Medical Identity Theft Final Report

Contract Number HHSP233200045008XI

January 15, 2009

Prepared by:

Booz Allen Hamilton
One Preserve Parkway
Rockville, MD 20852
TEL: (301) 838-3600
FAX: (301) 838-3606

Prepared for:

US Department of Health and Human Services
Office of the National Coordinator for Health Information Technology

This document is confidential and is intended solely for the use and information of the client to whom it is addressed. The content of this publication does not necessarily reflect the views or policies of the Department of Health and Human Services, nor does mention of trade names, commercial products, or organizations imply endorsement by the U.S. Government.

Booz | Allen | Hamilton

TABLE OF CONTENTS

LIST OF TABLES

Use or disclosure of data contained in this document is subject to the restriction on the title page

1.0 INTRODUCTION

Medical identity theft is an emerging issue that raises concerns for consumers, health care providers, health plans, government, and others. Interest in the issue has been spurred by concerns about identity theft in general and the work of the past two years by the President's Identity Theft Task Force.[1] In addition, the emphasis on the privacy and security of electronic health information exchange has heightened both concerns about medical identity theft's effects, and interest in possible solutions to address it. Pursuant to these increased concerns, the Office of the National Coordinator for Health Information Technology (ONC) initiated a project to improve its understanding of the issue and the role health information technology may play, open a dialogue among the stakeholder community, and share its discoveries publicly.

The project included three phases. The first phase of the project consisted of creating an "environmental scan," a research paper on existing knowledge, policies, and practices addressing the issue. The environmental scan[2] captured what is currently known about the scope of the problem, its costs, and available resources as they relate to prevention, detection, and remediation. The primary objective was to inform stakeholders about what medical identity theft is, to describe the potential impact it has on the U.S. health care system, and to catalog its effects on individuals and organizations that receive, provide, or pay for health care services, based on available information. The environmental scan was released on October 15, 2008.

The second phase of the project involved a "Town Hall" public meeting, held on October 15, 2008, to bring stakeholders together and facilitate a discussion about medical identity theft and the role health information technology (health IT) may play in addressing this issue. The meeting included panel discussions about four topics: current understanding and scope of the issue of medical identity theft; possible methods of examining the issues of prevention, detection, and remediation of medical identity theft; the role of health IT; and potential actions to address the issue. The Town Hall served as a forum to open a dialogue about medical identity theft among stakeholders.

The third phase of the project is the development of this report with recommendations for addressing the issues raised at the Town Hall. For purposes of this project, we defined medical identity theft in the environmental scan, as the misuse of an individual's personally identifiable information (PII)[3] such as name, date of birth, social security number (SSN), or insurance policy number to obtain or bill for medical services or medical goods. Medical identity theft may occur *with or without* the identified individual's consent or knowledge. Some of the potential

[1] The President's Identity Theft Task Force. http://www.idtheft.gov.

[2] Medical Identity Theft Environmental Scan, October 15, 2008. http://www.hhs.gov/healthit/resources/reports.html.

[3] Please note that although this particular Office of Management and Budget (OMB) definition defines Personally Identifiable Information (PII) as limited to data held by a government agency, we are using the term more broadly to mean any such data no matter who generates or uses it. This most broadly applicable definition of PII, given by OMB, is "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual." OMB Memorandum 06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006.

consequences of medical identity theft are the loss of accuracy in medical records, expenses to individuals whose identities are stolen, widespread expenses to the health care system, and compromised patient care if inaccurate health records are relied on at the point of care.

This report includes considerations of policy and technical approaches to addressing issues of prevention, detection, and remediation of medical identity theft.

2.0 PURPOSE

ONC sought to gain a better understanding of medical identity theft and the impact that health IT could play in its prevention, detection, and remediation. This report incorporates the findings from research conducted during the information gathering phase of the environmental scan and from the discussions at the Town Hall. Through the analysis and current understanding of the issue, this report was developed to provide possible actions that stakeholders may take to address medical identity theft. Although there is more information to understand and analyze about the topic, it is also critical to continue working toward a collaborative set of potential actions and broaden our understanding of how those next steps relate to the expanding world of health IT and the nationwide health information network (NHIN). A broad conclusion could be drawn that layering prevention, detection, and remediation methods for medical identity theft on top of ongoing health information exchange privacy and security initiatives could provide a scalable and cost-effective set of potential actions. These potential actions would be based on information that we have gathered thus far. Because we are in the early stages of understanding medical identity theft, these potential actions will need to evolve as more information about this topic becomes available and our understanding increases.

