

Medical Privacy at Risk

A Call for Effective Legislative Action

Tens of millions of Americans may have their health-related information lost, stolen, or exposed each year, and almost 200,000 may become victims of medical identity theft each year. We can, and must, do a better job of protecting the privacy and security of health-related information.

PogoWasRight.org
July 22, 2007

Index	
Executive Summary	
General Background	1
Potential Harm to Individuals	3
Medical Identity Theft	4
Has HIPAA Helped?	7
HIPAA Statistics	8
Surveys of HIPAA Compliance Rates	9
	12
Preliminary Study	
Method	12
Inclusion Criteria	12
Sources of Information	13
Results	14
Discussion	19
Need for Transparency and Accountability	21
Recommendations	22
Summary	22
For More Information	23
Acknowledgements	23
Disclosure	23
Appendix	
2003 Chronology of Incidents	
2004 Chronology of Incidents	
2005 Chronology of Incidents	
2006 Chronology of Incidents	
2007 Chronology of Incidents	

Executive Summary

Background

In 2004, President Bush established the office of Health Information Technology with the ambitious goal of creating a Nationwide Health Information Network (NHIN) by 2014. On paper, the concept seemed potentially beneficial, but a number of consumer and patient advocacy organizations have raised important concerns about gaps in our current laws and about the rights of individuals to control access to their health information. Incidents reported in the media, such as a laptop stolen from an employee's home that contained data on 26.5 million veterans or a hospital's backup tapes containing unencrypted data are lost in transit have generated understandable public anxiety as to whether sensitive health information is really secure and protected.

To date, there has been little systematic data that would enable us to determine the frequency, scope and severity of the security and privacy incidents involving health information. Partial statistics appear scattered across numerous governmental agencies and other sectors without any centralized analysis that has been made publicly available. The absence of mandatory disclosure or reporting laws has thwarted efforts to determine how many individuals have their health information lost, stolen, or compromised each year, and with what consequences.

The purpose of the present preliminary study was to analyze incidents that occurred after the HIPAA Privacy Rule was implemented in April 2003. Only incidents involving personally identifiable health information that were reported in the media or that were readily available from online sources were included. There was no requirement that the entity experiencing the incident be a HIPAA-covered entity because the issue is not whether HIPAA is effective, but rather, does our health information and medical privacy continue to be at great risk.

Major Findings

Out of 291 incidents meeting inclusion criteria, 249 incidents for which sufficient data were available for analysis accounted for the potential or actual exposure, loss, or compromise of health information of over 16,000,000 people in the approximate 4-year period. For the entire sample, 36 of the reported incidents (12%) resulted in fraud or identity theft, including medical identity theft.

Dishonest employees who acquired and then used or sold the individual's data to others accounted for 75% of all incidents that were reported to have resulted in misuse of information.

Consistent with GAO reports and health industry survey findings, some entities experienced multiple security or privacy incidents. This was evident across all sectors involved in the provision of services or the custody of health records, e.g., university-affiliated health care systems, state and county agencies, insurers, and pharmacy chains. During the time period covered by this study, the Department of Veterans Affairs experienced 8 incidents involving lost, stolen, or compromised health information.

Limitations of the Present Study

This preliminary study relied primarily on media reports, which are not a random sample of all health information incidents. Although almost all cases of insider theft resulted in misuse of information, one cannot conclude that the relationship would hold for the general population because of selective bias in what cases get reported by the media.

The 16,000,000 figure is undoubtedly only the “tip of the iceberg” when it comes to the number of individuals who have had their personally identifiable health information lost, stolen, exposed, or compromised since the HIPAA Privacy Rule was implemented. When a defense contractor fails to encrypt health-related data over an FTP connection, almost a million people may suddenly have their health information captured or compromised – and according to GAO reports, such security failures are probably happening much more often than the public discovers. Similarly, when insurance companies send backup tapes of health claims data to processors and the unencrypted tapes are stolen from a lock box in the processor’s office, hundreds of thousands’ patients’ sensitive information is suddenly at risk. Surveys and governmental reports make it clear that the 291 incidents located in this study are but a proverbial “drop in the bucket.”

Recommendations

1. Congress should authorize and fund a 3-year study where all incidents of privacy or security breaches of health information or patient information are reported to one agency for compilation and analysis. The Department of Justice survey that is scheduled for next year should be reviewed to determine if the wording of the questions will adequately permit assessment of the nature of health-related information incidents, their severity, frequency, and consequences.
2. Anonymized privacy and security breach incidents that involved personally identifiable health information should be made available on a publicly available web site to permit the public, patient advocacy organizations, researchers, and interested parties access to data.
3. Congress should enact legislation that closes the gaps in the existing network of laws and that requires any entity in possession of personally identifiable health-related information to comply with uniform privacy and security standards, allowing states to set higher minimal standards. Commercial data miners or resellers should be barred from obtaining or retaining health-related information without the express opt-in informed consent of the individual or their guardian.
4. Congress should hold hearings and require all federal agencies, cabinet departments, representatives of the health insurance industry, and state Medicaid agencies to provide statistics on the number of relevant incidents since April 2003 and their severity and consequences.

Even if data are not misused for fraudulent purposes, the privacy and security of health-related information is fundamental to individuals seeking care. We can and must do better.

General Background

Protecting the privacy, confidentiality, and security of health or medical information has always been a daunting task, but even more so since the shift to electronic health records (EHR) and information-sharing databases. In 2004, President Bush established the office of Health Information Technology with the ambitious goal of creating a Nationwide Health Information Network (NHIN) by 2014. On paper, the concept seemed potentially beneficial, but a number of consumer and health care groups raised important concerns that have yet to be adequately addressed.

As one example, in June 2006, the National Committee on Vital and Health Statistics (NCVHS) made a number of recommendations.¹ One of the most challenging aspects to both protecting privacy and assessing privacy violations is the fact that there are generally no specific types of data that are uniformly designated as “protected” or “private” across all settings and situations and across all states. Once protected information leaves the hands of an entity required to protect it and is shared with others who are not bound by the privacy laws, the information loses its protection. As the NCVHS explains:

As information flows away from the people and organizations that collect and use it for its primary purpose, health care delivery, it becomes increasingly difficult to understand or control how it is being used for secondary or even tertiary purposes. Therefore, before moving to the NHIN, it is essential to tighten the gaps in the Privacy Rule that permit information to leak and to adopt a more comprehensive privacy protection regime.

As one of their recommendations, then, they suggested:

[Health and Human Services] should work with other federal agencies and the Congress to ensure that privacy and confidentiality rules apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools.

That recommendation and other thoughtful and important recommendations made by the NCVHS have not been implemented.

