Mitigating Medical Identity Theft

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

Medical identity theft accounts for 3 percent of identity theft crimes, or 249,000 of the estimated 8.3 million people who had their identities stolen in 2005, according to the Federal Trade Commission.[1] But what exactly is medical identity theft and why does the World Privacy Forum say it is the most difficult of identity theft crimes to correct?

This practice brief explores medical identity theft, its ramifications, and how HIM professionals and others can work together to prevent, investigate, and mitigate the damages it causes.

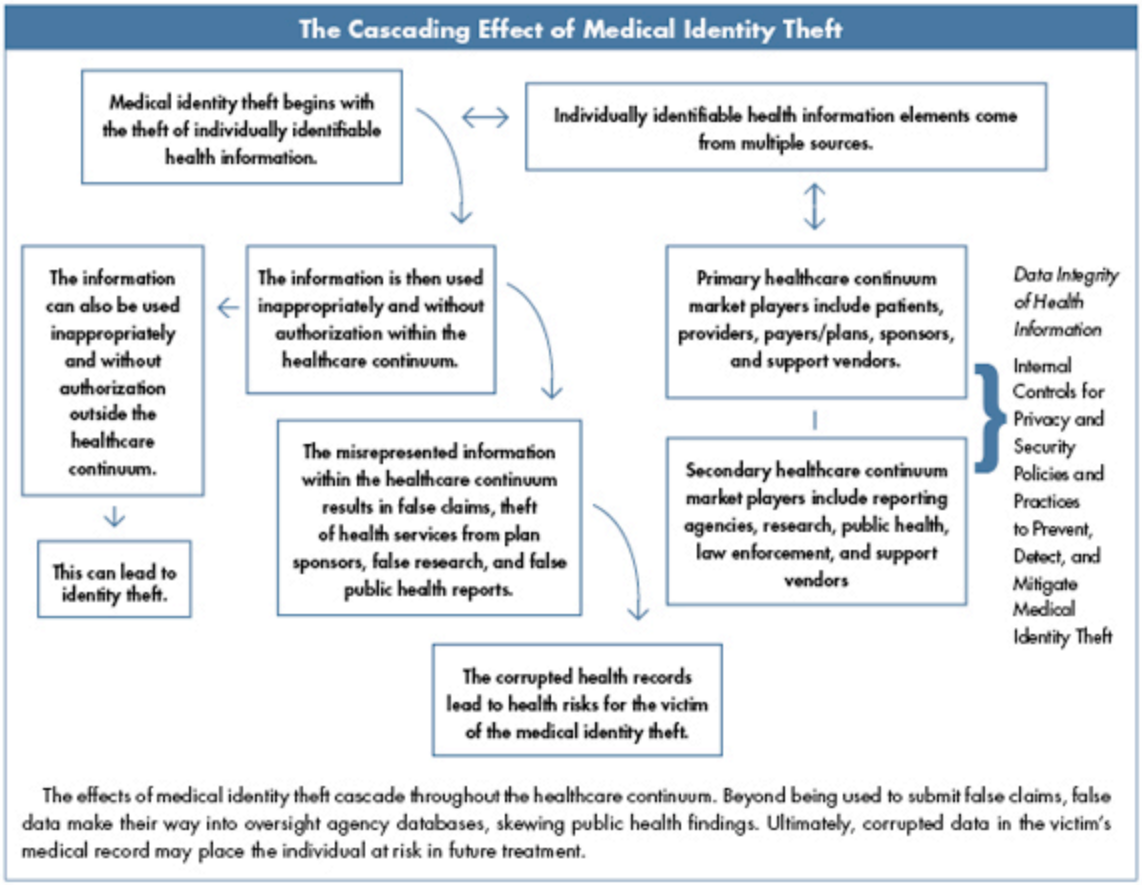
Defining Medical Identity Theft

Medical identity theft is the inappropriate or unauthorized misrepresentation of individually identifiable health information for the purpose of obtaining access to property or services, which may result in long-lasting harm to an individual interacting with the healthcare continuum.[2] It "frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[3]

Examples of medical identity theft include situations wherein an individual accesses medical services in another individual's name to:

- Obtain benefits or services for which the individual is not eligible
- Obtain services for which the individual will not pay
- Perpetrate other fraud or illegal activity (such as erroneous billings or drug-seeking behavior for personal use or illegal distribution)

"The Cascading Effect of Medical Identity Theft," [below], demonstrates how medical identity theft affects an individual and his or her healthcare from the initial theft to corrupted health records.



