

# Identity Theft and Security of Health Information Are Related

By Peter MacKoul, Esq.  
HIPAA Solutions, LC

The Health Insurance Portability and Accountability Act (HIPAA) addresses the need for privacy and security of an individual's personal health information.

Wide spread abuse involved in the use of such information has caused damage to careers, family relationships and financial situations in the past. In addition, identity theft crimes using stolen data is a growing problem and some of it comes from health data sources. Information released from the Justice Department's National Crime Victimization Survey on identity theft revealed it impacts over 3.6 million families a year and costs an estimated \$6.4 billion annually.<sup>1</sup>

The HIPAA Security rule is designed to protect "personal health information" or PHI by requiring that "covered entities" secure networks and databases to ensure the confidentiality and privacy of this information. The criminal enforcement of HIPAA violations related to this rule can reduce the intentional misuse or the "wrongful disclosure" of PHI.

Electronic PHI stored in medical databases consists of insurance information, social security numbers and bank account or credit card numbers, along with past and present medical conditions and treatments. "Covered Entities" include physicians, hospitals, schools and universities and also include local government entities, i.e., cities or counties that provide health insurance or health services.

HIPAA enforcement in the form of fines and jail time would provide an incentive to covered entities to actively prevent security breaches. Since medical databases often contain a great deal of sensitive information, they are a logical choice for identity theft by hackers and thieves.

A recent Computerworld article stated, "...these covered entities are appealing targets for identity theft, the fastest-growing crime in the U.S. today. While not as obvious or attractive a target as financial services or e-commerce companies, these covered entities represent a significant opportunity for enterprising thieves, by virtue of the data that they process and store."<sup>2</sup>

---

<sup>1</sup> <http://www.pcworld.com/news/article/0,aid,125291,00.asp>

<sup>2</sup> <http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,82051,00.html>

But, often entities and individuals responsible for the security of information have a casual or insensitive approach to the information they possess. The response of a physician, related to data stolen from him, quoted in an April 16, 2006 Computerworld article was revealing.

After the physician's laptop containing a database of medical information was stolen, his response was ". . . well, I don't see what the fuss is about. I'm the primary caretaker for my patients, and ultimately the data is mine. If I decide to disclose the information, that's my prerogative because those people have put their trust in me. I have the authority over medical information because I am the medical authority."<sup>3</sup>

A 2005 CBS news report discussed "what the fuss was all about" in a report entitled "An Identity Theft Nightmare."<sup>4</sup>

After four years of trying to clear his name, including letters from the Justice Department confirming he was a victim of identity theft, John Harrison was still being harassed by creditors for nearly \$140,000 dollars in debt that resulted from identity theft. In today's environment, this is not an uncommon occurrence.

A short chronological listing of major security breaches shows how common data theft has become and the broad scope of these breaches across many entities that are covered under the HIPAA regulations.<sup>5</sup>

<b>DATE</b>	<b>ORGANIZATION</b>	<b>INCIDENT</b>	<b>INDIVIDUALS AFFECTED</b>
March 11, 2005	Univ. of CA, Berkeley	Stolen laptop	98,400
March 11, 2005	Boston College	Hacking	120,000
April 8, 2005	San Jose Medical Group	Stolen Computer	185,000
April 15, 2005	Calf. Dept. of Health Services	Stolen laptop	21,600
April 26, 2005	Christus St. Joseph's Hospital Houston, TX	Stolen laptop	19,000
May 7, 2005	Dept. of Justice	Stolen laptop	80,000

<sup>3</sup> <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110446>

<sup>4</sup> <http://www.cbsnews.com/stories/2005/02/25/eveningnews/consumer/main676597.shtml>

<sup>5</sup> <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Aug. 27, 2005	Univ. of Florida, Health Sciences Center/ChartOne	Stolen laptop	3,851
Sept. 19, 2005	Children's Health Council, San Jose CA	Stolen laptop	5-6,000
Oct. 12, 2005	Ohio State Univ. Medical Center	Online exposure	2,800
Oct. 21, 2005	Wilcox Memorial Hospital, Hawaii	Lost backup tape	130,000
Nov. 1, 2005	Univ. of Tenn. Medical Center	Stolen laptop	3,800
Nov. 4, 2005	Keck School of Medicine, USC	Stolen laptop	50,000
Dec. 1, 2005	Univ. of San Diego	Hacking	7,800
Dec. 25, 2005	Iowa State Univ.	Hacking	5,500
Jan. 25, 2006	Providence Home Services, Oregon	Stolen Backup Tapes	365,000
Feb. 1, 2006	Blue Cross and Blue Shield of North Carolina,	Inadvertent exposure of information	600
Feb. 16, 2006	Blue Cross and Blue Shield of Florida	Contractor Error	27,000
Feb. 17, 2006	Mount St. Mary's Hospital, Lewiston NY	Stolen laptops	17,000
Mar. 1, 2006	Medco Health Solutions	Stolen laptops	4,600
April 24, 2006	University of Texas' McCombs School of Business	Hacking	197,000
April 26, 2006	Aetna	Stolen laptop	38,000
May 11, 2006	Ohio University Hudson Health Center	Improper Access to PHI	60,000

While two criminal prosecutions for HIPAA have been completed to date, as of August 2005, the Office of Civil Rights, (the federal entity responsible for HIPAA enforcement), has referred over 231 cases to the Department of Justice for criminal investigation.<sup>6</sup>

---

<sup>6</sup> <http://www.hipaadvisory.com/news/NewsArchives/2005/sep05.htm>

That should be a wake up call to those handling PHI that more aggressive enforcement is on the way.

If an individual believes their personal health information has been misused, they can file a complaint with the Federal Department of Health and Human Services using a form located at the following site.

<http://www.hhs.gov/ocr/privacyhowtofile.htm>

Peter MacKoul is an attorney and consultant with a background of over 15 years of legal and technical consulting for both corporate and governmental entities. His expertise includes the areas of HIPAA, Information Technology, Internet law, handicapped access to technology and healthcare issues that involve law, technology, privacy, and security. He currently serves on the State of Texas Health Information Technology Advisory Board.

<sup>6</sup> <http://www.hipaadvisory.com/news/NewsArchives/2005/sep05.htm>