In light of the lack of progress and ongoing risks to patient privacy, a recent Modern Healthcare editorial calling for the NHIN program to be scrapped. The editorial notes:

“[The Bush administration] has left “control” of the health IT process in the hands of a contentious mix of IT vendors, data-miners, insurers and a handful of healthcare interest groups. The only ones left out are the American people, who

¹ Privacy and Confidentiality in the Nationwide Health Information Network. National Committee on Vital and Health Statistics, June 2006. Retrieved from <http://www.ncvhs.hhs.gov/060622lt.htm>.

might be concerned that invading their privacy may be the signal accomplishment of this concatenation of conflicts of interest.²

Government Accountability Office reports have also noted significant concerns.^{3 4} It is somewhat troubling that in the face of substantive criticism and repeated expressions of concerns, HHS thought it was doing just fine, and it actually disagreed with GAO's recommendations. The GAO report states:

We recommended in our report that the Secretary of HHS define and implement an overall approach for protecting health information as part of the strategic plan called for by the President. This approach should (1) identify milestones for integrating the outcomes of its privacy-related initiatives, (2) ensure that key privacy principles are fully addressed, and (3) address key challenges associated with the nationwide exchange of health information.

In commenting on our report, HHS disagreed with our recommendation and referred to the department's "comprehensive and integrated approach for ensuring the privacy and security of health information within nationwide health information exchange."

While we acknowledged in our report that HHS had initiated key efforts to address its objective to protect consumer privacy, we found that HHS's approach for addressing privacy and security did not address elements that should be included in a comprehensive privacy approach, such as milestones for integration, identification of the entity responsible for integrating the outcomes of privacy related initiatives, and plans to address key privacy principles and challenges. In recent discussions with GAO, the National Coordinator for Health IT agreed with the need for an overall approach to protect health information and stated that the department was initiating steps to address our recommendation.

-- GAO 998-T, June 2007 pp 3-4

At the present time, then, most patient advocacy organizations and consumer organizations are concerned about the state of privacy and security of health information and the potential for harm to individuals if these concerns are not addressed.

² Retrieved online July 13, 2007 from <http://www.modernhealthcare.com/apps/pbcs.dll/article?Date=20070712&Category=FREE&ArtNo=70712003&SectionCat=FRONTPAGE&Template=printpicart>

³ HEALTH INFORMATION TECHNOLOGY: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy. Government Accountability Office, GAO-07-400T, February 2007. Retrieved online from <http://www.gao.gov/new.items/d07400t.pdf>.

⁴ HEALTH INFORMATION TECHNOLOGY: Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy. Government Accountability Office, GAO-07-988T, June 2007. Retrieved from <http://www.gao.gov/new.items/d07988t.pdf>.

Potential Harm to Individuals

When patients do not trust that their health information will be kept private, confidential, and secure, one potential consequence is that they may avoid seeking treatment. As one example, following breaches involving lists of AIDS or HIV+ patients, there was an immediate downturn in people seeking treatment. The reluctance of people to seek medical treatment if they risk exposure of their health information cannot be ignored, nor the consequences of lack of treatment on their health.

Loss of trust leading to less care or delayed care is not the sole consequence of inadequate privacy and security protection, however. People may be affected professionally and in their personal lives as revelation of personal health information may put careers and insurance at risk. On a personal level, a privacy breach may cause grievous pain to the patient or their family, with consequences to the employee or provider who breached privacy.

In Kentucky, a county ambulance employee took pictures at accident scenes with his cell phone and then uploaded pictures of some of the victims and accidents to MySpace, where he blogged about his work as a paramedic. One of the pictures was of a fatal accident involving a teenager. The paramedic was assaulted by the teen's grieving family, he was fired from his job for the privacy breach and unethical conduct, and the family members were charged with felony assault.⁵

From an employment perspective, to the extent that health records contain sensitive information which may or may not even be accurate, the importance of what is in a patient's health record and whether the patient gets to control access to the record and to correct any errors in it become critical concerns.

In 2006, a man identified only as "John Doe" who was HIV+ sued his physician for preparing a report about him that was faxed to Doe's office, where his employer saw it. The report contained information on Doe's diagnosis, symptoms, compliance with his medication regimen and other personal information. According to the lawsuit, the unauthorized disclosure led Doe to experience discrimination at work and caused him to be denied a promotion, leading to anxiety and severe depression.⁶

In addition to personal and professional consequences, there may also be financial consequences of failure to adequately secure personal health information. Hospital records are generally maintained in databases that, if hacked or accessed by unauthorized personnel, could provide sufficient information for someone to use the patient's information for purposes of credit card fraud or identity theft. A number of hospitals have reported hacks of their patient database servers. To date, however, none of the publicized incidents reported in the media have been definitively linked to any

⁵ Kentucky Paramedic Beaten, Fired Following Internet Post. Matt Sanders, *The Paducah Sun*, May 30, 2007. Retrieved from <http://www.emsresponder.com/online/article.jsp?siteSection=1&id=5448>

⁶ Man sues over HIV status disclosure. Eric Collins, *News & Record*, May 24, 2006. Retrieved from: <http://www.news-record.com/apps/pbcs.dll/article?AID=/20060524/NEWSREC0101/605240305>

financial fraud or identity theft. Because cybercriminals may not use information immediately and we may not discover fraudulent use until more than a year or two is passed, press releases that claim that “there is no evidence” that information has been misused may be providing false reassurance to those whose information was exposed or compromised.⁷

In the non-medical sectors, insider misconduct (accidental or intentional) is a primary factor in security incidents leading to financial fraud or identity theft. The same may be true in the medical or health-related sector. Establishing firewalls and encrypting data do not protect against dishonest employees or contractors to whom the employer has given the password and encryption key.

In addition to the potential health-related consequences of failure to secure personal health information and maintain rigorous privacy standards, and in addition to the potential for financial fraud or identity theft, the potential misuse of personally identifiable health poses one additional, but very serious, risk – the risk of medical identity theft.

Medical Identity Theft

In May 2006, the World Privacy Forum (WPF) published its first report on medical identity theft, defined as when “someone uses a person’s name and sometimes other parts of their identity – such as insurance information -- without the person’s knowledge or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods.”⁸

Using data from the Federal Trade Commission’s 2003 survey on identity theft conducted by Synovate,⁹ WPF conservatively estimated that there might be 250,000 – 500,000 victims of medical identity theft as of May 2006.

For calendar years 2004 through 2006, inspection of the Federal Trade Commission’s Sentinel statistics on identity theft indicate that out of 748,530 ID theft complaints over the three-year period, approximately 14,000 were of the “medical” subtype¹⁰; with “medical” currently accounting for 1.9% of all ID theft complaints.

The 1.9% rate is consistent with the 2003 Synovate survey which found that 2% of all respondents who had reported being victims of some type of identity theft within a 5-year period reported that their information had been misused to obtain medical care. Reports

⁷ In July 2007, evidence of misuse of data stolen from Polo Ralph Lauren first emerged – two years after the incident. TJX, Polo Data Surfaces in Credit Card Bust. Evan Schuman, *eWeek*, July 10, 2007. Retrieved from: <http://www.eweek.com/article2/0,1895,2156263,00.asp>

⁸ MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You. World Privacy Forum, May 2006. Retrieved from http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf, June 6, 2007.