3.0 APPROACH

Three overarching elements relating to medical identity theft were considered throughout the information gathering phase of the project. In the next section, these three elements are discussed as they relate to the potential actions. These elements are—

- **Prevention**. Prevention activities are those that may assist in stopping medical identity theft from occurring. Prevention minimizes risk to patients' health records. In a case of medical identity theft, the health care provider may update the health record owner's information, but in doing so will insert information that is not in fact about that person but about the individual posing as that person. This inaccurate information could at a later time compromise patient care. Prevention, therefore, decreases the possibility that inappropriate information will be inserted into individuals' records. It also can decrease unauthorized access by individuals seeking to sell or otherwise inappropriately disclose health records, which can also lead to medical identity theft as well as other forms of fraud.

- **Detection.** Detection activities are those that assist in accurately identifying instances of medical identity theft once they have occurred and may also include determining how, where, and when the theft occurred.

- **Remediation.** Remediation activities are those that will assist individuals who are victims of medical identity theft and affected organizations after the event has occurred and has been detected. Remediation activities are intended to minimize medical identity theft's effects, risks, and costs, with the goal of attempting to restore the victims' medical and financial information to the state it was in prior to the incident.

3.1 MEDICAL IDENTITY THEFT—COMMON THEMES

Many speakers at the Town Hall made observations in their comments and responses to questions indicating a shared set of beliefs about medical identity theft. A number of major themes emerged that are relevant to developing potential actions to addressing medical identity theft. The themes that emerged the most frequently were:

- The consumer should be the key focus for consideration of prevention, detection, and remediation of medical identity theft.
- Although there has been an increased awareness of medical identity theft, there is limited knowledge about its scope.
- Health IT has a role in addressing the problem of medical identity theft.

The Consumer Is Central to the Issue of Medical Identity Theft

The consumer has the greatest potential for loss as well as key roles in prevention, detection, and remediation. Of course, many other parties may be involved or affected by medical identity theft. An individual may inappropriately access health data when it is held by many participants in the health care delivery chain, including the insurer, health care provider, a third party (e.g., lab, pharmacy), or the consumer. When these misappropriations result in medical identity theft, however, the impact on the consumer has the possibility of being the most severe. Some potential effects on the consumer include compromise of patient care as a result of inaccurate health information entering his or her health record; inability to receive health insurance or other benefits; or financial obligations for services that were never received. In turn, the consumer is most knowledgeable about his or her own health record and, therefore, is the first line of defense for protecting against medical identity theft and identifying a potential issue early, which may help to reduce the damage.

There Is Limited Knowledge of the Scope of Medical Identity Theft

A dominant message that emerged during the initial research and was validated at the Town Hall was that a large number of individuals and organizations are unaware of the issue of medical identity theft and the extent to which this form of identity theft exists. A large part of this lack of awareness results from the limited data available specific to medical identity theft. In many instances, medical identity theft may be categorized as health care fraud. Although it does fall into the greater category of health care fraud, there are unique and important distinctions of medical identity theft that need to become more commonly understood to address this issue effectively. The primary motive for committing health care fraud is most often monetary gain, such as when fraudulent providers bill for more expensive services than those rendered. However, medical identity theft tends to be focused on the use of someone else's information to gain goods, services and health care, which can affect the victim's medical record and future care. This is an important distinction, which may result in different methods for addressing the problem. Understanding the scope and improving awareness of these issues are critical to addressing them.

