

2013 HOUSE INDUSTRY, BUSINESS, AND LABOR

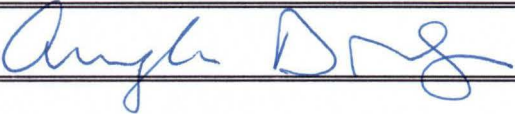
HB 1435

2013 HOUSE STANDING COMMITTEE MINUTES

House Industry, Business and Labor Committee
Peace Garden Room, State Capitol

HB 1435
January 30, 2013
Job 17957

Conference Committee



Explanation or reason for introduction of bill/resolution:

Medical information identity theft

Minutes:

Testimony 1, 2, 3

Committee reconvened.

(00:11) **Representative Corey Mock, District 42** introduced and sponsored HB 1435. Provided testimony (Testimony 1), discussed the bill and recommended an amendment for wording.

(8:46) **Parrell Grossman, Director of the Attorney General's Consumer Protection and Antitrust Division** testified in support of the bill (Testimony 2).

(16:24) **Representative M. Nelson:** Would it be legal if authorization for a release of information were written within the lengthy terms of service on a website to which people must agree in order to continue?

Parrell Grossman: It could possibly be legal.

Representative Kasper: Does the Attorney General have an opinion on if our personal medical information is a protected right under the fourth amendment?

Parrell Grossman: There is certainly a good argument that information like that is protected, but we prefer specific statutory authority.

Representative Kasper: In the Affordable Health Act, the federal government wants to acquire citizens' medical information. Does this bill provide protection for ND citizen who does not want medical information shared with the federal government?

Parrell Grossman: Not immediately. I am concerned you might run into preemption issues.

Representative Kreun: What is the penalty?

Parrell Grossman: A first offense is a Class B felony if it exceeds \$1000, otherwise it is a Class C felony. A subsequent offense is a Class A felony.

(28:51) **Sheldon Wolf, North Dakota Health Information Technology Director** testified regarding changes to the bill (Testimony 3).

Chairman Keiser closed the hearing.

Chairman Keiser: We have several suggested amendments.

Representative Gruchella motioned to adopt all amendments.

Representative Boschee seconded.

Voice vote to adopt amendments.

Representative Kasper motioned for Do Pass as amended.

Representative Johnson seconded.

(37:36) **Representative Corey Mock** questioned wording on the amendments.

(38:33) **Parrell Grossman** asked to hear wording of the amendments.

Roll call vote.

Yes: 14

No: 0

Absent: 1

Chairman: Carried by Representative Gruchella.

January 31, 2013

1/31/11
TD

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1435

Page 1, line 1, replace "54-59-26" with "51-30-06"

Page 1, line 12, overstrike "number" and insert immediately thereafter "information"

Page 1, line 19, remove "in"

Page 1, remove line 20

Page 1, line 21, remove "would permit access to an individual's financial accounts"

Page 2, line 1, replace "number" with "information"

Page 3, line 3, after "Health" insert "insurance"

Page 4, remove lines 1 through 30

Page 5, remove lines 1 through 30

Page 6, remove lines 1 and 2

Page 6, after line 2 insert:

"SECTION 3. AMENDMENT. Section 51-30-06 of the North Dakota Century Code is amended and reenacted as follows:

51-30-06. Alternate compliance.

Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is ~~deemed to be~~ in compliance with this chapter. A covered entity, business associate, or subcontractor subject to breach notification requirements under title 45, Code of Federal Regulations, subpart D, part 164, is considered to be in compliance with this chapter."