The effects of medical identity theft cascade throughout the healthcare continuum. Beyond being used to submit false claims, false data make their way into oversight agency databases, skewing public health findings. Ultimately, corrupted data in the victim's medical record may place the individual at risk in future treatment.

The Victims and the Implications

Medical identity theft is a lucrative form of identity theft. A stolen Social Security number has an estimated street value of $1 per identity; the price of stolen medical identity information averages a much higher street value, at an average of $50 per identity.[4]

The primary victim of medical identity theft is usually an individual—a patient, potential patient, health plan member, or healthcare consumer. Individuals who are particularly vulnerable include those with developmental or intellectual disabilities, minors, newborns, the elderly, and persons whose information may be included on public registries (e.g., cancer registry). Thieves often target the recently deceased.

Secondary victims include, but are not limited to, parties who generate, manage, use, or transfer individually identifiable health information. Examples include healthcare providers, health plans, and society as a whole.

Individuals

There have been numerous cases where individuals have been the primary victims of medical identity theft. In one case, an individual received a $44,000 bill for a surgery he never had.[5] In a second case, a victim was told her children would be taken away from her because her newborn baby tested positive for methamphetamines. The victim hadn't recently delivered a baby. In yet a third case, a victim was almost arrested when she went to a pharmacy to have a prescription filled and a well-meaning clerk noticed the identity theft flag on her records and called the police.[6]

Medical identity theft can be difficult to discover. An individual may have no idea he or she is a victim of a crime as it often remains hidden in complex payment systems, databases, and medical records. Unfortunately it may not be detected until much later, when a victim has some reason to scrutinize his or her records and discovers information that does not belong.

Individuals who report medical identity theft to the police may find it treated as a property crime and not a high priority for limited law enforcement resources. Some victims may even find themselves having to convince police they are indeed victims

and not the offenders responsible for the crime.

One victim hired an attorney to sort out the damage to her records. She avoided the hospital where the identity thief was treated, because of the inaccuracies in her health record as a result of the medical identity theft. Eventually, she was seen in a different hospital. Unfortunately, the inaccurate records of the thief's diagnosis and treatment had circulated and intermingled with her own records, causing her concerns about her healthcare because she has a serious blood-clotting disorder and the wrong medication could be life-threatening.[7]

There is no single place individuals can go to locate and correct inaccurate medical information. Individuals must identify all parties who received incorrect health information in their name and convince the custodians of such information to correct the information. This may prove challenging as the custodian may not allow access to information that has been identified as belonging to the identity thief and not the victim. Until such time as all records are corrected, medical identity theft victims may receive incorrect or even deadly treatment.

Providers and Plans

Healthcare providers and health plans may be secondary victims of medical identity theft. A provider who incorrectly bills the victim of identity theft may find it necessary to write off all its healthcare expenses related to treatment of the identity thief. In addition, the provider may experience difficulty in rescinding claims that were made prior to the determination of the theft. Both the provider and the plan may also incur significant expense as they work with the victim to correct records and mitigate further risk.

A provider or plan that is unaware of the identity theft may disclose inaccurate information to others or render or sponsor services to the individual that are inappropriate to that individual. Common law is not yet clear on legal actions that can be taken against a provider or plan related to negligence, malpractice, or other legal action.