Health IT Has a Role in Addressing the Problem of Medical Identity Theft

Health IT is an evolving resource for the health care community and "allows comprehensive management of medical information and its secure exchange between health care consumers and providers."[4] The ability to track, monitor, and audit health data electronically has the potential of helping to address the issue of medical identity theft. For example, using role-based access that allows individual access to health data on a need-to-know basis, combined with "red flag"[5] type auditing practices focused on identifying anomalies, may be helpful in preventing and detecting medical identity theft. The Town Hall included discussion of potential fears related to an NHIN, such as the vulnerability of the health data resulting from access to large quantities of it at one time, combined with the cascading effect [6] across the system in the case of data corruption. However, most of the leading experts who participated in the Town Hall agreed that, if implemented and executed properly, health IT and health information exchange could be used to prevent, detect, and help with correction of medical identity theft in a manner that has not been previously available. Overall, health IT would provide opportunities for greater communication channels, more standardized approaches to managing risk, and increased data security.

The development and adoption of health IT relies significantly on the trust of the security, validity, and accuracy of the system by consumers and those involved in health information exchange. Consumers want to be assured that their health information will be handled with privacy and security in mind. Providers want to know that the information they are using for the purpose of diagnosis and treatment is accurate and secure. These factors are directly linked to adoption because neither consumers nor providers will totally embrace health IT without confidence that these concerns are being addressed.[7] Medical identity theft is one of the issues to be addressed to promote the privacy and security of health information.

4.0 POTENTIAL ACTIONS

This section outlines potential actions based on the knowledge gained throughout the project. The steps are organized into four categories: leadership, education, business processes and technology, and policies and laws.

4.1 LEADERSHIP

A resounding theme from the community of stakeholders who participated in our research and the Medical Identity Theft Town Hall was the need for a strong national-level presence driving a

[4] U.S. Department of Health and Human Services. Health Information Technology. Retrieved December 10, 2008, http://www.hhs.gov/healthit/.

[5] Please see Section 4.4.4 Policies and Laws for more information on "red flag" approaches.

[6] American Health Information Management Association (AHIMA) refers to this idea that there may be impacts to the health care delivery chain such as the effects to claims data, which can result in incorrect public health data, as well as research, but ultimately the information may result in a corrupted patient's health record and place the consumer at risk during future medical visits. AHIMA reference-HIM Workgroup on Medical Identity Theft. "Mitigating Medical Identity Theft." *Journal of AHIMA* 79:7 (July 2008): 63–69.

[7] State Alliance for E-Health. *Accelerating Progress: Using Health Information Technology and Electronic Health Information Exchange to Improve Care.* National Governors Association, 2008.

standardized and coordinated approach to detection, prevention, education, and victim recovery. Just as there is now a standard process to follow in the case of financial identity theft, a similar approach is needed to respond to medical identity theft. This would require a core set of policies, principles, and methodologies applicable to data integrity for those entities responsible for personal health data.

The Federal Government has already recognized the need for national-level leadership to drive the development of a comprehensive response to address the broad issue of identity theft. This is supported by Executive Order 13402, May 10, 2006, that called for the establishment of the Presidential Identity Theft Task Force. The task force comprises 15 federal departments and agencies that have now completed the development of a strategic plan as well as a summary set of recommendations to address the crime of identity theft and ensure standard processes and procedures are in place to support victims of this crime. The task force's strategic plan focused on four key areas: data protection, data misuse, victim assistance, and deterrence.[8] In support of implementing the strategic plan, the task force further released a set of interim recommendations designed to raise awareness and increase the effectiveness of prevention, detection, and prosecution. These interim recommendations focused on law enforcement, education, and government safeguards.

Although medical identity theft has unique characteristics that are different from general identity theft (for example, it has an impact on medical records and patient care), many of the recommendations identified by the Presidential task force may be applicable in developing a response framework for this issue. An initiative similar to the Presidential task force combined with representatives from anti-fraud associations, provider organizations, payers, and consumer advocates could work together to ensure the topic is kept in the forefront, and to spearhead the development of cross-cutting solutions. The limited information that exists about medical identity theft indicates that leadership should establish a structure that enables all stakeholders to come together to communicate their experiences, best practices, and lessons learned. These efforts would have the potential to address significantly one of the Town Hall event's major themes, that of the lack of current information. The Town Hall event demonstrated the interest in and value of providing such an opportunity for public and private sector members to come together to discuss medical identity theft issues. More value, however, could be derived from a standing body of stakeholders that could track and address this issue over time, rather than a one-time assembly.

