

Journal of
**Health Care
Compliance**

Balance

Guidelines

**Augmented Informed Consent Helps
Health Care Organizations Respond to
New JCAHO Survey Tactics**

**Medical Identity Theft: The Future Threat
of Health Care Fraud Is Now**

**Teleradiology: Compliance Concerns
and Solutions, Part 1**

**Economic Credentialing: An Examination
and Critique of HHS' View of Conflict
Credentialing**

Effectiveness

Medical Identity Theft: The Future Threat of Health Care Fraud Is Now

Lack of Federal Law Enforcement Efforts Means
Compliance Professionals Will Have to Lead the Way

Latour "LT" Lafferty

Are you concerned about the future threat of identity theft in your health care organization as you transition to an electronic health care records system? Since 1992, there have been 19,428 complaints to the Federal Trade Commission (FTC) about medical identity theft, and the nonprofit public interest research group World Privacy Forum (WPF) estimates that medical identity theft has victimized as many as a half million people.¹ Pam Dixon, the executive director of the WPF and "the leading authority" on medical identity theft, believes "that future [threat] is now."²

Medical identity theft has been described as the "newest frontier in the ever-evolving crime of identity theft"³ and presents a ripe opportunity for a variety of perpetrators as the health care industry evolves into an electronic culture. This environment, however, is not adequately protected by current law enforcement agencies and criminal offenses.

As a result, medical identity theft presents a widespread threat in the health care industry, but there exists little deterrent threat from the threat of prosecution. Accordingly, health care compliance professionals must lead the way in the effort to combat the future threat of health care fraud through medical identity theft.

A. FINANCIAL VERSUS MEDICAL IDENTITY THEFT

There is a critical distinction between *financial* identity theft and *medical* identity theft, which is the fact that the "hallmark" of medical identity theft is the falsification of the victim's medical record with information from the perpetrator and crime.⁴ First, however, con-

Latour "LT" Lafferty is a shareholder with Fowler White Boggs Banker in Tampa, Florida and practices in the firm's White Collar Crime & Government Investigations Group. Mr. Lafferty is a former criminal and civil federal prosecutor having served 10 years as an Assistant U.S. Attorney (AUSA) in the Middle District of Florida. Mr. Lafferty is certified by the Health Care Compliance Association (HCCA) in Healthcare Compliance (CHC) and has published numerous articles and regularly speaks on Healthcare Corporate Compliance and Trial Advocacy topics. He can be reached at ltlafferty@fowlerwhite.com.

sider that financial identity theft is on the rise and ranks as one of the top consumer fraud complaints in the nation according to the FTC.⁵

Financial identity theft is characterized as a crime of opportunity⁶ and occurs anytime someone misappropriates your name, social security number, or other personal information to commit fraud or other crimes.⁷ Victims are targeted simply because their information is available (*i.e.*, they are easy targets). The federal Identity Theft and Assumption Deterrence Act (Act) and many state statutes (*e.g.*, Florida Statutes § 817.568) criminalize identity theft.⁸ The Act also established the FTC's identity theft program, which includes the core initiatives of assisting victims, educating consumers, law enforcement, and businesses, and established an identity theft data clearinghouse for the maintenance and dissemination of information.⁹

In 2003, the FTC published its identity theft survey report finding that in the previous five-year period approximately 10 million American consumers discovered that their personal information had been used to open fraudulent bank, credit card, or utility accounts or used to commit other crimes.¹⁰ The FTC estimated that the total loss to victims for identity theft was almost \$53 billion dollars annually and that Americans spent 300 million hours resolving issues related to identity theft.¹¹

Amazingly, the FTC found that in over 25 percent of reported identity theft cases, the victims knew or were related to the identity thief and that most cases originated in the workplace.¹² The survey found that approximately 70 percent of identity theft cases are committed by a co-worker, employee, or business owner (*i.e.*, insiders).¹³

Second, consider that *medical* identity theft is on the rise because of the increasingly high costs of health care services.¹⁴ Total health expenditures in the United States are estimated to be \$2.16 trillion in 2006 and are projected to rise to over \$4 trillion in 2015.¹⁵ It also is estimated that

health care fraud accounts for up to 10 percent of these expenditures.¹⁶

Consequently, Congress created the health care fraud and abuse program when it enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996.¹⁷ This highly coordinated national law enforcement effort is intended to ensure the integrity of federally subsidized health care benefits and resulted in 537 criminal prosecutions, 3,806 program exclusions, and 250 civil enforcement actions resulting in savings and expected recoveries of \$35.4 billion for fiscal year 2005.¹⁸

