxonomyId=17.

sitting on your computer is not a crime, nor is storing a key-logger virus" a crime.[432] If the alleged perpetrator of a hack has used a VPN or a proxy server, which can render their detection "by law enforcement very hard, if not impossible,"[433] demonstrating a tight nexus similarly fails.

Even after a tight nexus is established between the physical evidence of a cybercrime and a hacker defendant, the defendant may still avoid jail time if the case goes to the jury. The reason is that judges and juries are rarely fluent in cyber-speak.[434] If the triers of fact cannot follow the esoteric language of the cyberscribe, they are likely to develop doubts, which will undermine the prosecutor's ability to secure a guilty verdict.

The problem of understanding cyberscribe-speak is as old as the Egyptian pharaohs and arises any time a society is dependent on the literacy of a few of its members. So, if legal ambiguities, physical evidence considerations, and jury competence undermine our ability to use harsh penalties to deter hackers, how are we as a society to deter hackers from purloining PHI and committing MIT? The answer to this question does not require that we as a nation raise our computer science and code literacy level (as the Greeks and Roman might have suggested).

Nor is an e-security arms race a solution. Former President Reagan demonstrated that a well-funded party could use an arms race to defeat an opponent.[435] Imagining an arms race with hackers is not difficult. For example, HIPAA's Security Rule could be amended to mandate that PKI encryption be used for all PHI and that the HITECH Act's non-compliance penalties be made even harsher. But, given the money to be made trafficking in MIT, hackers would likely respond by ramping up their code breaking skills.[436] Already, a Quantum computing algorithm exists to factor very large numbers into their prime number factors, thereby creating the specter that PKI encryption could be defeated.[437] In addition, an e-security arms race is not in the United States' best interest because it will drive up the cost of healthcare. To illustrate, PKI encryption requires greater computing power, which would mean that healthcare providers would have to purchase more expensive EMR systems.[438] In turn, we as society would have to absorb the cost of more elaborate and more expensive EMR systems; a concept that would be anathema to both the HITECH Act and Affordable Care Act, which both seek to control healthcare costs.

---

432. *See* GLENNY, *supra* note 18 at 35.

433. GLENNY, *supra* note 18 at 94.

434. *See* DEBRA LITTLEJOHN SHINDER, SCENE OF THE CYBERCRIME COMPUTER FORENSICS HANDBOOK 36–37 (Ed Tittel et al. eds., Syngress Publishing 2002), *available at* EBSCO eBook Collection.

435. *See* Lee Edwards, Ronald Reagan and the Fall of Communism, Lecture No. 1141 (Dec. 4, 2009), *in* HERITAGE LECTURES, Mar. 2010, at 3.

436. *See supra* notes 326–27 and accompanying text.

437. *See* Gleick, *supra* note 12, at 370–71.

438. *See supra* note 131 and accompanying text.

A better solution for protecting PHI and curtailing MIT is to change the economic incentives offered to hackers. More specifically, if we are interested in protecting PHI and eliminating MIT, we need to remove the obscene profits that arise from trafficking in PHI and medical insurance information.[439] This could most easily be achieved by providing universal access to our healthcare system.

Recall that three factors drive up the cost of MIT: (1) the need to link personal information with health insurance coverage information; (2) the purchase of temporary insurance coverage by un- and underinsured patients purchase from the black market; and (3) the institutional healthcare providers who leverage medical identities by filing multiple fraudulent reimbursement claims.[440] Under a universal access to healthcare program, the first two factors would be negated: individuals' personality identity would establish insurance coverage and universal access would destroy the need for a black market.[441]

Arguably, provider healthcare fraud may even decrease in a healthcare system with universal access to patient care and a universal EMR system.[442] Even before the HITECH Act was enacted, professional medical record custodians recommended that patient verification processes:

> *[I]nclude obtaining and storing photo IDs or other means of identity verification or authentication if utilizing e-mail or Internet access. Make sure that the initial process is thorough, as determinations will be relied upon by subsequent users. The entire verification process and any data collected must be protected in accordance with the HIPAA security rule.*[443]