⁹ FTC Identity Theft Survey Report, September 2003, Federal Trade Commission. Available at <http://www.consumer.gov/idtheft/pdf/synovatereport.pdf>

¹⁰ Identity Theft Identity Victim Complaint Data Victim Data. Federal Trade Commission Identity Theft Data Clearinghouse. Retrieved from http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf

of misuse of information to obtain government benefits such as Medicaid or Medicare were not included in that category; new account fraud involving medical insurance was also excluded from that category. Applying the 2% rate to the yearly incidence of 9,000,000 cases of identity theft yields an estimate that there are approximately 900,000 victims of medical identity theft in a 5-year period, or approximately 180,000 victims per year.¹¹

As suggested above, medical identity theft may be implicated in some Medicare or Medicaid scams. Some fraudsters recruit patients who sell their information, knowing that it will be used for fraudulent purposes. In other cases, poor, elderly, or disabled patients are lured into schemes with the promise of free treatment, food, or other benefits. If patients knowingly provide their information and know that it is being misused, it would not be considered medical identity theft, but there are many cases where doctors or providers bill fraudulently for services or durable medical equipment never provided, and they use their existing patients' information as part of the scam – without the patients' knowledge or consent. That type of fraud not only creates a false medical and treatment record for the patient, but does constitute medical identity theft, as defined by the WPF. Unfortunately from the perspective of those who want to get a better sense of how prevalent and how costly medical identity theft may be, press releases issued by various prosecutors or federal agencies reporting on the successful prosecution of Medicare and Medicaid fraud generally do not mention how or where the scammers obtained the patient information – whether they purchased it from some source, whether they bought it from the patients, or whether the provider's patients unknowingly had their information used.¹²

As WPF correctly points out, medical identity theft may both limit patients' available benefits and affect their treatment in the future. Medical identity theft may also create a health risk to the patient whose records have been fraudulently doctored to reflect incorrect blood type, diseases, medications, diagnoses, or treatments never received. And unlike "garden variety" credit card fraud or identity theft, medical identity theft victims have no zero-liability protection for medical bills that are incurred by the identity thief in their name. As many hours or weeks or months as it may take to straighten out one's credit record following identity theft, it may be even more time-consuming, costly, and frustrating to correct one's health history or medical records. The false medical record may lead to loss of job opportunities, difficulty in obtaining insurance, and a whole host of problems.

¹¹ Given the size of Synovate's sample and the fact that these were self-reports and not validated, the possibility of overestimation of medical identity theft victims is certainly a possibility, but to date, the Synovate survey provides the only available data, and because their statistic does not include other forms of medical identity theft (to obtain medical insurance, Medicaid fraud, etc.), the 2% rate may turn out to be either accurate or an underestimate.

¹² In one or two cases, this investigator attempted to obtain that information, but was told that because it was not part of the public record, the information could not be released. A number of such cases prosecuted in Florida might contain evidence of medical identity theft. In contrast, a Medicare fraud prosecutor from New York City informed the investigator that stolen patient information was not a common occurrence in the cases they had prosecuted – that the majority of cases involved providers fraudulently billing for services or durable medical equipment not provided to the existing patients or to patients who knowingly gave their information to scammers, lured by the offer of food, free treatment, etc.

A few examples of medical identity theft may help illustrate the scope of problems victims may experience:

- A retired school teacher was contacted by hospital bill collectors who demanded that she pay for the amputation of her right foot. Since she had both her feet, it became clear that someone had used her information to fraudulently obtain medical services in her name. (Menn, J., ID theft infects medical records, *Los Angeles Times*, September 25, 2006)
- Another woman received a call from a Utah state social worker that her hospitalized infant had tested positive for methamphetamine, but the woman hadn't delivered a baby in two years. An investigation determined that a woman had used the victim's stolen driver's license to check into the hospital to give birth. (Menn, J., ID theft infects medical records, *Los Angeles Times*, September 25, 2006)
- A physician was charged with stealing information from the patient files of more than a dozen women who gave birth at hospitals he worked at. He allegedly then used the information to submit fraudulent bills to Medicaid. The women were not his patients, did not have the diagnoses he listed for them on the fraudulent bills, and had never been treated for the false diagnoses. His actions not only resulted in fraud, but created false and inaccurate medical records for his victims. (Carlson, J., Pediatrician accused of \$1M fraud. *The Times*, April 25, 2007)
- Between January 2004 and February 2005, one man used his co-worker's name and drug benefits card on 38 separate occasions to obtain prescriptions for Viagra without the co-worker's knowledge or authorization. The man obtained the co-worker's insurance information by removing the benefit plan card from the co-worker's wallet.¹³
- An employee at Cleveland Clinic in Florida sold patient information on over 1100 patients, including Medicare numbers, to her cousin, who then used the information as part of a scam to bill Medicare for services and equipment never provided. Both the employee and her cousin were charged with HIPAA violations as well as other charges.¹⁴ If any of the over 1100 patients ever do require the treatment or equipment fraudulently billed for, they may discover that the service is denied because their record shows that they have already received it.

Although medical identity theft can certainly pose financial problems for its victims, the most important reasons to protect the privacy and security of health or medical information are not financial. The most important reasons are to promote the confidence

¹³ Attorney General's Insurance Fraud Section charges former SEPTA employee with using co-worker's ID to obtain Viagra. Pennsylvania Attorney General's Office press release, July 2006. Retrieved from <http://www.attorneygeneral.gov/press.aspx?id=1351>

¹⁴ Cleveland Clinic Employee Sold Medicare Information (sic)- Pleads Guilty To Fraud Indictment - US Attorney News, January 11, 2007. Retrieved from <http://lawfuel.com/show-release.asp?ID=10187>.

of patients in their health care providers' and associated entities' ability to protect the privacy and confidentiality of their records, and to protect the health of patients by ensuring that their records are not tampered with or misused.

Has HIPAA Helped?

In April 2003, the federal HIPAA Privacy Rule went into effect. The Privacy Rule does not apply to all health data or medical information. The Rule only applies to what the Rule defines as *protected health information* (PHI) held by those types of facilities or agencies designated as *covered entities*.¹⁵ Thus, information held by a hospital might be PHI whereas the very same information would not be considered PHI if it was held by a non-covered entity. The same situation applies to the HIPAA Security Rule that went into effect in April 2005.¹⁶

HIPAA is not the only federal law addressing the privacy and security of health information. As examples, FERPA protects the privacy of student educational records (including student health information that is part of those records). Additionally, federal agencies are expected to comply with the Privacy Act of 1974 and the E-Government Act of 2002. The Privacy Act of 1974 places limits on agencies' collection, use, and disclosure of information maintained in a system of records. To add to the complex network of privacy regulations, individual states may have their own laws protecting the privacy and security of health information.¹⁷

From the standpoint of the individual, however, it may not matter much which law applies or whether the privacy or security of sensitive personal information has been lost or

¹⁵ The HIPAA Privacy Rule regulates the use and disclosure of "protected health information," which includes any oral or written information related to an individual's past, present, or future physical or mental medical condition, health care treatment, or payment. For the information to be considered "protected," it must either identify an individual or be of a kind that could reasonably lead to the identification of an individual. In general, health care providers (hospitals, physicians, dentists, and pharmacies) that transmit health information electronically are considered "covered entities" and must comply with the HIPAA regulations. Health plans that provide or pay for the cost of medical care are also covered entities. Clearinghouses -- entities that facilitate the flow of personal health information by transforming information submitted in nonstandard form into a standard electronic format -- are also covered entities.