Re-number accordingly

Date: 1-30-2013

Roll Call Vote #: 1

**2013 HOUSE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1435**

House Industry, Business, and Labor Committee

Legislative Council Amendment Number 13.0771.01001

Action Taken: Do Pass Do Not Pass Amended Adopt Amendment
 Rerefer to Appropriations Reconsider Consent Calendar

Motion Made By Gruchalla Seconded By Boschee

Representatives	Yes	No	Representatives	Yes	No
Chairman George Keiser			Rep. Bill Amerman		
Vice Chairman Gary Sukut			Rep. Joshua Boschee		
Rep. Thomas Beadle			Rep. Edmund Gruchalla		
Rep. Rick Becker			Rep. Marvin Nelson		
Rep. Robert Frantsvog					
Rep. Nancy Johnson					
Rep. Jim Kasper					
Rep. Curtiss Kreun					
Rep. Scott Louser					
Rep. Dan Ruby					
Rep. Don Vigesaa					

Total Yes _____ No _____

Absent _____

Floor Assignment _____

If the vote is on an amendment, briefly indicate intent:

Date: 1-30-2013

Roll Call Vote #: 2

**2013 HOUSE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1435**

House Industry, Business, and Labor Committee

Legislative Council Amendment Number 13-0771-01001

Action Taken: Do Pass Do Not Pass Amended ^{as} Adopt Amendment
 Rerefer to Appropriations Reconsider Consent Calendar

Motion Made By Kasper Seconded By Johnson

Representatives	Yes	No	Representatives	Yes	No
Chairman George Keiser	✓		Rep. Bill Amerman		ab
Vice Chairman Gary Sukut	✓		Rep. Joshua Boschee	✓	
Rep. Thomas Beadle	✓		Rep. Edmund Gruchalla	✓	
Rep. Rick Becker	✓		Rep. Marvin Nelson	✓	
Rep. Robert Frantsvog	✓				
Rep. Nancy Johnson	✓				
Rep. Jim Kasper	✓				
Rep. Curtiss Kreun	✓				
Rep. Scott Louser	✓				
Rep. Dan Ruby	✓				
Rep. Don Vigasaa	✓				

Total Yes 14 No 0

Absent 1

Floor Assignment Gruchalla

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

HB 1435: Industry, Business and Labor Committee (Rep. Keiser, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (14 YEAS, 0 NAYS, 1 ABSENT AND NOT VOTING). HB 1435 was placed on the Sixth order on the calendar.

Page 1, line 1, replace "54-59-26" with "51-30-06"

Page 1, line 12, overstrike "number" and insert immediately thereafter "information"

Page 1, line 19, remove "in"

Page 1, remove line 20

Page 1, line 21, remove "would permit access to an individual's financial accounts"

Page 2, line 1, replace "number" with "information"

Page 3, line 3, after "Health" insert "insurance"

Page 4, remove lines 1 through 30

Page 5, remove lines 1 through 30

Page 6, remove lines 1 and 2

Page 6, after line 2 insert:

"SECTION 3. AMENDMENT. Section 51-30-06 of the North Dakota Century Code is amended and reenacted as follows:

51-30-06. Alternate compliance.

Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is ~~deemed to be~~ in compliance with this chapter. A covered entity, business associate, or subcontractor subject to breach notification requirements under title 45, Code of Federal Regulations, subpart D, part 164, is considered to be in compliance with this chapter."

Renumber accordingly

2013 SENATE HUMAN SERVICES

HB 1435

2013 SENATE STANDING COMMITTEE MINUTES

Senate Human Services Committee
Red River Room, State Capitol

1435
3/19/13
20143

Conference Committee

Committee Clerk Signature



Explanation or reason for introduction of bill/resolution:

Relating to medical information identity theft.

Minutes:

See "attached testimony."

Vice Chairman Larsen opens the hearing for HB 1435

Rep. Mock introduces HB 1435 to the committee and is in support of HB 1435. See attached testimony #1. Clarifies sections of HB 1435.

(0:06:35) Paul Grossman Director, Consumer Protection and Antitrust Division from the office of Attorney General. See attached Testimony #2 **Senator Axness** questioned about BCBS card has stolen and used. **Senator Dever** asked about the use medical information already covered under identity theft laws and penalties. **Senator Larsen** asked about what types and how many identity thefts.

(0:14:51) heldon Wolf, the ND Health Information Technology Director. Provided information for HB 1435. See attached testimony #3. 1652

Vice Chairman Larsen closes the hearing on HB 1435

Senator Anderson Motions for Do pass

Senator Axness seconds

Do Pass 5-0-0

Senator Anderson will carry to the floor.