From this perspective, it is easy to understand why fraudsters will "set their sights" on health care providers — "because that is where the money is."¹⁹ Quite simply, "medical identity theft is the newest frontier in the ever-evolving crime of identity theft"²⁰ and grew by 197 percent from 2001 to 2005 according to the FTC.²¹

In the context of health care, *medical* identity theft may be viewed as a subset of both health care fraud and identity theft²² and has been characterized as combining "an unwholesome criminal trilogy of medical privacy violations, identity theft, and health care fraud."²³ Medical identity theft — in contrast to financial identity theft — occurs anytime a person's identity, such as his or her name or insurance information, is misappropriated to obtain medical services or goods or to make false claims for medical services or goods and falsify medical records to support those claims.²⁴

Identity theft may occur in a medical setting but not constitute medical identity theft, such as when a health care employee steals a patient's credit card and makes illegal purchases.²⁵ Further, health care fraud may involve the falsification of medical records and not involve identity theft, such as when a physician alters a medical record to cover up a medical error.²⁶ Neither of these cases, however, captures the true essence of medical identity theft, which is the theft of a person's *medical identity*.

Within this criminal trilogy of medical identity theft, however, there are core or "root" issues.²⁷ For example, identity theft encompasses the core issue of the intentional misuse of personally identifying information.²⁸ The core issue in health care fraud is the intentional submission of false claims.²⁹

The core issue in *medical* identity theft is derived from both identity theft and health care fraud and results in the intentional misuse of personally identifying information to receive medical goods or services typically resulting in the falsification of the victim's medical records.³⁰ The essence of medical identity theft is that it is both an information (*i.e.*, identity theft) and health care (*i.e.*, fraud and abuse) crime that results in financial, medical, and other harms to its victims.³¹

Medical identity theft, although not as well known as financial identity theft,³² is much more egregious because it victimizes people at one of their most vulnerable moments — when they are seeking medical treatment.³³ The "human cost" of medical identity theft includes financial losses, false entries in their medical history, the denial of insurance or the use of all available insurance resulting in benefits being "capped," the loss of reputation to the patient, physician, and health care organization depending on who was victimized, the loss of medical record privacy when records are subpoenaed as part of an investigation, and the loss of the proverbial value of time spent trying to correct the damage.³⁴

Without doubt the most significant harm that results from medical identity theft is when health care providers unknowingly base their medical decisions in treating a victim on inaccurate information from the thief's medical history. The harm caused by false entries in a victim's medical history is compounded because the entries are shared with a multitude of other health care providers, creating a significant risk of future harm.

B. COMMON CATEGORIES OF MEDICAL IDENTITY THEFT

Despite the fact that medical identity theft falls somewhere in between identity theft and health care fraud and is difficult to track because it is "a crime that hides," it is possible to identify some common categories or schemes for health care professionals to recognize.³⁵ First, be on the lookout for "*when bad guys get sick*" and use another person's medical identity for treatment.³⁶

In 2003, a career bank robber, check forger, and con artist — Joe Henslik — checked himself into a hospital for surgery using another person's identity, which he stole from his victim while working for a publisher after being released from prison.³⁷ Henslik received surgery costing \$41,188, which was billed to the unsuspecting victim — who has spent years trying to clear his medical and financial history.³⁸

Also consider Linda Weaver, a retired schoolteacher in Florida, who was erroneously diagnosed with diabetes in her medical history and was billed by a hospital for the amputation of her right foot after becoming a victim of medical identity theft.³⁹ Weaver refused to pay the hospital bill and sent the hospital notarized photos of her foot and toes, still attached.⁴⁰ Unbelievably, Weaver subsequently suffered a heart attack in May 2006. When she awoke in her hospital room two days later, a nurse asked her what drugs she had been taking for her diabetes — a disease with which Weaver had never been diagnosed.⁴¹