Providers may unknowingly submit incorrect precertification or claims and accompanying health information to health plans to justify treatment or payment for the health services rendered. The health plan may preapprove and pay the claim and apply the amount paid against the individual's annual or lifetime benefit allowance.

In addition, the health plan may maintain the inaccurate information in its database and may share the information with the MIB Group, Inc. This corporation, owned by insurance companies, maintains a database for members to exchange confidential information about individuals who apply for health and other types of insurance benefits.

Additionally, until such time as all third-party payer records are corrected, victims could be denied payment for health services rendered or be denied additional health, disability, or life insurance coverage should it be sought.

Healthcare providers and health plans may suffer permanent damage to their reputations, which may result in irreversible business consequences.

Society

The impact of medical identity theft on society is significant as well. Private-pay patients may find themselves paying more to healthcare providers to offset write-offs for medical identity theft. Purchasers of insurance may see increased rates to offset losses insurance companies may incur. Tax payers may pay additional taxes for government-provided benefits to offset the cost of undiscovered or unrecovered claims.

Tax payers also pay for increased federal and state law enforcement services to cover investigation, prosecution, incarceration, and enforcement with regard to medical identity theft. Tax payers might even be subsidizing drug-seeking behaviors when the stolen identification is used to obtain narcotics and pain-killers under false pretenses.

Preventing and Detecting Medical Identity Theft

The prevention and detection of medical identity theft requires diligent monitoring and appropriate response. Responses may include a variety of administrative, technical, or physical safeguards. HIM professionals (as well as privacy and security

officers and other organizational leaders), individuals, healthcare organizations, health plans, and other stakeholders who may be affected must work in cooperation to establish prevention and detection programs.

The first line of defense may well rest with the individual. Individuals are encouraged to practice the same preventive measures for medical identity theft as they would for financial identity theft. Common preventive measures include:

- Sharing personal and health insurance information only with trusted providers.
- Monitoring the explanation of benefits received from insurers and obtaining a summary each year of all the benefits paid in the patient's or guarantor's name.
- Contacting the insurer and provider about charges for care that was not received, even when there is no money owed.
- Maintaining copies of healthcare records.
- Checking personal credit history for medical liens.
- Demanding that providers and insurance companies correct errors or append and amend medical records to alert a user to inappropriate content.
- Questioning "free" medical services or treatments (sometimes illicit entities use the lure of "free" services to obtain names and insurance information for use in fraudulent claim submissions). Individuals should always question what is being offered and who is paying the cost. If not satisfied with the answers, they should decline the offer.
- Protecting health insurance information. Individuals should safeguard insurance cards, explanation of benefits, and health plan correspondence in the same way they would safeguard credit cards.
- Refusing to provide insurance numbers to telephone marketers or door-to-door solicitors.[8,9]

In addition, AHIMA recommends obtaining and maintaining personal health records that include copies of significant health information from each healthcare provider.

IT research and consulting company Gartner, Inc., offers health insurers the following recommendations to mitigate risk of medical identity theft:

- Empower consumers to avoid being victimized. Incorporate specialized consumer education on Web sites or direct mail. Educate consumers to closely monitor their explanations of benefits and treat their insurance cards as securely as their credit cards.
- Provide more frequent summaries of services to allow consumers more proactive viewing of their past treatments to identify early signs of fraud.
- Educate providers about medical identity theft and encourage them to ask for a photo identification before treating patients.
- Make benefit cards more secure by incorporating the member's photo directly on the ID card.
- Deploy pattern-recognition technology. By integrating a variety of data sources, payers can compare analyses of customary claims experience and repeatable fraudulent patterns against current claims information.
- Address security gaps for all health information exchanges before trust erodes.
- Institute sophisticated security monitoring measures and implement a broadly accepted, executive-supported information security charter for effective security policy and governance.[10]

A risk analysis is the foundation of any sound privacy and security program for a healthcare provider or health plan; it is also a requirement of the HIPAA security rule. From the perspective of medical identity theft prevention, the risk analysis process is an appropriate method of identifying threats and vulnerabilities to medical information and determining if existing privacy and security controls are sufficient to prevent medical identity theft.