Date: 3-19-13
Roll Call Vote #: 1

2013 SENATE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1435

Senate Human Services Committee

Check here for Conference Committee

Legislative Council Amendment Number _____

Action Taken: Do Pass Do Not Pass Amended Adopt Amendment
 Rerefer to Appropriations Reconsider

Motion Made By SEN. ANDERSON Seconded By SEN AXNESS

Senators	Yes	No	Senator	Yes	No
Chairman Judy Lee	✓		Senator Tyler Axness	✓	
Vice Chairman Oley Larsen	✓				
Senator Dick Dever	✓				
Senator Howard Anderson, Jr.	✓				

Total (Yes) 5 No 0

Absent _____

Floor Assignment SEN ANDERSON

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

HB 1435, as engrossed: Human Services Committee (Sen. J. Lee, Chairman)
recommends **DO PASS** (5 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING).
Engrossed HB 1435 was placed on the Fourteenth order on the calendar.

2013 TESTIMONY

HB 1435

Mitigating Medical Identity Theft

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:

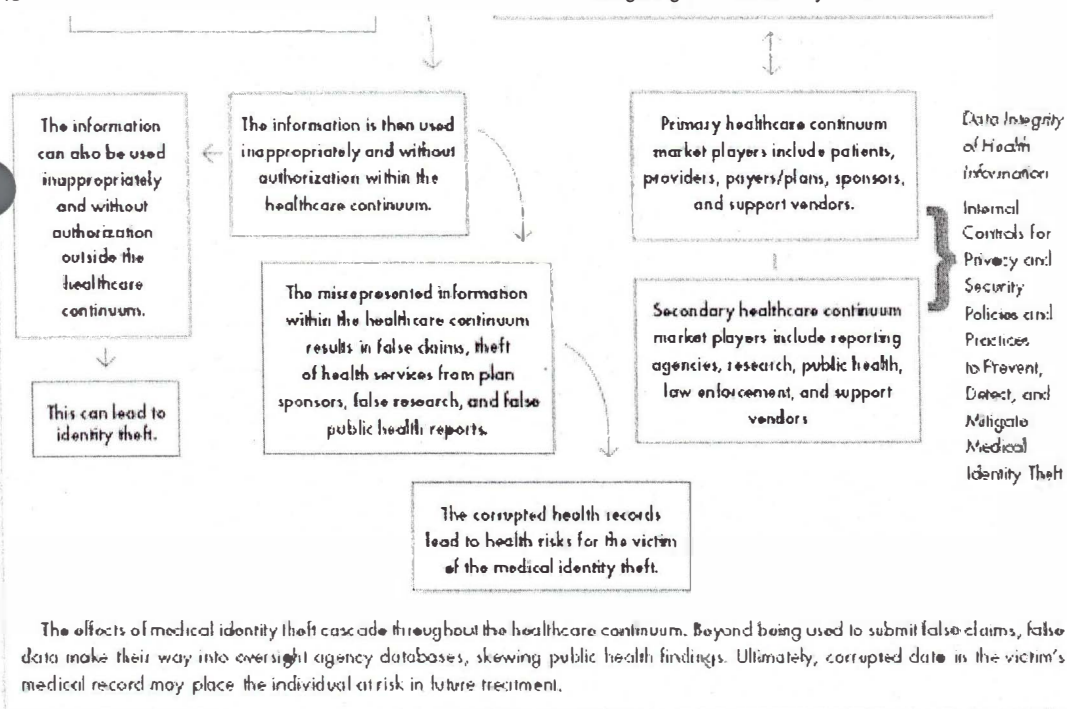
- Obtain benefits or services for which the individual is not eligible
- Obtain services for which the individual will not pay
- Perpetrate other fraud or illegal activity (such as erroneous billings or drug-seeking behavior for personal use or illegal distribution)

“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 Cascading Effect of Medical Identity Theft

Medical identity theft begins with the theft of individually identifiable health information.

Individually identifiable health information elements come from multiple sources.



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.

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.