Second, beware of "*friends or relatives in need.*"⁴² Although seasoned criminals typically commit medical identity theft to obtain health care services, occasionally an individual who has no criminal background but is desperate for health insurance will commit the crime.⁴³ For example, a man with AIDS used his cousin's health insurance information to receive approximately \$76,000 worth of treatment over 15 years before confessing on his deathbed.⁴⁴ There also is the case of a New Mexico woman

treated for a toothache at a local hospital after assuming her sister's identity.⁴⁵

One provider stated that it gets about a dozen imposters presenting at its facility each week claiming they left their identification in their car, and the Pennsylvania Attorney General predicts that insurance cards eventually will come with photographs and signatures.⁴⁶

Third, the most outrageous form of medical identity theft is "*when professionals are dishonest*," which arises when insiders — anyone with access to your medical information including clerks, nurses, and even physicians — fabricate care on real patients for profit.⁴⁷ Richard Skodnek, a Boston psychiatrist, was convicted of fraud after falsely billing insurance companies for treatment sessions involving false diagnosis, treatment sessions, and medical histories.⁴⁸ Skodnek diagnosed one of his victim's children, whom he had never seen, and then billed insurance for his services.⁴⁹

Most notably, however, Ronald Mikos, a Chicago podiatrist under grand jury investigation, was convicted of murder after shooting and killing one of his patients in 2002.⁵⁰ The jury found that Mikos killed his patient when she refused to lie for Mikos after he misused her personal information to falsely bill insurance.⁵¹

Fourth, organized crime has been known to implement complex schemes called "*clinic takeovers*" in which Medicare patients are lured into a clinic staffed with either legitimate or illegitimate physicians. Services are performed and then billed to the government without the patient even realizing he or she has been victimized.⁵² These schemes are designed to conceal themselves through large numbers of smaller, routine claims for a short period of time. Consequently, the perpetrators typically operate the clinic for only a few months before shutting it down and disappearing.⁵³

In California, two Ukrainian brothers were indicted for allegedly setting up a phony health clinic where phony doctors performed cursory exams and ordered ul-

trasound tests on patients who were lured to the clinic with offers of free transportation and baby formula.⁵⁴ It is hard for some to imagine that the health care industry is a ripe breeding ground for organized crime, according to Dixon.⁵⁵

Fifth, there are both the innocent and not so innocent "*opportunists*," or individuals working in a setting where there is access to confidential patient data and the temptation to take advantage of their access.⁵⁶ Opportunists have included 39 employees, or insiders, of a medical center in New York City's public health system who simply could not resist the "innocent" temptation to review the records of a seven-year-old girl in a highly publicized child abuse case even though they did not steal the child's medical identity.⁵⁷

More typical is the recent indictment of Fernando Ferrer, Jr. and Isis Machado by the United States Attorney for the Southern District of Florida. According to the indictment,⁵⁸ Machado was employed as a front desk office coordinator with access to computerized patient information in the performance of her duties at a health care facility. Machado wrongfully accessed the facility's computerized patient files and downloaded the personal identification information of more than 1,100 patients — including patients' names, dates of birth, social security numbers, Medicare numbers, and home addresses.

Machado sold the patient information to her cousin, Ferrer, who then caused the stolen patient information to be used in connection with the submission of approximately \$2.8 million in false claims to Medicare. Machado and Ferrer were charged with conspiracy to commit computer fraud, identity theft, and wrongfully disclosing individually identifiable health information⁵⁹ as well as computer fraud,⁶⁰ aggravated identify theft,⁶¹ and wrongful disclosure of individually identifiable health information under HIPAA.⁶² This HIPAA prosecution is the first of its kind in the Southern District of Florida and only the third in the nation, but it is not an isolated incidence.⁶³

C. ELECTRONIC HEALTH CARE SYSTEMS

The advent of digitized patient medical and health records⁶⁴ toward a new vision for health care through the use of information technology could both aggravate the spread of medical errors caused by the reliance on false medical histories and make it easier to actually correct these false medical histories all at the same time. In 2004, President Bush called for widespread adoption of interoperable electronic health records (EHRs) within 10 years and established the position of the National Health Information Technology Coordinator by Executive Order.⁶⁵

The executive order required the development and implementation of a strategic plan for the nationwide implementation of interoperable health information technology in both the public and private sectors.⁶⁶ The National Health Information Network (NHIN) is a government-sponsored plan for the development of a sophisticated national network of digitized patient health records and medical files for access by hospitals, physicians, insurers, and others — including fraudsters.⁶⁷