In addition, the Government should take the lead to ensure that medical identity theft is taken into consideration as part of the broader interoperability, governance, and privacy and security initiatives associated with the interchange and protection of personal health data. Feedback from our research and the medical identity theft Town Hall indicated agreement across the stakeholder community that the prevention and detection of medical identity theft needs to be built into and considered as an integral part of health IT activities now and in the future.

- **Potential Action**: Establish a public-private task force, a formation and membership of public and private entities, under government leadership to focus on medical identity theft that includes initiatives such as—

[8] The President's Identity Theft Task Force. "Combating Identity Theft—A Strategic Plan," April 2007.

  - Health Information Security and Privacy Collaboration (HISPC)
  - Department of Health and Human Services, Office of the National Coordinator for Health Information Technology
  - National eHealth Collaborative (formerly known as the American Health Information Community 2.0)
  - Certification Commission for Healthcare Information Technology (CCHIT)
  - Healthcare Information Technology Standards Panel (HITSP)
  - Nationwide Health Information Network (NHIN)
  - TRICARE Management Activity's (TMA) Health Information Privacy and Security Compliance Committee (HIPSCC).
- **Potential Action:** Review and analyze the processes used to respond to financial identity theft and consider developing a similar approach for responding to medical identity theft.

- **Potential Action:** Develop strategies and an approach, at a national level, to further identify and classify risks related to medical identity theft for all stakeholders, and to address these risks.

4.2 KNOWLEDGE AND EDUCATION

Panelists at the Town Hall event agreed that the true scope of medical identity theft is not well known. Although preliminary data from a 2006 Federal Trade Commission (FTC) survey suggested there are approximately 250,000 victims of the crime,[9] this estimate may no longer be a reasonable measure of the scope of the problem. In addition, in many instances, individuals may not be aware that they are victims of the crime, which may lead to significant underreporting. Panelists at the Town Hall commented that there is a need to raise awareness and educate consumers on this form of identity theft and the potential impact on their personal health information. Another reason that medical identity theft may be more prevalent than is generally believed is that few organizations are subcategorizing these incidents within the larger category of identity theft or health care fraud. In the absence of the collection of specific data, current knowledge is incomplete. Furthermore, it would be valuable to have a better handle on the true risks that are raised in this area and the potential tools and techniques that can help address these risks. Since this has not been an issue that has been considered and addressed broadly, greater understanding of the risks will help develop strategies for prevention, detection, and remediation. Further research would assist in addressing the limited knowledge that was one of the major themes to emerge from the Town Hall event.

- **Potential Action:** Conduct systematic, structured surveys on the frequency of medical identity theft.

- **Potential Action:** Take a risk management approach, to identify, classify, and potentially quantify the impact of medical identity theft, develop mitigation strategies, and identify tools, techniques, and controls appropriate for specific applications.

[9] *Federal Trade Commission – 2006 Identity Theft Report*. Prepared by Synovate, November 2007. http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

Researchers may, for example, be able to consider data collected for other primary purposes to estimate the frequency of medical identity theft. There are a number of organizations, such as credit reporting agencies, health care insurers, and providers, that currently house consumer data or health care data. Although these organizations may not use the information to track medical identity theft, researchers may be able to analyze this data to provide better insight into the problem. For example, in 2007, the United States Public Interest Research Group (PIRG) conducted a survey on the accuracy of credit reports. The results of the survey indicated that "29% of the credit reports that individuals reviewed contained serious errors that could result in the denial of credit or other benefits."[10] These survey results indicate the potential value of having consumers play a role in detection. A credit report may be used to identify instances of medical identity theft based on possible financial ramifications such as unpaid bills, or a delinquent health account that may appear on an individual's credit report.

- **Potential Action:** Use data analytics to review existing data sets such as claims and collections, and credit reports to provide better estimates about the magnitude of medical identity theft.

Participants from the Medical Identity Theft Town Hall and the information collected from research and stakeholder interviews for the Environmental Scan Report indicated that addressing education and awareness initiatives for consumers, health care plans, and law enforcement and health care professionals is critical to tackling this emerging form of identity theft. The need to increase awareness and educate stakeholders about medical identity theft is important for prevention, detection, and remediation. It is essential that consumers know how to protect their information and how to use resources such as explanation of benefits (EOB) to identify an error or discrepancy. Industry experts who participated in the Town Hall suggested the following options for consumers and health care professionals to proactively help safeguard health information:

- **Potential Action:** Identify effective mechanisms and best practices used in the financial industry for educating consumers about medical identity theft.
- **Potential Action:** Develop appropriate educational programs about medical identity theft for consumers, health care payers, health care professionals, and law enforcement.