Copyright ©2008 American Health Information Management Association. All rights reserved. All contents, including images and graphics, on this Web site are copyrighted by AHIMA unless otherwise noted. You must obtain permission to reproduce any information, graphics, or images from this site. You do not need to obtain permission to cite, reference, or briefly quote this material as long as proper citation of the source of the information is made. Please [contact Publications](#) to obtain permission. Please include the title and URL of the content you wish to reprint in your request.

HOUSE JUDICIARY COMMITTEE
GEORGE J. KEISER, CHAIRMAN
JANUARY 30, 2013

② HB 1435
1-30-2013

TESTIMONY BY
PARRELL D. GROSSMAN
DIRECTOR, CONSUMER PROTECTION AND ANTITRUST DIVISION
OFFICE OF ATTORNEY GENERAL
IN SUPPORT OF
HOUSE BILL NO. 1435 (SECTIONS 1 AND 2)

Mr. Chairman and members of the House Industry, Business and Labor Committee. I am Parrell Grossman, Director of the Attorney General's Consumer Protection and Antitrust Division. I appear on behalf of the Attorney General in support of Sections 1 and 2 of House Bill 1435, with proposed amendments.

Identity Theft continues to be a priority for the Attorney General and Consumer Protection Division. The Identity theft problem continues to grow on a national and state basis. The Consumer Protection Division acts as a clearinghouse for ID theft victims. We process ID theft complaints and assist consumers when their identities have been stolen. The Attorney General's Office has received 112 ID Theft complaints in the current biennium, since July 1, 2011. The Consumer Protection Division has received 76 ID theft complaints in 2012. ID theft was the number two complaint category in the Attorney General's Top Ten Complaints in 2012.

With some likely unintended consequences for the changes proposed on page 1, lines 18-21, the changes to the definition of "personal identifying information" enhance protections for potential "identity theft victims."

Attached are proposed amendments to lines 18 through 21 that address "an individual's financial institution account number, credit card number, or debit card number." I have discussed the Attorney General's proposed amendments with Representative Mock, the prime sponsor of HB1435, and he supports the proposed amendments. Current law provides that "[t]he identifying number of a depository account in a financial institution" is personal identifying information. The proposed changes in lines 18 through 21 appear to synchronize this definition with a similar definition in section 51-30-01 of North Dakota's Data Security Breach Law, specifically subdivision (a)(4) of subsection 4, as contained in current law and set forth on page 3, lines 17 through 20, of House Bill 1435.

I was involved in drafting that definition and specific legislation in the 2005 legislative session, as enacted by the Legislature at that time. I worked with the North Dakota Banker's Association on that language to ensure that a data security breach or other inadvertent release of an account number only did not constitute a security breach that would trigger a security breach notice requirement that would be burdensome or otherwise impose unnecessary compliance costs on financial institutions. There did not

appear to be any real risk to an account holder in circumstances in which an access code, security code, or password was not compromised or released in conjunction with the account number. Without the access codes, an individual would not be able to steal another person's identity or access the financial account.

However, the perspective and potential consequences to identity theft victims change in regard to the definition in the identity theft statute. The initial change proposed in this legislation would provide less protection to potential victims. There is a risk to consumers when account numbers, without access codes, are stolen, misused, *et cetera*. Imposing this new requirement would now provide less protection to account holders. While many retailers require the 3 or 4 digit code on the credit card before authorizing purchases with that credit card, there are retailers or other businesses that will accept charges on a credit card without any security code. Just recently an employee of the Attorney General's Office disclosed that a spouse had used her credit card (with permission) to book hotel rooms on a website for a third party hotel reservation entity. The business did not require any security or access codes.

The Attorney General requests this Committee amend lines 18 through 21 to state as follows: " An individual's financial institution account number, credit card number, or debit card number (period). The attached amendments will make this change.

All the other changes in Section 1 of this legislation are improvements. The Attorney General also supports the changes and improvements in Section 2 addressing data security breaches.

The Attorney General is neutral on Section 3 of this legislation.

The Attorney General respectfully asks the House Judiciary Committee to adopt the proposed amendments and give Sections 1 and 2 of House Bill 1435, a "Do Pass" recommendation.

Thank you for your time and consideration. I would be pleased to try and answer any questions.