When a covered entity enters into an arrangement with others who will have access to the protected health information, they must contract with the "business associate" to adhere to HIPAA standards and require the business associate to similarly require any of its subcontractors, vendors, or associates to also adhere to the standards.

¹⁶ If a hospital exposes employee records that pertain to the employee's health care or treatment at the hospital, then those records would be covered by HIPAA, but if a hospital's servers are hacked and the database contained only employee personnel records without any of the employee's health records as a patient at the hospital, it would not fall under HIPAA. Similarly, if a non-medical facility self-insures and loses or exposes employee records pertaining to their health care, those records would fall under HIPAA.

¹⁷ Although there is no federal law requiring it, the Department of Defense instituted a policy in 2005 requiring notification to affected individuals within 10 days when protected personal information is lost, stolen, or compromised.

compromised by a covered entity or a non-covered entity. As the Department of Health and Human Services (HHS) itself stated in the introduction to the HIPAA regulations:

No matter how or why a disclosure of personal information is made, the harm to the individual is the same.¹⁸

HIPAA Statistics

Since it went into effect in April 2003, some statistics on HIPAA complaints have been made available. The HHS Office for Civil Rights (OCR) has reported that it received 27,778 complaints through May 31, 2007.¹⁹ HHS said it has resolved 78% of the complaints (21,801) with 5,997 remaining open. Many of the complaints submitted to HHS OCR are dismissed because either the complaint does not constitute a violation of the Privacy Rule or the party is not a covered entity under HIPAA. Of the 7,014 complaints that OCR investigated, 4,732 cases required covered entities to make changes in policies and procedures; while in the other 2,282 cases, OCR determined that no violation had occurred.

According to HHS, the top five reasons for complaints OCR are:

- Impermissible use or disclosure of PHI;
- Lack of adequate safeguards for PHI;
- Refusal to provide access for copy or access to records;
- "Minimum necessary" violations; and
- Failure to get authorization.

A recent GAO report²⁰ analyzed breach reports or incidents where the nature of the data might lend itself to identity theft. Their purpose was to try to determine the extent to which incidents resulted in identity theft and whether it would be appropriate for Congress to incorporate some risk-based criteria in any mandatory disclosure and notification law. As part of their analysis, the GAO asked the American Hospital Association to ask a "nonrepresentative sample" of 78 large hospitals whether they had experienced any breaches of sensitive personal information (excluding medical records) since January 2003. Of the 46 hospitals responding to the query, 13 reported a total of 17 data breach incidents. No additional information about the incidents was provided in the GAO report, and we do not know how many of these large hospitals experienced breaches involving medical records or health information.

When the complaint is in the nature of a Security Rule violation, OCR shares responsibility with Centers for Medicare & Medicaid Services (CMS) for compliance and

¹⁸ Federal Register, Vol. 65, No. 250 / Thursday, December 28, 2000, 82467

¹⁹ Monthly statistics are provided by the [Health Information Privacy/Security Alert](#), Melamedia, LLC

²⁰ PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown. GAO-07-737, retrieved online from <http://www.gao.gov/new.items/d07737.pdf>, July 7, 2007.

investigation. Since April 2003, OCR has referred 171 complaints to CMS. They have also referred 401 cases to the Department of Justice for possible criminal prosecution. Once cases are referred to the DOJ for consideration, OCR does not track what happens after that

Because the federal agencies do not provide detailed statistics as to how many security rule complaints were determined to be founded, how many of them involved large databases that were hacked or stolen, and how many records or individuals were affected by the security rule violations, or how many people may have reported medical identity theft as a result of a privacy rule or security rule breach, we have no numbers to estimate how many patients may have been affected by improper or accidental disclosure of PHI. Other sources of information, however, shed some small light on these questions.

Surveys of HIPAA Compliance Rates

One source of information on HIPAA compliance and violations can be found in the US Healthcare Industry Quarterly HIPAA Survey Results.²¹ Their survey sample represents only a small percentage of those asked to participate in the survey, suggesting that the sample results may not be representative of all providers and payers to whom HIPAA applies, but a comparison of their Summer quarterly reports for 2003 through Summer 2006 suggests that privacy and security are not firmly established among those who are responding to their survey²²:

- For 2003, 77% of respondent providers reported being (mostly) in compliance.
- For 2004, the self-reported compliance rate was 78%²³.
- For 2005 and 2006, the compliance rate remained at 78%.

Based on their sample, approximately 20% or more of covered entities still report that they are not in compliance with the Privacy Rule.

For the Summer 2005 survey, the most commonly reported roadblocks to compliance with the Privacy Rule were: "no public relations or brand problems anticipated with non-compliance" and "no anticipated legal consequences for non-compliance."²⁴

²¹ Quarterly survey results can be found linked from <http://www.hipaadvisory.com/action/surveynew/results.htm>.

²² The number of responses to the survey request seems to have declined each year, which also complicates interpretation of the response data.

²³ For all years, payers reported significantly higher rates of compliance with the Privacy Rule than providers.

²⁴ One frequently raised concern about HIPAA enforcement is that there have been no fines levied for significant breaches and no real prosecution of HIPAA violators. Hence, to the extent that motivation to comply would be boosted by penalties or prosecution, the lack of penalties or prosecution that might serve as an example for others may lead some covered entities to feel that they have nothing to really lose by not complying.

In slight contrast to the US Healthcare Industry's findings of a plateau in provider compliance, a January 2006 survey conducted by the American Health Information Management Association (AHIMA) reported that provider compliance actually decreased in 2006 compared to 2005²⁵. AHIMA reports:

The percentage of healthcare privacy officers and others whose jobs relate to HIPAA privacy who believe their institution is more than 85 percent compliant dropped to 85 percent in 2006, down from 91 percent in 2005. As a result, the percent who believe they are less than 85 percent compliant increased from 9 percent in 2005 to 15 percent in 2006²⁶.

AHIMA's analysis of compliance also differs somewhat from US Healthcare Industry's analysis in terms of reasons given for lack of compliance. Respondents to AHIMA's January 2006 survey listed lack of resources and lack of administrative support as their main challenges to greater compliance.

In addition to asking about compliance with the Privacy Rule, the US Healthcare Industry surveys also inquired about privacy breaches in the first 6 months of each year:

- In 2004, 64% of provider and 58% of payer respondents reported that they had experienced between one and five privacy breaches in the first six months of the year.²⁷
- In 2005, 59% of provider and 45% of payer respondents reported that they had experienced one or more privacy breaches in the first six months of 2005, i.e., there were fewer entities reporting incidents in 2005.
- In 2006, 52% of provider respondents reported privacy breaches in the first six months of the year. As in 2005, providers who reported that they were not in compliance with the Privacy Rule experienced more privacy breaches (64%) than compliant providers.

Taken together, and conceding that neither US Healthcare Industry nor AHIMA are obtaining random samples of covered entities, the preceding data suggest that three years after HIPAA went into effect, what may be a significant percentage of covered entities are still not in compliance with the Privacy Rule, and although there has been a reduction in the percent of providers experiencing privacy breaches, it is possible that over half of compliant providers continue to experience privacy breaches, with a subset experiencing up to 5 or 6 breaches in a 6-month period.