The basic premise behind the NHIN's ambitious modernization effort is the transition from paper to electronic medical files⁶⁸ and the creation of an "electronic health care culture"⁶⁹ in which health care information systems (HISs) and supporting applications have created an environment of open electronic access among nurses, employees, physicians, specialists, supporting clinics, and other partners in the spirit of collaboration.⁷⁰

Although the current mantra is that digitized medical records will improve health care, reduce fraud, and save lives by reducing medical errors, this mantra does not take into account the growing incidence of medical identity theft and the opportunity digitized records present for fraudsters.⁷¹ At the American Health Information Community, a health care information technology advisory panel recently established by the Department of Health and Human Services (HHS), a physician recently testified before

the confidentiality, privacy, and security work group that "we believe that as PHRs (personal health records) and EHRs (electronic health records) proliferate and users reach the tens of millions, fraudsters will set their sights on many of these healthcare sites, starting with those with the largest user bases coupled with the weakest defenses...because that is where the money is."⁷²

The movement toward digitized health records has in fact created a riskier environment that is virtually impossible to audit and monitor for prevalent security risks⁷³ and was imagined and designed, as was HIPAA, without regard to the complexities presented by medical identity theft.⁷⁴

In particular, the greatest benefit of digitized information in the context of the NHIN and EHRs (*i.e.*, increased portability) also increases the potential improper accessibility of an individual's personally identifiable health information within the health care system to criminals.⁷⁵ Further, the NHIN could simply transmit false entries in digitized records arising from medical identity theft and exponentially perpetuate the damage through a nationwide system.⁷⁶

According to the World Privacy Forum, "the digitization and wider availability of patient health records without adequate understanding and risk assessment could pose many difficulties."⁷⁷ The Government Accountability Office (GAO) recently noted that there are "significant weaknesses in information security controls" in Medicare and Medicaid claims processing, which have already been digitized.⁷⁸ Further, "electronic healthcare records are viewed by criminals as 'fresh meat' and are worth an estimated \$50 to \$60 each on the black market, according to Dixon."⁷⁹

As one U.S. attorney has stated, "In a rapidly expanding world of electronic medical records, preserving the privacy and integrity of confidential patient information is critical."⁸⁰ Consequently, regulatory agencies are paying more attention to privacy and security issues as the industry evolves into an electronic culture.⁸¹

D. ENFORCEMENT INITIATIVES

The critical point to be gleaned from these examples of medical identity theft and the impact of digitized health care systems is that medical identity theft impacts every level of the system, including the patient, physician, and health care organization as well as the payors, and there must be increased diligence to prevent this crime. Because the future of health care fraud is now, specific measures must be taken to deter this unique and ever-more-common crime.

A health care organization and its patients may be victimized simply because health information is readily available. In this context, the confidentiality of patient information is strictly protected by HIPAA and state law.⁸² HIPAA is enforced by the HHS Office of Civil Rights (OCR) and includes a criminal sanction including a maximum fine of \$100,000 and up to five years imprisonment or a maximum fine of \$250,000 and up to 10 years imprisonment if the person intended to sell, transfer, or use the protected health information for personal gain or malicious harm.⁸³ The health care provider also may be assessed a civil monetary penalty for the HIPAA violation.⁸⁴

HIPAA is a federal regulation designed in part to promote uniformity and confidentiality in the use and transmission of health information through "administrative simplification," or the creation of a uniform, national language for the health care industry.⁸⁵ HIPAA's administrative simplification provision is intended to facilitate the electronic exchange of health information and thereby promote efficiency and reduce costs.⁸⁶

In this context of administrative simplification, Congress authorized HHS to develop three sets of national standards including the following:

- Standards for electronic transactions and code sets (*i.e.*, standards for format and content to be used by all health care organizations when they conduct transactions electronically),
- Standards for privacy of individually identifiable health information (*i.e.*, pro-

tection of privacy and confidentiality of personal medical records), and

- The security standards (*i.e.*, practices and technologies used to protect electronic networks and devices used to house and transmit electronic health information).⁸⁷

These national standards are intended to facilitate the goal of demonstrative simplification while addressing the public's concerns about transferring confidential information electronically.