Panelists at the Town Hall cited that adding medical identity theft education and awareness details to health literacy programs and continuing to advance health literacy in general could aid in the prevention and detection of medical identity theft. According to the American Medical Association (AMA), health literacy is "the ability to obtain, process, and understand basic health information and services needed to make appropriate health decisions and follow instructions for treatment." AMA goes on to note, "a recent government study estimates that over 89 million American adults have limited health literacy skills. Furthermore, studies also show that people of all ages, races, income, and education levels are challenged by this problem. Individuals with limited health literacy incur medical expenses that are up to four times greater than patients with adequate literacy skills, affecting the costs to the health care system in the billions of dollars

[10] Public Interest Research Group. PIRG: Mistakes Do Happen: Credit Report Errors Mean Consumers Lose. March 1998, http://static.uspirg.org/reports/mistakesdohappen3_98.pdf.

every year in unnecessary doctor visits and hospital stays."[11] Inadequate health literacy skills, such as difficulty understanding EOBs, may hinder a patient's ability to recognize that someone has accessed his or her health information and exploited it. During the Town Hall, panelists noted that education programs do exist but should be evaluated to determine ways to include education about medical identity theft, patient rights, and access to medical record information. The HHS Health Resources and Services Administration (HRSA) and various private sector organizations offer health literacy training programs focused on training health care professionals on effective methods for communicating and educating patients. Possible topics to include in these health education programs are how to interpret EOBs and individuals' rights under the Health Insurance Portability and Accountability Act (HIPAA) and its associated regulations, such as the HIPAA Privacy and Security Rules. These consumer-focused education activities will have the benefit of addressing the problem at the consumer level, consistent with the theme of the Town Hall event the consumer is the most affected by medical identity theft.

- **Potential Action:** Identify existing health literacy programs that can be expanded to include information on medical identity theft to help educate and raise consumer awareness.

In addition, feedback from stakeholders indicated that education about medical identity theft should be included as part of an organization's overall communications strategy for staff and patients. Health care organizations may consider evaluating their current communications tools and consider tailoring them to integrate education on medical identity theft, which could include how medical identity theft might occur, the potential impact, and what to do in the event of a possible breach of information contained in health records.

- **Potential Action:** Integrate education on medical identity theft as part of employee communications at provider organizations; include information on medical identity theft in patient education materials.

4.2.1 Patient Access

Another way in which patients can participate in the detection and remediation of medical identity theft is to ensure they are allowed appropriate access to their medical records. Key to more fully leveraging this opportunity will be providing greater education and awareness about patients' access rights to both providers and consumers. Under the Privacy Rule, patients have the right to inspect and obtain copies of their protected health information (PHI) contained in a designated record set held by "covered entities" (i.e., individuals and organizations that are required to address HIPAA), subject to certain limitations.[12] One of the most important reasons why patients may want to access their records is to ensure the health records are complete and accurate, and therefore be able to inform their health care providers appropriately and accurately.

[11] American Medical Association. *Health Literacy*. October 14, 2008. Retrieved December 10, 2008, http://www.ama-assn.org/ama/pub/category/8115.html.

[12] "[An] individual has a right of access to inspect and obtain a copy of [PHI] about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set…." Standards for Privacy of Individually Identifiable Health Information; Final Rule ("The HIPAA Privacy Rule"), 45 CFR § 164.524 (a)(1), "Access of individuals to protected health information." Some limited exceptions apply.

Some covered entities, however, are unclear about the appropriate implementation of this aspect of the HIPAA Privacy Rule. Town Hall participants asserted that some providers will provide records only if confronted with a court order or subpoena, citing costs and administrative burdens. Participants also related that some health care providers are confused about the effects of having the data of another, unidentified individual incorporated into health records. These providers believe that providing patients with copies of their corrupted records would amount to an inappropriate disclosure of the medical identity thief's health care information. Although guidance, frequently asked questions (FAQ), and other resources are available on the Privacy and Security Rules,[13] there is still a lack of clarity on the interaction of the right of access under the HIPAA Privacy Rule and medical identity theft.