²⁵ From their report, it is clear that their overall compliance figures are higher than those reported by US Healthcare Industry. The differences may be due to differences in the nature of the samples used by both sources. As with the US Healthcare Industry surveys, AHIMA's samples are also likely to be somewhat nonrepresentative of all covered entities.

²⁶ Survey Shows Need for Renewed Focus on Privacy Efforts. AHIMA press release, April 19, 2006. Retrieved from http://www.ahima.org/press/press_releases/06.0419.asp July 10, 2007. The full report, The State of HIPAA Privacy and Security Compliance, April 2006, can be found at http://www.ahima.org/emerging_issues/2006StateofHIPAACompliance.pdf

²⁷ A higher percentage of non-compliant organizations (72% of providers and 80% of payers) reported privacy breaches than compliant organizations.

Turning to compliance with the Security Rule, which went into effect in April 2005, reports from the US Healthcare Industry Quarterly HIPAA Survey indicate less provider compliance with the Security Rule than with the Privacy Rule:

- In 2005, 43% of providers and 74% of payers reported compliance with the Security Rule.
- In 2006, 56% of providers and 80% of payers reported compliance.

Data from AHIMA are again somewhat different in terms of compliance with the Security Rule. AHIMA reports that 25% of January 2006 respondents reported full compliance with the Security Rule while an additional 50% indicated that they were between 85% and 95% compliant. Both surveys, however, agree that there was some progress being made in compliance with the Security Rule from 2005 to 2006. It is important to remember, however, that the implementation dates were not intended as “Now you start coming into compliance,” but rather, represent the date by which all covered entities should have been fully compliant.

When asked about breaches of the Security Rule, the US Healthcare Industry Quarterly HIPAA Survey respondents reported that:

- In 2004 (before compliance was required), 28% of providers and 17% of payers reported that they had experienced one to five data security breaches in the first six months of the year.
- In 2005, 57% of providers and 68% of payers reported no incidents, but 32% of providers and 27% of payers experienced at least one security breach, including an average of 4% of both providers and payers that experienced between six and ten security breaches in the first six months of the year.
- In 2006, 32% of providers experienced between one and five incidents, and another 7% reported six to eleven incidents. Additionally, 29% of payers experienced between one and five security incidents, and another 4% experienced between six and eleven breaches.

These survey results paint a troubling picture. Compliance with the Privacy Rule appears to have plateaued, or worse, declined, and a significant percentage are not in compliance with the Security Rule. If the nonrandom samples are biased towards respondents who seriously care about security and privacy, then the data suggest that there are many breaches occurring on a daily basis around the country, each of which has the potential to harm an individual or many individuals and each of which may be lessening the public’s trust in the health care system to protect privacy, confidentiality, and security of health information.

The AHIMA survey noted that in 2006, 22% of their respondents reported an increase in the number of patients who refused to sign release of information forms. Whether this reflects patient uneasiness about whether providers are really complying with HIPAA and protecting their information or some other factor is unclear, but trust in providers is key in the development of any national network of EHR. A November 2006 survey

conducted by Lake Research Partners and American Viewpoint for the Markle Foundation on attitudes towards EHR found that 80% of the Americans sampled said they are very concerned about identity theft or fraud or the possibility of their information getting into the hands of marketers (77%).²⁸

Although the surveys suggest that there are many breaches occurring on a daily basis that the public never finds out about, neither the HIPAA statistics nor the surveys mentioned above provide us with any information on how many individuals or records are exposed or compromised in breaches of either the Privacy Rule or the Security Rule. The FTC's data are based on non-validated self-reports of problems and we do not have much information as to how often breaches or data loss result in additional harm to the individual due to fraud or identity theft.

Because there are many incidents that are not covered by HIPAA, and because there is no mandatory disclosure law on a federal level or centralized database of incidents involving health-related or patient information, the present study undertook to determine how many cases we do know about where individuals may have had their personal health-related or protected health information exposed, lost, or compromised since April 2003, when HIPAA's Privacy Rule went into effect.

An Analysis of Incidents

Method

The present study primarily relied on available online resources to assess incidence and prevalence of breaches or incidents involving health information or patient information.

Inclusion Criteria

Currently available chronologies or databases compiled by various groups and cited in GAO reports have tended to exclude small-n or individual case reports. Most of these studies are focused on identity theft and incidents that could result in identity theft. In contrast to that approach, the present study's inclusion criteria did not require exposure of SSN or financial data, but did require that the information be either: (1) PHI as defined by HIPAA, (2) student health information that would be protected by FERPA,²⁹ or (3) health-related information that individuals would likely want to be kept private and secure.

Because of its focus on health information or medically related information, the present study specifically excluded hospital, medical center, insurance company, or other

²⁸ Respondents were also very concerned about employers (56%) and health insurers (53%) gaining access to their information. Retrieved from http://www.patientprivacyrights.org/site/DocServer/Markle_survey_dec_2006.pdf?docID=1161

²⁹ HIPAA provisions explicitly exclude health records that are under the protection of FERPA, a federal statute that protects the privacy of educational records.

breaches if the information exposed or compromised consisted only of non-health employee information³⁰.

Sources of Information

Incidents included in the present analyses were obtained from the following sources:

1. Google's news and web search engines were a primary source, using a variety of search strings such as "medical privacy breach," "hospital +security breach," "health privacy breach," "medical data breach," "pharmacy data breach," "stolen laptop +medical," etc.
2. A number of reports included in the analyses were obtained by [Chris Walsh](#) from New York State and North Carolina under their freedom of information laws. The reports obtained by Walsh were particularly helpful for a number of reasons. In a few cases, numbers that were not provided in media reports were provided to the states. In at least one case, a covered entity reported a significantly lower number to the media than was reported to the states. In other cases, health-related incidents were never reported in the media but were reported to the states.
3. Two additional states post mandatory disclosure notices online and some incidents were located via those sites.³¹
4. The World Privacy Forum's May 2006 report³² and the Health Privacy Project's "Health Privacy Stories"³³ also contain descriptions of incidents that were cross-checked against the current listing for post-HIPAA incidents.
5. Some incidents were identified by review of federal reports such as the House Committee on Government Reform's October 2006 report³⁴, as well as a variety

³⁰ The rationale for this exclusion is that HIPAA distinguishes between a covered entity experiencing a privacy or security incident in its role as an employer from its role as a health care entity. So if the "Here's To Your Good Health Hospital" discovered that its employee database was hacked, but there was no health information about the employees in that database, it would not be included in this analysis. On the other hand, if one of the hospital's patient databases was hacked, and the database contained personally identifiable information, then the incident would be included in the current analyses even if there were no diagnostic or treatment records in that database.

³¹ The Wisconsin Office of Privacy Protection maintains a listing at <http://privacy.wi.gov/databreaches/databreaches.jsp> while the New Hampshire Department of Justice Consumer Protection & Antitrust Bureau maintains a listing at <http://doj.nh.gov/consumer/breaches.html>.

³² MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You. World Privacy Forum, May 2006. Retrieved from http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf, June 6, 2007.

³³ Health Privacy Stories. Health Privacy Project, rev 3.5.2007. Retrieved from http://www.healthprivacy.org/usr_doc/Privacystories.pdf June 6, 2007

³⁴ Agency Data Breaches Since January 1, 2003. House Committee on Government Reform staff report. October 13, 2006. Retrieved from: <http://oversight.house.gov/documents/20061013145352-82231.pdf>

- of GAO reports that cited specific breaches that had not been reported in the media.
6. Chronologies or databases provided by the [Privacy Rights Clearinghouse](#) (PRC) the [Identity Theft Resource Center](#) (ITRC), and [Attrition.org](#) were also checked to determine if they had reported any relevant incidents that had not been included in the current analysis³⁵. In a few cases, Attrition.org's archived news stories were used as the documentation for incidents reported in this study as the original sources were no longer freely available online.
 7. Medline (PubMed) was also searched, using keywords "HIPAA," "privacy violation," and "privacy breach." No specific breach incidents were located via this search, however.

Results

A descriptive chronology of incidents for each year is provided in the **Appendix** to this report, with links to the media sources or reports upon which they are based.

Summary Statistics. Table 1 (p. 15) presents a summary of some of the basic findings.

For 2003, only incidents that occurred after HIPAA went into effect on April 14, 2003 are included.³⁶ Data for 2007 are based on incidents which occurred or were reported between January 1, 2007 and July 10, 2007.

The "Resulted in Misuse" column in Table 1 refers to the number of incidents each year where fraud, identity theft, or medical identity theft was reported or confirmed to be a consequence of the incident. The "Number Potentially Affected" column refers to the number of individuals whose records were potentially exposed, lost, or compromised by the situation or incident.

³⁵ Both PRC and ITRC have analyzed some of their data by sector, with "Medical Centers" (PRC) or "Medical/Healthcare" (ITRC) being one of the classifications. Because not all medical center breaches involve PHI or patient data, and because non-medical entities can lose health information, their statistics are not directly comparable to those of the present study. Similarly, using [Etiolated.org](#)'s site to search Attrition.org's database for US incidents involving "MED" data identified (only) 32 incidents affecting 1,506,628 records (not necessarily individuals) since HIPAA went into effect (search date July 11, 2007). Searching the database by "MED" for type of entity and "MED" for type of data breach returned only 24 incidents affecting 1,253,528 records since HIPAA went into effect. Because Attrition.org's stated orientation is to only include large data loss incidents and because they do not provide any definition of what they mean by "MED" and do not appear to be considering some incidents as "MED" breaches that HIPAA would include as PHI, their statistics were expected to represent a significant underestimate of the number and extent of health-related incidents.

³⁶ If pre-HIPAA incidents for that year had been included in analyses, there would be three more incidents affecting another 12,500 known individuals in two incidents plus an unknown number of individuals for a third incident.

Table 1. Number of Incidents of Health- or Patient-Related Data Losses

Year	Incidents	Resulted in Misuse	# Potentially Affected	# Affected
2003	10	1	151,524	Unknown
2004	17	5	2,858,852	3
2005	45	6	914,163	89
2006	131	15	7,625,095	1414
2007	152	28	6,909,121	1084
Totals:	355	55	18,458,755	2,590

As indicated in the actual chronologies in the Appendix, the exact number of individuals potentially affected and/or actually affected are either not known or not revealed for many incidents. Although 355 incidents are included in the current analysis and chronology, only 249 had actual numbers associated with them that could be used in the analysis. Thus, the column in Table 1 reflecting the number of individuals potentially affected and the last column reflecting the number of individuals actually affected should both be considered an underestimate for the current sample.

Inspection of the data in the “Incidents” column of Table 1 suggests that the number of incident reports is increasing each year. Whether this represents an actual increase in the number of privacy or security breaches is unclear, however, as the increased number of reports may simply reflect an increased public interest in breaches and increased media focus on breaches. That said, when we consider: (1) overall estimates of approximately 9,000,000 cases of identity theft each year, (2) an estimated incidence of 180,000 cases of medical identity theft each year, and (3) the US Healthcare Industry’s surveys indicating numerous breaches in a six-month period with some entities experiencing multiple incidents, it is clear that there are many more than 291 incidents for the time period covered by the study and the vast majority of incidents are neither disclosed to the public nor reported by the media.

In light of the above, it seems safe to say that if we know that over 16 million people had their information lost, stolen, or exposed to possible misuse in the 249 incidents for which we have reports, the actual number of people who have had the privacy or security of their health information exposed or compromised may be staggering.^{37 38}

Types of Incidents. Table 2 (p. 17) provides some data on the type of incident or breach by year, expressed as percentage of total incidents for the year. Because of the relatively small amounts of data, some types of incidents were included in a broader category, and more refined analyses may need to wait until more data are available. For purpose of analysis, the following main categories were used:

Employee Conduct. The “Employee” categories include employees of subcontractors, business associates, and others involved in the chain of handling health information. The following broad employee-related categories were used to analyze data:

- **Employee Access (Info):** incidents where employees inappropriately copy, steal, or otherwise obtain patient- or health-related information that may or may not be used for fraud or ID theft. This category also includes employees stealing paper records or equipment or media and then either using it or giving or selling it to others with resulting misuse.
- **Disclosure (Disc):** includes all types of accidental disclosures such as mail errors, faxes gone awry, email errors, and web exposure of information due to human error or web vulnerability. This category also includes intentional (willful) disclosure of personal health information other than cases involving employees obtaining or stealing information for fraudulent purposes and then selling it to others; the latter is included in the **Info** category above.
- **Theft of Information from Employee:** includes incidents when paper records or files (**Thft-P**) or laptops or other electronic devices or media (**Thft-D**) are stolen while in possession or under the control of the employee outside of the main work environment.
- **Extortion (Ext):** threats by employees to expose health information.
- **Improper Disposal (Disp):** The accidental or knowing failure to secure and properly dispose of files or records containing health- or patient-related information by any party with access to the health- or patient information.

Outside Sources. For purposes of analysis, “office” includes the offices of subcontractors, business associates, and any others involved in handling health- or patient-related information. The following “outside” sources of breaches or compromise were used as part of this analysis:

³⁷ Note that we are not talking about the number of identity theft victims, but about the number of people who have had their health- or patient-related information potentially exposed, stolen, or misused.

³⁸ Unlike analyses of data breaches by PRC and others, the numbers reported here are more likely to represent the number of individuals affected as opposed to the number of records affected.

- **Hack:** Unauthorized network intrusion. Incidents identified as “Hacks” in the current analyses may or may not have resulted in health-related information or patient records being accessed or downloaded.
- **Theft:** Two theft categories reflect incidents in which information is stolen from the entity’s office or the office of a subcontractor, business associate, or other party in a hoped-for “chain of trust.”
 - The **(Thft-D)** category reflects incidents involving stolen hardware (laptops, desktops), discs, backup tapes, and/or external drives. This category also includes two incidents of laptops stolen from Red Cross mobile vans, as the vans essentially constitute a mobile office. One incident involving laptop theft from an ambulance, where the laptop was part of the ambulance setup, was also included in this category.
 - The **(Thft-P)** category includes incidents where paper records or files were stolen from the office by a non-employee.