As the Federal Trade Commission (FTC) has stated with respect to identity theft in general, the most important deterrent to any crime is the increased threat of prosecution.⁸⁸ Currently, there is no separate and distinct medical identity theft crime, which the World Privacy Forum finds to be "remarkable."⁸⁹

Further, one commentator has noted that "because of its nature, medical identity theft doesn't fall neatly under the purview of an individual federal or state agency. As such, there is no single agency or single point of contact for victims."⁹⁰ For example, consider that in 2006, the President established the Identity Theft Task Force — a collaboration between the U.S. Department of Justice (DOJ) and the FTC for the purpose of "developing a comprehensive national strategy to combat identity theft."⁹¹

The Identity Theft Task Force's goals include improving the government and the private sector's ability "to bring identity thieves to justice, to mitigate the risks of identity theft for individuals and companies, and to assist identity-theft victims in recovering from the effects of this pernicious crime."⁹² The Identity Theft Task Force includes 17 federal agencies and departments, each with particular expertise contributing to their ability to fight identity theft.⁹³

DOJ has prosecuted many identity thieves, including charging 432 defendants in fiscal year 2006 (through the end of July 2006) with aggravated identity theft, and the Federal Bureau of Investigation (FBI), an agency of the DOJ, has 1,587 pend-

ing identity theft-related cases.⁹⁴ The first criminal conviction under HIPAA was a financial identity theft case in which Richard Gibson, an employee of a Seattle cancer center, misappropriated a patient's identity and charged more than \$9,000 on falsely obtained credit cards.⁹⁵

The federal government's Identity Theft Task Force empowers the FBI, the U.S. Secret Service (USSS), the U.S. Postal Inspection Service (USPIS), and the Social Security Administration Office of the Inspector General (SSA OIG) to investigate identity theft.⁹⁶ Notably absent from this task force, however, is the Office of Inspector General, whose primary responsibility is to investigate health care fraud. While victims of financial identity theft can report their offense to the FTC and various other investigatory agencies, Dixon believes that "what happens to victims of medical identity theft is they're just [left] floundering."⁹⁷

Today's health care environment is very dynamic and ripe for opportunity notwithstanding that it is highly regulated. According to Elizabeth Roop, a health care reporter, Dixon gave the following warning,⁹⁸ "I don't know that the medical professional really understands the thundering herd that's coming their way. It's not pretty; these people are resourceful, determined, and stealthy. There are some hospitals and healthcare providers that are more sophisticated and have built a few more moats around their castle, but in general, I think in the healthcare sector the problems and challenges are so complex that they're just not ready for the influx of organized crime."

"You can't just clamp down a hospital the way you can clamp down a bank, so it's infinitely more complicated," she adds. "The path ahead will be tough; it's doable, but it's tough."

So how can you beef up the "moat" around your health care castle and confront the tough job of the future of health care fraud? For starters, it is very important that the executive management team be fully aware

of and committed to the importance of patient information security and the potential repercussions for violations.⁹⁹ The health care organization should foster a culture of compliance recognizing the zero-tolerance policy for violations of federal and state patient confidentiality regulations that reverberates throughout the organization and acts as a meaningful deterrence.

Second, compliance and privacy officers responsible for ensuring the confidentiality and privacy of health records within their organizations are urged to assess the risk within their organizations for HIPAA compliance — paying close attention to their own employees because "medical data has a street value today of \$50 a record," according to Dixon.¹⁰⁰ Dixon urges us to pay attention to "healthcare insiders," including "physicians, nurses, technicians and other trusted employees" because "healthcare already is under attack."¹⁰¹

Third, create and implement effective policies and procedures based upon your knowledge and understanding of your specific risks.¹⁰² These procedures should include, for instance, requiring patients to present picture identification before receiving treatment.¹⁰³ Pay particular attention to physical security within your organization and ensure that your policies and procedures protect confidential information.¹⁰⁴

A California medical group suffered a significant security violation after someone broke into its facility and stole two new Dell computers containing patient information for 185,000 people that had been transferred to the computers from its secured servers as part of a patient billing project and year-end audit.¹⁰⁵ This example further illustrates the prudence of controlling access through physical security but also that sensitive patient information should be encrypted to minimize the risk of exposure.¹⁰⁶ Also, consider protecting your patients by not using their name, social security number, or date of birth for identification purposes to further minimize the risk of exposure.¹⁰⁷