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1435
HOUSE INDUSTRY, BUSINESS AND LABOR COMMITTEE
GEORGE J. KEISER, CHAIRMAN
JANUARY 30, 2013

PRESENTED BY
PARRELL D. GROSSMAN, DIRECTOR
CONSUMER PROTECTION & ANTITRUST DIVISION
OFFICE OF ATTORNEY GENERAL

Page 1, line 19, replace "in" with a period

Page 1, remove line 20

Page 1, line 21, remove "would permit access to an individual's financial account"

Renumber accordingly

3 HB 1435
1-30-2013

**TESTIMONY BEFORE THE HOUSE
INDUSTRY, BUSINESS AND LABOR COMMITTEE
HOUSE BILL 1435
JANUARY 30, 2013**

Mr. Chairman, members of the committee, I am Sheldon Wolf, the ND Health Information Technology Director. I am here today to provide information and suggest a couple of changes to House Bill 1435 on behalf of the Health information Technology Office and the Health Information Technology Advisory Committee (HITAC) (see attached).

HITAC is charged with making recommendations and implementing a statewide interoperable health information infrastructure that is consistent with emerging national standards and promotes interoperability of health information systems for the purpose of improving health care quality, patient safety, and overall efficiency of health care and public health services. Section 2 would specifically require notification of any breach that may happen through the North Dakota Health Information Network (NDHIN). Section 3 of this bill specifically addresses a requirement that the administrative code include a protocol to address identity theft.

As part of our work, we try to coordinate policies and procedures with current state and federal regulations regarding the protection of an individual's health information. As we were reviewing this section, we noted that for covered entities, (NDHIN, providers, health plans and business associates) the requirements being added in section 2 may be covered by the health insurance portability and accountability act (HIPAA). Specifically, Part 164 of title 45 of the code of federal regulations. Therefore, we would recommend that you treat covered entities that

are required to report breaches like you do financial entities at NDCC 51-30-06. To do this, we suggest the following amendment:

Page 3, after line 30 insert:

SECTION 3. AMENDMENT. Section 51-30-06 of the North Dakota Century Code is amended and reenacted as follows:

51-30-06. Alternate compliance.

Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is ~~deemed~~ considered to be in compliance with this chapter. A covered entity, business associate, or subcontractor subject to the breach notification requirements of Subpart D of Part 164 of title 45 of the Code of Federal Regulations is considered to be in compliance with this chapter.

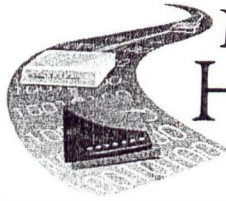
Additionally, the health information technology office is specifically required in Section 3 of the bill (line 25-27 on page 4) to include in administrative rules a protocol for an individual to address identity theft or other errors that result in erroneous medical records being included in the health information exchange. The health information exchange does not create medical record information. It

serves only as a conduit and consolidator of information from disparate systems when a provider requests information through the network. To ensure that these records are modified or deleted correctly, the individual should work directly with the provider that created the record and not the health information exchange.

The health information technology office does not have any authority to require a provider to change their records. However, HIPAA specifically addresses how individuals can request an amendment of protected health information in Part 164 of title 45 of the code of federal regulations (see attached). Therefore, this should be the process that an individual uses to amend their records with health care providers.

In summary, since there is a federal regulation specifically outlining the process for an individual to amend their records, the health information exchange is not the original creator of the medical records and the health information technology office does not have any authority to make a provider change a medical record, please consider removing the proposed additional sentence starting on line 25 of page 4.

Please consider both of these changes and thank you for the opportunity to appear before you today, I would be happy to address any questions.



North Dakota Health Information Technology

Quality Healthcare for all North Dakotans - Anywhere, Anytime

MISSION

Advance the adoption and use of technology to exchange health information and improve healthcare quality, patient safety and overall efficiency of healthcare and public health services in North Dakota.

VISION

Quality Healthcare for all North Dakotans – Anywhere, Anytime.