Lost or Missing. The final category includes incidents where health- or patient information is reported as lost or missing from its primary location or office or is lost in transit between locations (**LM-P** for paper files, **LM-D** for hardware or media).

Entries in Table 2 may not sum to 100% for some rows (years) due to rounding and due to omission of cases where there was insufficient information provided to determine the type of incident.

Table 2. Percent of All Reported Incidents by Type of Incident and Year

Year	Employee Sources:						Outside Sources:			LM	
	Info	Disc	Thft-P	Thft-D	Disp	Ext	Hack	Thft-P	Thft-D	P	D
2003	10	40	0	0	10	20	10	0	10	0	0
2004	25	25	0	13	6	0	13	0	13	0	0
2005	13	16	0	11	7	0	0	2	36	2	4
2006	14	15	3	19	12	1	4	0	27	0	4
2007	21	19	3	7	22	0	3	3	11	<1	8

For 2006: 13 out of 18 (72%) of Emp-Info incidents resulted in misuse of data.

For 2007: 25 out of 32 (78%) of Emp-Info incidents resulted in misuse of data.

Inspection of Table 2 suggests that over time, hacks have constituted a smaller percentage of all reported incidents, while incidents involving theft of equipment or media accounted for almost half of all incidents in 2005 and 2006. The fact that hacks have decreased proportionally, however, does not mean that hacks have actually decreased. For this small sample, there were more hacks in 2006 than in 2003, 2004, and 2005 combined.

Drawing any inferences about trend is plagued by confounds, not the least of which is media bias in reporting certain types of news stories – or even going hunting to create news stories (e.g., “dumpster diving” investigations). Similarly, one or two “huge” incidents (such as the theft at Concentra Preferred Systems and Electronic Registry Systems offices in 2006) can inflate a particular category for one year³⁹.

Highlighted cells in Table 2 represent conditions associated with misuse of data for purposes of fraud or identity theft. As indicated in Table 1, 55 out of the 3541 incidents, or 16%, reported fraud or identity theft as consequences. The 12% rate appears somewhat higher than similar rates reported in the business sector, but the difference may be an artifact of the present study including smaller incidents that are reported in the media precisely because they did result in identity theft or fraud.

Inspection of the highlighted entries in Table 2 suggests that employee access to, and misuse of information may be the most consistent risk to the privacy and security of health- or patient-related information, a finding that is comparable to analysis of incidents in the business sector.

The 36 incidents of known or verified misuse of information were subsequently analyzed to determine the relative frequency of each type of source. Of the 36 incidents:

- 27 involved dishonest employees who stole information and either used it for credit card fraud, new account fraud, or in 3 cases, medical identity theft. Of those 27 incidents:
 - 19 employees and 3 employees of contractors used the information themselves,
 - 5 employees gave or sold stolen information to others who used the data for fraudulent purposes, including medical identity theft.
- 9 remaining incidents included:
 - 1 incident involving a laptop stolen from the trunk of an employee’s car,
 - 1 incident of misuse resulting from intentional disclosure of information on the web of by a county clerk,
 - 1 incident involving theft of paper records from a hospital nursing station, and

³⁹ Even though the Concerta Preferred Systems and Electronic Registry Systems incidents have not been reported to have resulted in any misuse by the time of this report, it is clear that failure to encrypt data needlessly increases the risk that health information of millions of Americans may be misused.

- reports of medical identity theft where the theft was either by an acquaintance (1 case), an employee of a nonmedical business (1 case), or of unknown or unreported origin.

Several cases of medical identity theft involved multiple victims. Two of those cases involved employees stealing patient information and using it to obtain prescription drugs. The third case, and perhaps the most publicized case, involved an employee at Cleveland Clinic in Florida who sold information to her cousin or others, who then used it as part of a fraud scam. That incident resulted in 1,130 cases of medical identity theft.⁴⁰

The Cleveland Clinic incident is typical of the type of problem reported in California in 2005 where employees of medical facilities sold patient information to unscrupulous providers who then filed fraudulent Medi-Cal and Medicare claims totaling millions of dollars⁴¹. In recent years, Florida has also seen more Medicare and Medicaid fraud of this kind. Recent press releases from the U.S. Attorney's Office in Florida attest to the concerted effort to address the massive ongoing theft⁴².

Entities Experiencing Multiple Incidents. A number of the entities who experienced breaches experienced more than one incident. As but a few examples:

- The University of California system was involved in 6 incidents that were reported in the media during this time period, while the University of Pittsburgh Medical Center had 5 incidents;
- Los Angeles County and Palm Beach County in Florida each reportedly had 4 incidents;
- Kaiser Permanente had 1 incident of web exposure (for which they were fined \$200,000), 1 incident of employee theft and misuse of data, and 3 incidents of stolen laptops; and
- The Department of Veterans Affairs had 8 incidents involving health information during this time period, the most for any entity.

Discussion

Unlike chronologies or databases that were used by the GAO for its recent analysis, the present study incorporated small-n reports and individual reports. A comparison of the database for this study against other databases indicates that for each year of the study, approximately 50% of the incidents in this chronology are not included in their databases. Significantly, many of the cases of ID theft or medical identity theft reported

⁴⁰ U.S. Attorney's Office, Southern Florida – Press Release: Two Defendants Sentenced in Health Care Fraud, HIPAA, and Identity Theft Conspiracy, May 3, 2007. <http://www.usdoj.gov/usao/fls/PressReleases/070503-01.html>

⁴¹ "Medi-Cal Fraud Flourishing on Black Market," Jason Kandel, *Los Angeles Daily News*, August 7, 2005.

⁴² cf, <http://www.usdoj.gov/usao/fls/PressReleases/070525-01.html>

in this study are associated with the incidents that are not included in the other databases. For example, for 2006, the present study identified 131 incidents; 58 of which were not on Attrition.org's list. Those 58 incidents include 10 of the 14 incidents known to have resulted in fraud or ID theft that year. Similarly, for the first part of 2007, Attrition.org's site lists 177 incidents in its archives. This study located 90 incidents; at last 46 of these do not appear on Attrition's list, including 9 out of the 11 incidents known to have resulted in fraud or ID theft⁴³.

It should be clear from the preceding that databases or chronologies which emphasize large data loss incidents may not be appropriate or helpful if we want to get a better sense of rates of fraud and misuse of data stemming from incidents involving health information.