- **Potential Action:** Develop clear, accurate resources for HIPAA covered entities, which clarify how they can comply with the HIPAA Privacy Rule's access requirements in cases of possible medical identity theft.

For patient access to be meaningful, patients need to be informed before a privacy or security breach occurs that they have the right to request access to their health records and to be notified regarding how they can make that request. All HIPAA covered entities have obligations to patients concerning patient access. HIPAA requires covered entities to provide patients with a copy of their "notice of privacy practices,"[14] which should include an explanation of how patients can obtain a copy of their medical records. In cases of security breaches, some health care organizations do not wait for patients to make these requests, but automatically provide affected patients' copies of their medical records after a breach so those patients can detect any inaccuracies. A major theme of the Town Hall was the belief that patients are in the best position to validate the integrity of the data in their own records, and increasing access to their records will allow them greater opportunity to conduct an appropriate review.

This belief appears to be mirrored in current practices. In a recent Health Information and Management Systems Society (HIMSS) survey, for example, 25 percent of health care IT staff surveyed reported that their organizations responded to the threat of medical identity theft by providing patients with greater resources to identify and report suspected medical identity theft or other fraudulent activities to the organization's management.[15] That survey did not ask respondents to verify what these resources were, but one of the most common ones discussed by stakeholders has been to allow patients direct, read-only access to their medical records using web-enabled tools. To the best of our knowledge, however, no studies have been conducted to evaluate the effectiveness of these kinds of measures in increasing the detection of medical identity theft. Many Town Hall participants returned to the theme that stakeholders have not yet fully explored health IT's ability to address medical identity theft.

[13] HHS's Office for Civil Rights (OCR) enforces the HIPAA Privacy Rule,[13] and CMS enforces the HIPAA Security Rule.[13] Enforcement of one or both against a HIPAA-covered entity may be appropriate if medical identity theft is a result of privacy and/or security practices that do not meet the requirements of these HIPAA rules.

[14] "Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information." HIPAA Privacy Rule § 164.520 (Notice of privacy practices for protected health information; Standard: notice of privacy practices).

[15] HIMSS. HIMSS Security Survey sponsored by Booz Allen Hamilton, October 2008. Can be accessed at http://www.himss.org/advocacy/d/HIMSS_SecurityReport102408.pdf.

- **Potential Action:** Evaluate the effects of providing real-time access to patient records on the detection of medical identity theft.

Other methods of ensuring patients have access to their medical records rely on existing business practices. Many health insurers also provide patients with EOB statements. Insurers typically send these statements after each patient encounter, and include information concerning the patient visit, including dates, providers' names, services received, and co-payments or deductibles. Some Town Hall participants, however, indicated that EOBs can be technical, confusing, or sent too long after the patient encounter to provide an effective warning of irregularities. However, many stakeholders, including Town Hall attendees, have suggested that EOBs may be an effective a tool in identifying medical identity theft. The HIMSS survey noted that 3.2 percent of respondents stated that their organizations had simplified their EOBs in response to the rise of medical identity theft.[16]

- **Potential Action:** Evaluate the effectiveness of various models of EOBs as a method of communicating with consumers by conducting customer surveys and focus groups. Explore applications currently available to send and manage EOBs electronically.

4.2.2 Resources for Victims and Organizations

Currently there is not a comprehensive centralized source of information on the topic of medical identity theft. Whether a provider organization wants to learn more information about what medical identity theft is, or a victim would like know what to do and where to go to handle the situation, this resource is yet to be developed. On the topic of general identity theft, the FTC has been recognized as the leading resource for stakeholders. The FTC provides extensive amounts of information on its website, as well as a consumer hotline on which to report instances of identity theft.[17]

Independent organizations and associations, such as the World Privacy Forum, the Identity Theft Resource Center, the American Health Information Management Association (AHIMA) and now ONC have developed some information and resources on medical identity theft. No centralized source, however, has been designated or emerged as a primary source of data. The concept of a national resource center has been used for many important topic areas, and could be beneficial to the stakeholders of medical identity theft. This center could provide a centralized database and location for consumers to visit to gather more information and guide them through any specific questions they may have. The resource center might provide materials to educate staff and consumers about their rights and assist in increasing awareness and understanding of the issue. These efforts could support the findings of two of the major themes of the Town Hall event: one, that more information is needed on the topic to address it fully; and two, consumers are most affected by medical identity theft and therefore most in need of resources to address it.