Daniel Garcia, chief compliance officer for Kaiser Foundation Health Plan, Inc., one of the nation's largest integrated delivery systems, likened Kaiser's encryption policy to a "cultural revolution" because restricting physician's access to health information is counter to what they believe is in the best interests of patient care.¹⁰⁸ The first step in instituting new privacy policies, Garcia added, is to get physicians to accept new ideas about protecting health information in light of technology advances.¹⁰⁹

After a Kaiser employee's laptop containing beneficiary information was stolen, Garcia started a policy prohibiting the access or storing of personal health information on personal laptops unless that information is encrypted.¹¹⁰ Garcia admitted that allowing physicians and others to store personal health information on laptops was an outdated practice.¹¹¹

Perhaps most importantly, the compliance and privacy officer should develop a rapid response plan, including an instant response team, to prevent and mitigate security breaches because putting a response plan together quickly is a challenge.¹¹² The appropriate response may include immediately notifying the patient of the security breach under state law. State security breach laws are designed to prevent identity theft and require certain organizations not only to implement and maintain security procedures as well as protect personal information from unauthorized access, but also expeditiously notify a state resident whose information was or was reasonably believed to have been acquired by an unauthorized person when a security breach occurs.¹¹³

Further, federal legislation entitled the "Privacy Rights and Oversight for Electronic and Commercial Transactions Act of 2006" (PROTECT Act) was introduced this year with the intent of "empowering consumers and giving them a say in how companies buy, sell, and market their private data, while entitling them to effective security protections."¹¹⁴ Recognizing that identity theft is one of the fastest growing

crimes, the Act includes a Privacy Bill of Rights encompassing the right to know and correct information that is being kept about them, a right to medical privacy including the promulgation of a HIPAA regulation requiring the reporting of any unlawful disclosures of identifiable health information, a private right to sue and seek damages for negligent data handling, and the right to the immediate consumer notification and disclosure of a data security breach.¹¹⁵

Finally, be prepared to respond to your own patients' request for an accounting of disclosures, copies of medical files, and corrections of erroneous information in their medical files. Remember, one of the chief complaints cited by the World Privacy Forum was the inability of victims to access and correct their own medical records.¹¹⁶

The advent of digitized medical records and an electronic health care culture presents a wonderful vision for the future of health care; a vision of improved quality, increased efficiency, and more cost-efficient care. There is another vision, however, that is gaining greater recognition and understanding as more and more patients are being preyed upon at their most vulnerable moment, when they seek medical treatment.

Medical identity theft is a relatively new crime that falls somewhere in between the more commonly known crimes of financial identity theft and health care fraud. Consequently, there is no federal law enforcement agency specifically tasked with the responsibility of investigating and prosecuting this offense because, quite simply, there is no specifically recognized crime of medical identity theft. Therefore, compliance professionals must step up and lead the way in the health care industry with increased vigilance to combat and deter this future threat of health care fraud because the future is now.

Endnotes:

1. Dixon, Pam, Medical Identity Theft: The Information Crime That Can Kill You, *The World Privacy Forum*, pg. 13, 22 (Spring 2006).
2. Conn, Joseph, Healthcare Seen As Ripe For ID Theft, *Modern Health* (2006).