The present study, preliminary in nature, can only suggest trends at best, as it cannot be viewed as a random sample of all incidents for the time period, it does not include most large Medicare or Medicaid scams that may result in numerous cases of medical identity theft, it does not include most large incidents involving HHS/CMS or defense contractors resulting from failure to properly secure access controls and encrypt data during transmission, and it does not include incidents that were reported to over 30 states under mandatory disclosure laws. As but two examples of how much information is not publicly available:

- The HHS reported that it had 24 breaches or incidents between January 2003 and October 2006⁴⁴, but the public does not know the details of 20 of those incidents or how many resulted in additional demonstrable adverse consequences to individuals. Indeed, we would not even know that those incidents had occurred but for a Congressional inquiry and public disclosure of agency responses.
- A 2006 GAO report⁴⁵ noted that over 40% of the federal contractors and state Medicaid agencies responding to their survey reported that they experienced a privacy breach involving personal health information during the 2-year period of the survey. By survey group, 47% of Medicare Advantage contractors reported privacy breaches, as did 44% of Medicaid agencies, 42% of Medicare fee-for-service (FFS) contractors, and 38% of TRICARE contractors. The GAO did not obtain reports on the frequency or severity of breaches, and their report does not include any specific incidents⁴⁶.

⁴³ This is not a criticism of Attrition.org. Their focus and scope is different than that of the present study. The point in comparing the current sample to their sample was to determine if existing chronologies would be useful for analyzing incidents involving health information.

⁴⁴ Email correspondence to the House Committee on Government Reform, 2006.

⁴⁵ PRIVACY: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE. GAO-06-676, June 2006 Retrieved online from:
<http://www.gao.gov/new.items/d06897t.pdf>

⁴⁶ An incident involving defense contractor SAIC reported after July 10, 2007 and not included in the current figures reportedly exposed 580,000 – 900,000 beneficiaries' health claims information when data were transmitted without encryption; the unencrypted data also included names and Social Security numbers and health information. It is easy to see how the total number of

The Need for Transparency and Accountability

Information about the frequency, severity, and consequences of health information privacy or security breaches is currently scattered across a variety of federal, state, and private sector entities or agencies. In what appears to be a case of “Don’t ask, don’t tell,” Congress has yet to ask and demand answers to questions such as:

1. How many privacy and security breaches of health information are there each year? How many of them have involved paper records and how many of them have involved electronic data?
2. How many individuals have had their sensitive health information lost, stolen, or compromised?
3. How many incidents have resulted in medical identity theft and how many victims are there?
4. What factor(s) predict(s) whether lost, stolen or exposed information will result in fraud, identity theft, or medical identity theft?
5. What are the consequences of these incidents to the individuals in terms of financial costs, time, worry, job discrimination, or medical identity theft?
6. Is the situation getting better over time, or is it actually getting worse?

Somewhat worryingly, a recent GAO report analyzing nonmedical breaches and their relationship to identity theft⁴⁷ suggested that it would be appropriate for Congress to consider enacting mandatory disclosure and notification requirements using risk-based criteria. A recent report that information from the Polo Ralph Lauren incident in 2005 was first being misused appeared⁴⁸ after their report was published, but points out the dangers in both using risk-based criteria where the risk is calculated by the entity experiencing the breach and in assuming that if data have not been misused shortly after the incident, they will not be misused.

The GAO’s recommendations also fail to give sufficient weight to the fact that many of the very incidents that would now fall under any such federal legislation and criteria often contain aspects of patient or health information and that individuals have a need to know and right to know when the privacy and security of their health information have been compromised.

If Congress wants the American public to trust a networked health system, it needs to stop treating the public like children by deciding what we need and do not need to know. When our data are lost, stolen, or exposed, we need to be told so that we can decide whether to continue to trust providers or insurance companies. We need to know who is in possession of our health information and we need to know that every element in any

individuals whose health information has been lost, stolen, or exposed could easily totally in the tens of millions very quickly.

⁴⁷ PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown. GAO-07-737, June 2007. Retrieved from <http://www.gao.gov/new.items/d07737.pdf>.

⁴⁸ Schuman, E. TJX, Polo Data Surfaces in Credit Card Bust. *eWeek*, July 10, 2007. Retrieved from <http://www.eweek.com/article2/0,1895,2156263,00.asp>

chain of transmission or handling is secure. We need to know that we can control who has access to our information, and that there are mechanisms in place to correct errors in our records.

When we cannot determine what, if any, relationship exists between incidents and particular types of consequences, and when we cannot determine what, if any, costs are associated with adverse consequences, we need more data and more transparency, not less. The GAO's endorsement of risk-based criteria would be a financial relief to businesses and entities who may incur costs for notification and disclosure, but it does not serve the public well and would only complicate any attempts to identify rates and risks.

Recommendations

1. Congress should authorize and fund a 3-year study where all incidents of privacy or security breaches of health information or patient information are reported to one agency for compilation and analysis. The Department of Justice survey that is scheduled for next year should be reviewed to determine if the wording of the questions will adequately permit assessment of the nature of health-related information incidents, their severity, frequency, and consequences.
2. Anonymized privacy and security breach incidents that involved personally identifiable health information should be made available on a publicly available web site to permit the public, patient advocacy organizations, researchers, and interested parties access to data.
3. Congress should enact legislation that closes the gaps in the existing network of laws and that requires any entity in possession of personally identifiable health-related information to comply with uniform privacy and security standards, allowing states to set higher minimal standards. Commercial data miners or resellers should be barred from obtaining or retaining health-related information without the express opt-in informed consent of the individual or their guardian.
4. Congress should hold hearings and require all federal agencies, cabinet departments, representatives of the health insurance industry, and state Medicaid agencies to provide statistics on the number of relevant incidents since April 2003 and their severity and consequences.

Summary

Americans have repeatedly demonstrated their concern for the privacy, confidentiality, and security of their health information. Four years after the HIPAA Privacy Rule went into effect and two years after the HIPAA security rule went into effect, the privacy and security of health information continues to be at risk. To date, the government has provided no meaningful statistics and most statistics have come from nonprofit or volunteer organizations who have tried to raise public awareness about the extent of problems. Previous research suggests that there may be 180,000 new cases of medical identity theft each year. The present study suggests that if 16,000,000 Americans are known to have had their health information or patient records exposed or compromised in the past four years, the true number is likely to be well over 100,000,000, and even that may be a conservative estimate.

It is time for Congress to get serious about protecting the privacy and security of health information. Americans' trust in health care systems and their providers depends on it. A person's financial status can be restored, but there is no taking back sensitive health information once it is "in the wild."

The time has come for a public debate that is informed by actual data and facts. To do that, we need greater transparency.

For More Information:

The PDF version of this report is located at
http://www.pogowasright.org/MedicalPrivacy_2007.pdf

Updates to this report and to the data chronologies that constitute the Appendix to this report will be found on PogoWasRight.org's [Medical Privacy Project](#) page.

For questions about this report, or to report errors or other incidents for subsequent inclusion in updates, contact:

PogoWasRight.org
www.pogowasright.org
admin@pogowasright.org

Acknowledgements:

The author gratefully acknowledges the assistance of Joanna Crane, Program Manager of the Federal Trade Commission ID Theft Program for her help in providing additional clarification on the 2003 FTC report and Chris Walsh for his volunteer efforts to obtain and share incident reports under FOIA from New York and North Carolina. All errors are solely the author's, however.

Disclosure:

The author of the report is a licensed health care professional who is not affiliated with any pharmaceutical company, insurance carrier, or any other entities that might pose a conflict of interest.

PogoWasRight.org is a nonpartisan site that accepts no advertising or commercial sponsorship and is a purely volunteer effort.