- **Potential Action:** Evaluate existing programs and tools that could serve as a starting point for developing a centralized resource to help support organizations and victims.

[16] Ibid.
[17] Federal Trade Commission. http://www.ftc.gov/bcp/edu/microsites/idtheft/.

4.2.3 Law Enforcement Resources

Law enforcement plays a critical role in the mitigation of the incidence of medical identity theft. Law enforcement investigation can assist in identifying thieves; prosecution can assist in collecting fines that can offset the cost of losses resulting from the incident; and the possibility of prosecution serves as a deterrent. Law enforcement officials may not, however, understand what medical identity theft is, the legal theories under which it can be pursued, the jurisdictional authority that may apply, or how to quantify damages. Law enforcement officials could benefit from resources to help them pursue and prosecute medical identity theft.

- **Potential Action:** Prepare educational materials and guidance for law enforcement officials on the methods in which medical identity theft might occur, impacts, forensics, and prosecution approaches.

To ensure that law enforcement officials are advised of incidents that may be appropriate for investigation and prosecution, health care organizations may want to focus on building a stronger communication infrastructure with law enforcement officials to refer incidents of medical identity theft effectively. Many state and federal agencies may be involved in the prosecution of medical identity theft. Some, like the HHS Office for Civil Rights (OCR), and Centers for Medicare and Medicaid Services (CMS) Office of E-Health Standards and Services (OESS), may not have direct roles in law enforcement but coordinate with law enforcement agencies. These agencies' enforcement authority is limited to investigating civil complaints of regulatory violation, although many also have the authority to refer allegations to other federal agencies that possess criminal jurisdictions. Others, like the Federal Bureau of Investigation (FBI), Criminal Division of the Department of Justice (DOJ), HHS Office of the Inspector General (OIG), and state Medicaid fraud control units and attorneys general may actually investigate and prosecute these crimes. In addition, the FTC enforces data protection and privacy laws and rules.

- **Potential Action:** Prepare educational materials and guidance for health care organizations about the federal and state agencies that may provide assistance for reporting medical identity theft.

It is important for all stakeholders to understand that the HIPAA Privacy Rule permits health care providers to disclose PHI to law enforcement officials, without the individual's written authorization, in certain circumstances, such as—

- "To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena
- To respond to an administrative request
- To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but the covered entity must limit disclosures …, and
- To disclose protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity. 45 CFR § 164.512(f)(5)."[18]

[18] 45 CFR 164.512(f)(1), (2), and (5).

- **Potential Action:** Prepare educational materials and guidance for health care organizations to explain permissible communications, and limitations on communicating with law enforcement agencies.

Local law enforcement agencies, such as police departments, may also assist effectively in combating medical identity theft. As highlighted by the Identity Theft Resource Center, a nonprofit clearinghouse of identity theft resources, it is imperative for a victim of medical identity theft to file a police report in his or her city and state of residence. A police report is critical in helping victims get rid of fraudulent debts and clear up their credit and will notify law enforcement that a crime may have been committed. Local agencies, however, are often not familiar with medical identity theft or may not have the resources to investigate it thoroughly. For example, in cases involving hacking and other cyber security breaches, investigation may require expertise and interagency collaboration that are beyond the scope of a local agency's resources. Increasing awareness and training on the various aspects of medical identity theft can help to integrate local law enforcement agencies into the process and could be beneficial in properly mitigating the issue.

- **Potential Action:** Provide local law enforcement agencies with educational resources for documenting and referring cases of medical identity theft appropriately.