Website: www.healthit.nd.gov

ND Health Information Technology Advisory Committee

(Member List)

Lisa Feldner, CIO

CHAIR – ADVISORY COMMITTEE

CHAIR – GOVERNANCE DOMAIN WORKGROUP

State of North Dakota, Information Technology Department

Phone: (701) 328-3193

E-mail: lfeldner@nd.gov

Representing state government interests

Laurie Peters, RHIT, Past-President

CHAIR – COMMUNICATION DOMAIN WORKGROUP

North Dakota Health Information Management Assoc.

Phone: (701)748-3485

E-mail: lauriepeters@catholichealth.net

Representing health information management workforce

Lynette Dickson, MS, LRD, Program Director

VICE-CHAIR – ADVISORY COMMITTEE

CHAIR – CLINICAL DOMAIN WORKGROUP

Center for Rural Health, University of North Dakota

School of Medicine and Health Sciences

Phone: (701) 777-6049

E-mail: lynette.dickson@med.und.edu

Representing rural healthcare facilities, organizations and communities

Nancy Willis, Director, Medicaid System Operations and HIT

CO-CHAIR – LEGAL & POLICY DOMAIN WORKGROUP
NDDHS-ITS

Phone: (701) 328-4578

Email: nwillis@nd.gov

Representing Medicaid

Todd Bortke, Director of Information Systems

St. Alexius Medical Center

Phone: (701) 530-8005

E-mail: tbortke@primecare.org

Representing large hospitals

Jennifer Witham, IT Director

CO-CHAIR – LEGAL & POLICY DOMAIN WORKGROUP

North Dakota Department of Human Services

Phone: (701) 328-2310

E-mail: jwitham@nd.gov

Representing Department of Human Services

Janis Cheney, Executive Director

AARP

Phone: (701) 355-3641

E-mail: jscheney@aarp.org

Representing consumers

Barb Groutt, CEO

North Dakota Healthcare Review

Phone: (701) 852-4231

E-mail: bgroutt@ndqio.sdps.org

Representing Medicare's Quality Improvement Organization

Lisa Clute, Executive Officer

First District Health

Phone: (701) 852.1376

E-mail: lclute@nd.gov

Representing local public health units

Caryn Hewitt, CIO

Sanford Health System, Fargo

Phone: (701) 234-6616

E-mail: Caryn.Hewitt@Sanfordhealth.org

Representing tertiary hospitals

Neil Frame, Operations Director

Metro Area Ambulance

Phone: (701) 255-0812

E-mail: nframe@maas-nd.com

Representing EMS

Jerry Jurena, President

North Dakota Hospital Association

Phone: (701) 224-9732

E-mail: jjurena@ndha.org

Representing rural and urban hospitals

Member List continued...

Dan Kelly, CEO

McKenzie County Healthcare System
Phone: (701) 842-3000
E-mail: dkelly@mckenziehealth.com
Representing rural hospitals

Courtney Koebele, Director of Advocacy

North Dakota Medical Association
Phone: (701) 223-9475
E-mail: ckoebele@ndmed.com
Representing physicians

Senator Judy Lee

North Dakota Senator
E-mail: jlee@nd.gov
Representing state legislature

Jim Long, CEO

West River Health Systems
Phone: (701) 567-4561
E-mail: jim1@wrhs.com
Representing rural hospitals

Darin Meschke, Director, Division of Vital Records

North Dakota Department of Health
Phone: (701) 328-2494
E-mail: dmeschke@nd.gov
Representing Department of Health

Health Information Technology Director ~

Sheldon Wolf

State of North Dakota, Information Technology Department
Phone: (701) 328-1991
E-mail: shwolf@nd.gov

HIN Technology Manager ~

Charles Peterson

CHAIR- TECHNICAL INFRASTRUCTURE DOMAIN WORKGROUP
State of North Dakota, Information Technology Department
Phone: (701) 328-1955
E-mail: chapeterson@nd.gov

HIN Business Analyst ~

Tina Gagner, RN

State of North Dakota, Information Technology Department
Phone: (701) 328-1126
E-mail: tgagner@nd.gov

Dave Molmen, CEO

Altru Health System/Chair Hospital Association
Phone: (701) 780-5000
E-mail: dmolmen@altru.org
Representing large hospitals