3. Medical Identity Theft Case Pursued in Florida, Rutgers Identity Theft Resolution Center, at http://www.identitytheft911-sunj.com/alerts/alert_ext?sp=631.
4. Dixon, Pam, *supra* n.1 at pg. 17. (For the purpose of separating medical identity theft from the plethora of health care fraud and identity theft crimes, the essential hallmark of medical identity theft is the use of identity information that results in falsification of the victim's medical charts with information related directly to the crime, not the actual conditions of the real patient.)
5. The State of Florida Department of Elder Affairs, Consumer Resource Guide, 4th Ed. Pg. 179 (2005).
6. US-CERT, United States Computer Emergency Readiness Team, Cyber Security Tip ST05-019, Preventing and Responding to Identity Theft.
7. State of Florida Department of Elder Affairs, *supra* n. 5.
8. 18 U.S.C. § 1028; e.g., Florida Statutes § 817.568.
9. Report, Federal Trade Commission, Overview of the Identity Theft Program, Oct. 1998 – Sept. 2003 pg. 2 (2003).
10. Koerner, Brian, General Identity Theft Statistics, About Identity Theft; Federal Trade Commission, Identity Theft Survey Report (Sept. 2003).
11. *Id.*
12. *Id.*
13. *Id.*
14. Long, Kurt, *Healthleaders EXTRA! Addressing the Growing Threat of Medical Identity Theft*, Health Leaders Media at http://www.healthleadersmedia.com/view_feature.cfm?content_id=83793.
15. Centers for Medicare and Medicaid Services, Office of the Actuary, National Health Statistics Group, at <http://www.cms.hhs.gov/NationalHealthExpendData/> (see Historical; NHE summary including share of GDP, CY 1960-2004; file nhegdp04.zip).
16. Dixon, *supra* n. 1 at pg. 24-25.
17. Title 42, U.S.C. § 1320a-7c.
18. Semiannual Report, Office of Inspector General (April 1, 2005 - September 30, 2005), U.S. Dept. Of Health & Human Services Pg 7.
19. Conn, *supra* n. 2.
20. Medical Identity Theft Case Pursued in Florida, Rutgers Identity Theft Resolution Center, at http://www.identitytheft911-sunj.com/alerts/alert_ext?sp=631.
21. Long, Kurt, The Grave Costs of Medical Identity Theft, at <http://health-care-it.advancweb.com/common/editorial/editorial.aspx?CC=78748>.
22. Dixon, *supra* n. 1 at pg. 16-19.
23. Press Release, Two Charged in Computer Fraud, Identity Theft And Health Care Fraud Conspiracy, The United States Attorney's Office, Southern District Of Florida (Sept. 8, 2006).
24. Dixon, *supra* n. 1 at pg. 16.
25. *Id.*
26. *Id.*
27. *See Id.* pg. 16-19, 35.
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.*
32. Dixon, *supra* n. 1 at pg. 7.
33. Rutgers Identity Theft Resolution Center, *supra* n. 20.
34. *See* Dixon, *supra* n. 1 at pg. 26-30.
35. *See Id* at pg. 36-38; Alexander, Max, ID Thieves' New Target, How to Protect Yourself at <http://www.rd.com/content/openContent.do?contentId=30232>.
36. Alexander, *supra* n. 35.
37. *Id.*
38. *Id.*
39. Menn, Joseph, ID Theft Infects Medical Records. Victims Face Bogus Bills and Risk Injury or Death. Privacy Laws Make Such Fraud Hard to Pursue, *latimes.com* at <http://www.latimes.com/business/la-fi-medid25sep25,0,5686619.story?coll=la-home-headlines> (Sept. 25, 2006).
40. *Id.*
41. *Id.*
42. Alexander, *supra* n. 35.
43. *See* Dixon, *supra* n. 1 at pg. 37. Alexander, *supra* n. 35.
44. *Id.*
45. *See* Dixon, *supra* n. 1 at pg. 38.
46. Alexander, *supra* n. 35.
47. *See* Dixon, *supra* n. 1 at pg. 36, 38 (Spring 2006); Alexander, *supra* n. 35; Menn, *supra* n. 39.
48. *See* Alexander, *supra* n. 35; Menn, *supra* n. 39.
49. *See* Alexander, *supra* n. 35.
50. *See* Menn, *supra* n. 39.
51. *Id.*
52. *See* Dixon, *supra* n. 1 at pg. 36, 38; Alexander, *supra* n. 35; Menn, *supra* n. 39; Roop, Elizabeth S., Stealing You, Medical Identity Theft Vol. 7, No. 21 Pg. 16 (Oct. 23, 2006).
53. *Id.*
54. *See* Alexander, *supra* n. 35; Menn, *supra* n. 39.
55. Roop, *supra* n. 52.
56. *See* Dixon, *supra* n. 1 at pg. 36, 38.
57. Long, Kurt, *supra* n. 14.
58. Press Release, Two Charged in Computer Fraud, Identity Theft and Health Care Fraud Conspiracy, The United States Attorney's Office, Southern District Of Florida (Sept. 8, 2006).
59. 18 U.S.C. § 371.
60. 18 U.S.C. § 1030.
61. 18 U.S.C. § 1028A.
62. 42 U.S.C. § 1320d-6(a)(2).
63. United States Attorney's Office, *supra* n. 58.
64. This category of records includes electronic medical records "EMRs," electronic health records "EHRs," or electronic health information "EHI," which are all used interchangeably.
65. Request for Information, Department of Health and Human Services, National Coordinator for Health Information Technology, Development and Adoption of a National Health Information Network at <http://www.hhs.gov/healthit/>