A proper risk analysis includes:

- Asset inventory and prioritization
- Threat and vulnerability identification
- Examination of existing security controls associated with addressing identified threats and vulnerabilities
- Determining the likelihood of exposure to identified threats and vulnerabilities
- Determining the impact (fiscal, workflow, etc.) associated with the exercise of a threat or vulnerability exploitation
- Determining, prioritizing, and mitigating identified risks

The risk analysis should address three areas clearly articulated in the HIPAA security rule: administrative, physical, and technical safeguards. It should be noted that the primary cause of security breaches is related to the people or business side of an organization's operations. The most extensive section on safeguards in the HIPAA security rule does not focus on technology. It focuses on administration.

HIM professionals can guide their organizations in establishing the following measures to prevent and detect medical identity theft:

- Ensure appropriate background checks of employees and business associates, both prior to hiring and in high-risk areas, as well as periodically after hiring. Consider minimizing the use of noncredentialed or nonlicensed individuals in temporary positions if they are not bound by professional codes of conduct or ethics.
- Establish patient verification processes that may include obtaining and storing photo IDs or other means of identity verification or authentication if utilizing e-mail or Internet access. Make sure that the initial process is thorough, as determinations will be relied upon by subsequent users. The entire verification process and any data collected must be protected in accordance with the HIPAA security rule.
- Minimize the use of Social Security numbers for identification. Avoid displaying the number on any document, screen, or data collection field. Where possible the entire Social Security number should be suppressed, and where it is absolutely necessary only the last four or six digits should be visible.
- Store individually identifiable health information in a secure manner and ensure that administrative, technical, and physical safeguards are in place, such as restricted access and locks.
- Consider securing a release of liability to cover the entity against possible claims by any individual who may choose not to use the secure storage provided.
- Implement and comply with organizational policies for the appropriate disposal, destruction, and reuse of any media used to collect and store individually identifiable health information.
- Implement and comply with organizational policies and procedures that provide safeguards to ensure the security and privacy of individually identifiable health information collected, maintained, and transmitted electronically:
    - Limit access to electronic individually identifiable health information to a minimum necessary basis.
    - Establish minimum necessary access controls.
    - Require unique user identification and password controls.
    - Implement encryption practices for transmitting individually identifiable health information.
    - Install appropriate hardware and software protective mechanisms such as firewalls and protected networks.
    - Audit routinely to determine appropriate access to information, including access to individually identifiable health information by staff with a newly assigned user ID.
    - Eliminate open network jacks in unsecured areas that could provide unauthorized access.
- Create an "alert" process for medical records where identity verification may be required upon patient admission.
- Develop a proactive identity theft response plan or policy that clearly outlines the response process:
    - Identify current and evolving federal and state laws applicable to identity theft, reporting, and disclosure.
    - Complete a preemption analysis addressing HIPAA's permitted disclosures to law enforcement (§164.512(2)(5)) versus state law, determining when there is a need for court order, subpoena, or patient authorization.[11]
    - Identify the organization's obligations to report or disclose to law enforcement or government agencies information related to medical identity theft.
- Develop ongoing staff training programs to ensure work force understanding of organizational policies and practices developed to provide protection and appropriate use and disclosure of individually identifiable health information.