In the current era, where almost everyone has a cell phone that can receive email, it does not seem unreasonable to require insurers to verify with patients — in real time — that they are purchasing a healthcare service. After all, for more than twenty years health insurers have utilized pre-certification of healthcare services as a condition of coverage;[444] and modern strategies for combating healthcare fraud eschew the "pay-and-chase" enforcement scheme.[445] Prior verification that a patient

439. *See* Stanley C. Ball, Note, *Ohio's "Aggressive" Attack on Medical Identity Theft*, 24 J.L. & Health 111, 120 (2011) (finding that the rise in medical identity theft can be attributed to the high black market value of medical information documents); *see also supra* Table II and accompanying text.

440. *See supra* Part III.

441. *See supra* notes 148–54 and accompanying text.

442. *See supra* notes 155–60 and accompanying text.

443. Chris Apgar et al., *Mitigating Medical Identity Theft*, 79 J. AHIMA 63, 66 (2008).

444. *See* Committee on Utilization Management by Third Parties, Institute of Medicine, Controlling Costs and Changing Patient Care?: The Role of Utilization Management 14 (Bradford H. Gray & Marilyn J. Field, eds., 1989); *see also* Edward P. Richards & Thomas R. McLean, *Physicians in Managed Care: A Multidimensional Analysis of New Trends in Liability and Business Risk*, 18 J. Legal Med. 443, 447, 449 (1997).

445. *See* Verizon Business, *A New Approach to Combat Healthcare Fraud*, Solutions Briefs (2011), http://www.verizonbusiness.com/resources/solutionbriefs/sb_new-approach-to-combat-healthcare-fraud_en_

intended to purchase healthcare services would go a long way toward the elimination of the current lag time between the commission of MIT and its detection.

The point here is not to open a comprehensive debate on universal access to healthcare in America. Rather, our point is that as long as MIT is wildly lucrative, it is extremely unlikely that harsh penalties or a technology arms race with hackers will motivate hackers to stop probing EMR e-security systems. Accordingly, if we are interested in protecting PHI and minimizing EMR e-security breaches, the most rational solution is to destroy the black market for PHI and insurance information.

V. CONCLUSION

In the healthcare field, the "mummy's curse" is that we are allowing our medical record systems to be erected and guarded by a class of individuals who speak a foreign language. As a consequence, EMR e-security breaches and MIT are on the rise. We have attempted to combat these rising trends by enacting the HITECH Act to amplify HIPAA's Privacy and Security Rules, as well as to magnify civil monetary penalties applied to healthcare providers who are non-compliant with these rules. Yet, from the point of view of the malicious cyberscribe, these legal changes are nothing more than cosmetic changes. Accordingly, the HITECH Act's promise to reduce e-security breaches perpetrated by hackers (in search of a modern-day Aladdin's cave of wonders), may be somewhat illusory. On the other hand, if we are genuinely serious about protecting patients' privacy, a superior methodology to protecting PHI is to shift our healthcare system to one with universal access because a healthcare system with universal access would destroy the financial incentives associated with MIT.[446] It would create an effective deterrence to the commission of this crime.

xg.pdf (introducing a "new approach to healthcare fraud detection, [which] employ[s] integrated processes and a highly sophisticated data-reduction platform, capable of processing billions of transactions daily. . .[and] appl[ies] domain-specific predictive models, artificial intelligence algorithms and risk scoring to identify and prioritize abnormal patterns indicative of healthcare fraud" because "[t]he pay-and-chase approach to fraud remediation cannot compete with the omnipresent danger of an increasingly sophisticated criminal element"); *see also* Thomas R. McLean, *Big Brother and the Need for a Performance Measure Integrity and Fraud Detection Act*, LAW/TECH. J., 2d Quarter 2009, at 10–17 (arguing that metadata should be used to audit providers of EMRs).

446. *See supra* notes 144–60 and accompanying text.