- documents/NHIN_RequestForInformation_Final.doc.
66. *Id.*
 67. Dixon, Pam, *supra* n. 1 at pg. 9-10 (Spring 2006).
 68. *Id.*
 69. Fahrner, Stacey, "Kaiser CCO Offers Tips On Emerging Compliance Issues," *CCH Health Care Compliance Letter*, Vol, 9, Issue 23 (Nov. 14, 2006).
 70. Long, Kurt The Grave Costs of Medical Identity Theft, at <http://health-care-it.advanceweb.com/common/editorial/editorial.aspx?CC=78748>.
 71. Dixon, *supra* n. 1 at pg. 9-10.
 72. Conn, *supra* n. 2.
 73. Long, *supra* n. 70.
 74. See Dixon, *supra* n. 1 at pg. 36, 42.
 75. *Id.* at pg. 9-10.
 76. *Id.*
 77. *Id.*
 78. Alexander, *supra* n. 35.
 79. Roop, *supra* n. 2.
 80. The United States Attorney's Office, *supra* n. 58.
 81. See Fahrner, *supra* n. 69.
 82. Title 42, U.S.C. § 1320d *et seq.*; see e.g., Florida Statutes §§ 295.3025, 3035, and 456.057 regarding the confidentiality of hospital and physician medical records respectively.
 83. 42 U.S.C. § 1320d-5.
 84. *Id.*
 85. CCH *HIPAA Security Guide*, Chapter. I-1 at 11,001(2006).
 86. *Id.*
 87. Speers, Tom, Wilcox, Spence, and Brown, Bob, The Privacy Rule, Security Rule, and Transaction Standards: Three Sides of the Same Coin, *Journal of Health Care Compliance*, pg. 11-12 (Jan. – Feb. 2004).
 88. Report, Federal Trade Commission, Overview of The Identity Theft Program, Oct. 1998 – Sept. 2003 pg. 7 (2003).
 89. Dixon, *supra* n. 1.
 90. Roop, *supra* n. 52.
 91. Fact Sheet: The Work of the President's Identity Theft Task Force, U.S. Dept. Of Justice (Sept. 19, 2006).
 92. *Id.*
 93. *Id.*
 94. *Id.*
 95. *United States v. Gibson*, W.D. Wash., No. CR04-0374 RSM.
 96. U.S. Dept. Of Justice, *supra* n. 91.
 97. Roop, *supra* n. 52.
 98. *Id.*
 99. Long, *supra* n. 14.
 100. Conn, *supra* n. 2.
 101. *Id.*
 102. Hubbard, Catherine, Response Plan Key to Mitigation of Security Breach, *CCH Health Care Compliance Letter*, Vol 9, Issue 11 (May 30, 2006); Long, *supra* n. 14.
 103. Long, *supra* n. 14.
 104. *Id.*
 105. Kawamoto, Dawn, Medical Group: Data of 185,000 People Was Stolen ZDNet News at http://news.zdnet.com/2100-1009_22-5660514.html.
 106. Hubbard, *supra* n. 102.
 107. Song, Kyung. M., 3 Swedish Patients Say IDs Stolen At Ballard Campus; Worker Fired, the Seattle Times.
 108. Fahrner, *supra* n. 69.
 109. *Id.*
 110. *Id.*
 111. *Id.*
 112. Hubbard, *supra* n. 102.
 113. *Id.*
 114. Lynch-Afryl, Sheila, "Clinton Bill Would Broaden Scope of Covered Entity Definition," *CCH Health Care Compliance Letter*, Vol. 9, Issue 16 (Aug. 7, 2006).
 115. *Id.*
 116. Dixon, *supra* n. 1 at pgs. 40-41.

(© 2007, CCH, Incorporated, Journal of Health Care Compliance, Volume 9, Number 1, January- February 2007, page, 11. Reprinted with permission.)