Medical Identity Theft Response Checklist for Consumers

Consumer awareness is critical for timely detection of and thorough response to a medical identity theft incident. Consumers may follow this checklist for proactive guidance and quick action.
[printable version of checklist]

Task	√ When Complete
1. Explore the resource "Tools for Victims" provided by the Federal Trade Commission (available online at www.ftc.gov/bcp/edu/microsites/idtheft/tools.html). Consider completing the universal affidavit to submit to creditors.	
2. Review credit reports, correct them, and place a "Fraud Alert" on them.	
3. If a Social Security number is suspected of being used inappropriately, contact the Social Security Administration's fraud hotline at (800) 269-0721.	
4. In the case of stolen or misdirected mail, contact the US Postal Service at (800) 275-8777 to obtain the number of the local US Postal Inspector.	
5. For stolen passports, contact the US Department of State at (877) 487-2778 or http://travel.state.gov.	
6. If the thief has stolen checks, contact both check verification companies: Telecheck ([800] 366-2425) and the international Check Services Company ([800] 526-5380) to place a fraud alert on the account to ensure that counterfeit checks will be refused.	
7. Contact the health information manager or the privacy officer at the provider organization or the antifraud hotline at the health plan where the medical identity theft appears to have occurred.	
8. Request an accounting of disclosures. If the provider or plan refuses access to medical records, file a complaint with the Office for Civil Rights at Health and Human Services at (866) 627-7748 or www.hhs.gov/ocr/privacyhowtofile.htm.	
9. Take detailed notes of all conversations related to the medical identity theft. Write down the date, name, and contact information of everyone contacted, as well as the content of the conversation.	
10. Make copies of any letters, reports, documents, and e-mail sent or received regarding the identity theft.	
11. Work with the organization where the medical identity theft occurred to stop the flow of the incorrect information, correct the existing inaccurate health record entries, and determine where incorrect information was sent.	
12. File a police report and send copies with correct information to insurers, providers, and credit bureaus once the identity theft has been confirmed.	
13. File a complaint with the attorney general in the state where the identity theft occurred. The National Association of Attorneys General provides state-by-state information at www.naag.org/attorneys_general.php.	
14. Check with state authorities for resources. Many states provide consumer protection and education related to insurance and accept online complaints. To determine if a state has a state insurance department for online complaints, visit the National Association of Insurance Commissioners at www.naic.org and file a complaint as appropriate.	
15. File a complaint with the Identity Theft Data Clearinghouse, operated by the Federal Trade Commission and the Internet Crime Complaint Center. Information available for filing a complaint can be found at https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03.	
16. Contact the Office of the Inspector General, HHS TIPS Hotline at (800) 447-8477 or by e-mail at HHSTips@oit.hhs.gov for suspected Medicare or Medicaid fraud. [note: information updated December 2008]	
17. Review health records to make sure they have been corrected prior to seeking healthcare.	
18. Change all personal identification numbers and passwords for protected accounts, sites, access points, etc. Choose unique personal identification numbers and complex passwords rather than common ones (e.g., mother's maiden name, birth date, or pet name).	

Responding to Medical Identity Theft Incidents

Effectively responding to incidents of medical identity theft requires the collaborative efforts of individual victims, HIM professionals, privacy and security officers, other organizational leaders, and other external stakeholders.

Individuals may be the first to learn about an incident of identity theft involving their health information. Should they become aware of medical identity theft they are encouraged to:

- Contact the health information manager or privacy officer at the provider organization or antifraud hotline at the health plan where the medical identity theft appears to have occurred.
- Request an accounting of disclosures from the relevant healthcare providers or health plans.
- Take detailed notes of conversations. Write down the date, name, and contact information of everyone contacted as well as the content of the conversation.
- Make copies of any letters or e-mail sent or received regarding the identity theft.
- Work with the organization where the medical identity theft occurred to stop the flow of incorrect information, correct the health record entries, and determine where incorrect information was sent.
- File a police report and send copies with correct information to insurers, providers, and credit bureaus once the identity theft has been confirmed.
- File a complaint with the attorney general in the state where the identity theft occurred. The National Association of Attorneys General provides state-by-state information at www.naag.org/attorneys_general.php.
- File a complaint with the state insurance department, if possible. Many states provide consumer protection and education related to insurance fraud and accept online complaints. To determine if a state has a state insurance department for online complaints, visit the National Association of Insurance Commissioners at www.naic.org.
- File a complaint with the Identity Theft Data Clearinghouse, operated by the Federal Trade Commission and the Internet Crime Complaint Center at www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html.
- Contact the Office of the Inspector General, HHS TIPS Hotline at (800) 447-8477 or by e-mail at HHSTips@oit.hhs.gov for suspected Medicare or Medicaid fraud. [note: information updated December 2008]
- Check and correct credit reports as appropriate.
- Review health records to make sure they have been corrected prior to seeking healthcare.