Shelly Peterson, President

ND Long Term Care Association
Phone: (701) 222-0660
E-mail: shelly@ndltca.org
Representing long term care

Tony Tardugno, CIO

BCBSND
Phone: (701) 282-1470
E-mail: tony.tardugno@bcbsnd.com
Representing 3rd party payor

Tami Ternes, Sr. Policy Advisor-HHS

Governor's Office
Phone: (701) 328-2207
Email: tlternes@nd.gov
Representing government interests

Representative Robin Weisz

North Dakota Representative
Phone: (701) 962-3799
E-mail: rweisz@nd.gov
Representing state legislature

Legal Counsel ~

Pam Crawford, Assistant Attorney General

Attorney General's Office, State of North Dakota
Phone: (701) 328-2210
E-mail: pacrawford@nd.gov

HIN Trainer ~

Robin Hirsch

State of North Dakota, Information Technology Department
Phone: (701) 328-2508
E-mail: rhirsch@nd.gov

ELECTRONIC CODE OF FEDERAL REGULATIONS

e-CFR Data is current as of January 25, 2013

Title 45: Public Welfare
PART 164—SECURITY AND PRIVACY
Subpart E—Privacy of Individually Identifiable Health Information

§ 164.526 Amendment of protected health information.

(a) *Standard: Right to amend* . (1) *Right to amend* . An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment* . A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: requests for amendment and timely action* . (1) *Individual's request for amendment* . The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity* . (i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: Accepting the amendment* . If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Making the amendment* . The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual* . In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others* . The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: Denying the amendment* . If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial* . The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) *Statement of disagreement* . The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement* . The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping* . The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures*. (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: Actions on notices of amendment*. A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: Documentation*. A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

For questions or comments regarding e-CFR editorial content, features, or design, email ecfr@nara.gov.

For questions concerning e-CFR programming and delivery issues, email webteam@gpo.gov.



Log In Communities Home Advanced Search Contact Us Help

Mitigating Medical Identity Theft

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.