Every organization that collects, maintains, uses, or transmits individually identifiable health information should have a policy and procedure and response team for responding to medical identity theft. This process may be covered under the security incident response. This framework will help the organization implement an efficient, effective, and comprehensive incident response and stop the continued flow of information that may otherwise negatively affect the victim and others.

"The Data Breach Investigation and Mitigation Checklist" published in the January 2008 *Journal of AHIMA* (and available online in the FORE Library: HIM Body of Knowledge at www.ahima.org) offers organizations guidance on the steps they should take to address medical identity theft.

HIM professionals can assist victims and their organizations by:

- Coleading the appointment of a medical identity theft response team and working with the team to conduct a risk analysis, discuss medical identity theft mitigation and response, draft policies and procedures, and educate leadership.
- Training HIM staff as to appropriate responses to identity theft events.
- Giving victims a free copy of their health information before and after it is corrected.
- Setting up mechanisms to correct inaccurate information. Consider establishing Jane or John Doe records in which the identity thief's information is maintained separately from the victims with links to the original record.
- Implementing legal hold policies and procedures.
- Assisting victims in identifying those who may possess inaccurate records by providing a full accounting of disclosures.
- Supporting victims as they attempt to navigate their way through the complex systems that hold copies of incorrect information about them.
- Providing victims with a list of resources and contact information (see the checklist on the preceding page).
- Staying abreast of medical identity theft-related legislation that may be drafted at the state and federal level and providing constructive input and feedback.

HIM professionals can offer victims of medical identity theft the checklist of actions and resources shown [above].

Medical identity theft is a complex and evolving crime that can only be dealt with through a concerted effort. Consumer involvement is paramount to the success of any strategy. HIM professionals collaborating with all stakeholders have a unique opportunity to contribute to solutions that will prevent, investigate, and mitigate the damages of medical identity theft.

All victims of medical identity theft require and deserve every protection and support that healthcare industry stakeholders can develop and apply. An effective protective program starts with front-end preventive safeguards and ends with follow-through that reaches wherever incorrect information has flowed.

AHIMA challenges the healthcare industry and all individuals to organize efforts for proactive steps to stem the impact of this quietly growing threat. Only by reporting all instances of fraudulent activities can the medical identity theft be addressed and mitigated.

Notes

1. Federal Trade Commission. "FTC Releases Survey of Identity Theft in the U.S. Study Shows 8.3 Million Victims in 2005." November 27, 2007. Press release. Available online at www.ftc.gov/opa/2007/11/idtheft.shtm.
2. The elements that define individually identifiable health information are listed in the HIPAA privacy rule, 42 U.S.C. Sec. 1320 d (6).
3. World Privacy Forum. "The Medical Identity Theft Information Page." Available online at www.worldprivacyforum.org/medicalidentitytheft.html.
4. McKay, Jim. "Identity Theft Steals Millions from Government Health Programs." *Government Technology*. Feb. 13, 2008. Available online at www.govtech.com.
5. Griffin, R. Morgan. "The Scary Truth about Medical Identity Theft." WebMD February 2, 2007. Available online at www.webmd.com/a-to-z-guides/features/scary-truth-medical-identity-theft.
6. Rys, Richard. "The Imposter in the ER." MSNBC.com. March 13, 2008. Available online at www.msnbc.msn.com/id/23392229.
7. Ibid.
8. ConsumerReports.org. "Prevent Medical Identity Theft." February 11, 2008. Available online at http://blogs.consumerreports.org/health/2008/02/prevent-medical.html.
9. Blue Cross Blue Shield Association. "What You Can Do to Help Prevent Healthcare Fraud and Abuse." Available online at www.bcbs.com/blueresources/anti-fraud/what-you-can-do.html.
10. Lopez, Jorge, et al. "Gartner's Top Predictions for Industry Leaders, 2007 and Beyond." December 2006. Available online at www.gartner.com.
11. Davis, Nancy, Chrisann Lemery, and Kim Roberts. "Identity Theft and Fraud—The Impact on HIM Operations." *Journal of AHIMA* 76, no. 4 (Apr. 2005): 64A–D.

References

Clymer, Adam. "Officials Say Troops Risk Identity Theft after Burglary." *New York Times,* January 12, 2003.

Federal Trade Commission. "Consumer Fraud and Identity Theft Complaint Data, January–December 2007." February 13, 2008. Available online at www.ftc.gov/opa/2008/02/fraud.pdf.

Long, Kurt. "Medical Identity Theft: The Case for Electronic Privacy Auditing and Continuous Compliance." *New Perspectives: Association of Healthcare Internal Auditors,* Summer 2007: 5 .

Knight, Victoria E. "Escalating Health-Care Costs Fuel Medical Identity Theft: Patients Are Told to Guide ID Cards Like Other Plastics." *Wall Street Journal,* October 11, 2007 (Eastern edition).

Newman, Graeme R., and Megan M. McNally. "Identity Theft Literature Review." Paper prepared for presentation and discussion at the National Institute of Justice Focus Group. January 2005. Available online at www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

Bibliography

AHIMA. "Online, On Message, On Duty: Privacy Experts Share Their Challenges." April 2008. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

AHIMA e-HIM Work Group on Regional Health Information Organizations (RHIOs). "Using the SSN as a Patient Identifier." *Journal of AHIMA* 77, no. 3 (Mar. 2006): 56A–D.

Foundation for Research and Education. "Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities." 2005. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Harman, Laurinda B., and Virginia L. Mullen. "Emerging HIM Identity Ethical Issues." AHIMA's 79th National Convention and Exhibit Proceedings, October 2007. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Nichols, Cindy, ed. *Medical Identity Theft* . Chicago: AHIMA, 2008.

O'Brien, Jenny. "Responding to Identity Theft: One Organization's Effort to Turn a Negative Event into a Positive Result." *Journal of AHIMA* 79, no. 4 (Apr. 2008): 40–41.

Wernick, Alan S. "Connectivity, Privacy, and Liability: What Medical Professionals Must Consider." *Journal of AHIMA* 78, no. 4 (Apr. 2007): 64–65.

Wernick, Alan S. "Data Theft and State Law: When Data Breaches Occur, 34 States Require Organizations to Speak Up." *Journal of AHIMA* 77, no. 10 (Nov.–Dec. 2006): 40–44.

Prepared By

AHIMA e-HIM Work Group on Medical Identity Theft

Chris Apgar, CISSP
Gordon Apple, JD
Larry Ayers
Mary Lynn Berntsen, MS, RHIA
Rebecca Busch, RN, MBA, CCM, CFE, FHFMA
Jennifer Childress, RHIT
Elizabeth Curtis, RHIA, CHP
Nancy Davis, MS, RHIA
Martha Dawson, RHIT, CCS
Beth Hjort, RHIA, CHPS
Gwen Hughes, RHIA, CHP
Chrisann Lemery, MS, RHIA
Desla Mancilla, MPA, RHIA
David Mozie, PhD, RHIA
Jennifer O'Brien, JD, CHC
Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA
Tara Shewchuk, LLB, LLM
David Sweet, MLS
Margie White, MS, NHA, RHIA, CPHQ
Yeva Zeltov, RHIA

The information contained in this practice brief reflects the consensus opinion of the the professionals who developed it. It has not been validated through scientific research.

Article citation:
AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft" *Journal of AHIMA* 79, no.7 (July 2008): 63-69.