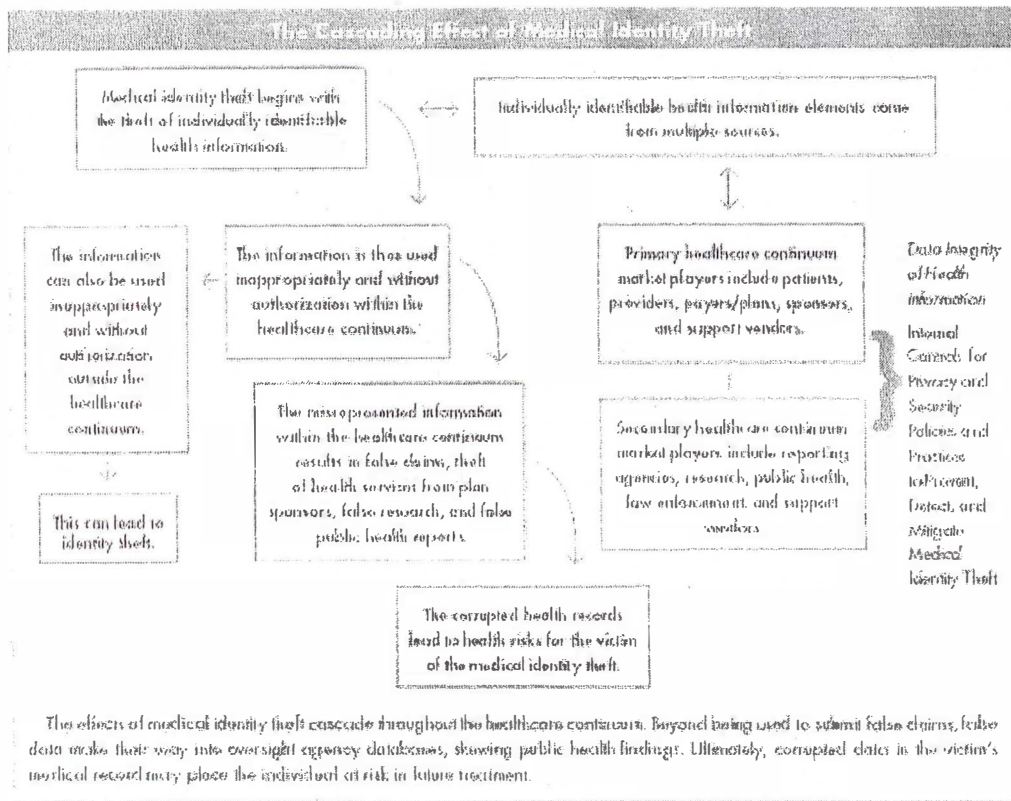
Defining Medical Identity Theft

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 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/privacy/howtofile.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@oig.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

2

SENATE HUMAN SERVICES COMMITTEE
JUDY LEE, CHAIRMAN
MARCH 19, 2013

TESTIMONY BY
PARRELL D. GROSSMAN
DIRECTOR, CONSUMER PROTECTION AND ANTITRUST DIVISION
OFFICE OF ATTORNEY GENERAL
IN SUPPORT OF
ENGROSSED HOUSE BILL NO. 1435

Chairman Lee and members of the Senate Human Committee. I am Parrell Grossman, Director of the Attorney General's Consumer Protection and Antitrust Division. I appear on behalf of the Attorney General in support of Engrossed House Bill No. 1435.

Identity Theft continues to be a priority for the Attorney General and Consumer Protection Division. The Identity theft problem continues to grow on a national and state basis. The Consumer Protection Division acts as a clearinghouse for ID theft victims. We process ID theft complaints and assist consumers when their identities have been stolen. The Attorney General's Office has received 112 ID Theft complaints in the current biennium, since July 1, 2011. The Consumer Protection Division has received 76 ID theft complaints in 2012. ID theft was the number two complaint category in the Attorney General's Top Ten Complaints in 2012. In the last week, the Consumer Protection Division received several identity theft complaints from ID theft victims who indicated other individuals had files income tax returns using the victims' social security numbers.

The changes to the definition of "personal identifying information" on Page 1, lines 18-24 and Page 2, line 1, enhance protections for potential identity theft victims. It is helpful and important to include an individual's health insurance policy or subscriber identification number, an individual's non-driver photo identification card issued by the Department of Transportation, and an individual's digitized or other electronic signature within the information that should be protected for potential identity theft victims. The theft or unauthorized use of this additional information should constitute identity theft.

The Attorney General also supports the changes and improvements in Section 2 addressing data security breaches. N.D.C.C. chapter 51-30, North Dakota's Data Security Breach Law, was drafted by the Attorney General and is enforced by the Attorney General's Consumer Protection Division. The proposed changes regarding "medical information" and "health insurance information" are good changes to this law.

The Attorney General respectfully asks the Senate Human Services Committee give Engrossed House Bill No.1435 a "Do Pass" recommendation.

Thank you for your time and consideration. I would be pleased to try and answer any questions.

**TESTIMONY BEFORE THE SENATE
HUMAN SERVICES COMMITTEE
HOUSE BILL 1435
MARCH 19, 2013**

Madam Chairman, members of the committee, I am Sheldon Wolf, the ND Health Information Technology Director. I am here today to provide information on Section 3 of House Bill 1435 on behalf of the Health Information Technology Office and the Health Information Technology Advisory Committee (HITAC).

HITAC is charged with making recommendations and implementing a statewide interoperable health information infrastructure that is consistent with emerging national standards and promotes interoperability of health information systems for the purpose of improving health care quality, patient safety, and overall efficiency of health care and public health services. As part of our work, we try to coordinate policies and procedures with current state and federal regulations regarding the protection of an individual's health information.

Section 3 of the bill was amended by the House to allow alternative compliance for those entities that are covered by the health insurance portability and accountability act (HIPAA). Specifically, Part 164.404 of title 45 of the code of federal regulations requires covered entities to notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

This alternative compliance treats covered entities that are required to report breaches according to HIPAA similar to the treatment of financial entities at NDCC 51-30-06.

Thank you, I would be happy to address any questions.