Other law enforcement resources are available to victims of medical identity theft. There is not, however, one centralized entity that handles such cases. Some Town Hall participants advised that victims should file complaints with the attorney general in the state where the identity theft occurred. The National Association of Attorneys General provides state-by-state information on where to file these complaints.[19] Victims may also wish to check with state authorities for resources by visiting the National Association of Insurance Commissioners[20] and filing a complaint, as appropriate. In addition, victims have the option of filing a complaint with the Identity Theft Data Clearinghouse, operated by the FTC, and the Internet Crime Complaint Center.[21] Victims should file a report with the FTC, as well as the Social Security Administration (SSA),[22] if their SSN has been stolen or compromised. After obtaining a copy of their credit report, victims should immediately file a dispute regarding inaccurate or fraudulent information.

Although a wide variety of resources are available to victims of medical identity theft, they may not be aware of the existing options. Centralized resource centers and networks may be able to assist victims and prevent further harm by educating them on how to protect their identities once a breach has occurred, and how to work with law enforcement appropriately if their medical identity is actually stolen. It may also be beneficial to have a centralized unit for reporting medical identity theft incidents that would link victims to the proper authorities. Although a single process to handle all medical identity theft cases does not currently exist, having a single entry point to assist victims with connecting to resources could help to resolve instances of medical identity theft expeditiously.

[19] For more information visit http://www.naag.org.
[20] For more information visit http://www.naic.org.
[21] For more information visit http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html.
[22] For more information visit http://ssa-custhelp.ssa.gov.

- **Potential Action:** Provide patients with information and resources on which law enforcement agencies may be able to assist them in the event of medical identity theft and how they can be contacted.
- **Potential Action:** Identify a single point of entry for victims to report potential cases of medical identity theft that automatically helps them link to the proper authorities and corresponding recovery resources.

4.3 BUSINESS PROCESSES AND TECHNOLOGY

According to research from the World Privacy Forum, instances of medical identity theft frequently occur as an “inside job.”[23] Staff members who have access to information may abuse their access for fraudulent purposes. Although technology provides opportunities to advance productivity, accuracy, and consistency, it is critical that business processes and administrative policies are properly aligned to ensure oversight. Many stakeholders indicated that medical identity theft solutions include providing technical protections for privacy and security, but effectively addressing the problem will also require actions that affect policies, processes, and technology. During the research phase as well as during the Town Hall, it became apparent that in many organizations there is currently a “silo mentality” approach to internal business operations models. For example, in many organizations, financial departments work separately from security departments which work separately from clinical departments. Usually these departments do not have a reason to cross paths. However, by allowing departments to remain focused within themselves, a great deal of information may be lost or not used to its full potential. Coordinating resources and encouraging collaboration through business policies may eliminate the gaps in information that provide opportunities for medical identity theft to occur, addressing the knowledge gap that was a major theme of the Town Hall event.

Massachusetts General Hospital has begun implementing this approach to address cases of medical identity theft within its health system. The Data Integrity Group at Massachusetts General Hospital comprises representatives from across the organization such as the health information systems department, members from police and security, clinical departments as well as, radiology, EKG, lab, and patient registration members. This group meets to discuss any inconsistencies its members may see within their own work that may relate to the role of others in the hospital. Sometimes these issues may seem to affect only one group, but by providing an opportunity to discuss, members of the group begin to learn the work, expectations, and processes of other departments within their organization. For example, if the billing department receives a call from an individual claiming he or she received a bill for services not received, the billing department may follow up with the clinical department to determine whether the patient’s health record may indicate any type of inconsistencies. This type of cross-communication allows for better use of the processes and technology in place and closes the gaps where a breach might otherwise go unnoticed. This knowledge can also be used to leverage health IT better, a theme heard repeatedly at the Town Hall.

[23] Dixon, Pam. “Medical Identity Theft: The Information Crime that Can Kill You.” World Privacy Forum, Spring 2006.

- **Potential Action:** Develop communication tools for use among departments within stakeholder organizations to allow for cross-communication, and update business processes to incorporate this communication.

- **Potential Action:** Develop a model for data integrity management using current examples of hospital industry best practices.

4.3.1 Technology

To date, stakeholders have developed and implemented only a few technology solutions aimed at addressing medical identity theft. Town Hall participants noted the use of technology as a major theme. Given that technology solutions have proven effective in addressing other forms of fraud, medical identity theft stakeholders may wish to consider whether analogous approaches are available in their industries. The financial industry, for example, has demonstrated success in using technology to improve many of its business processes, especially in ensuring the privacy and security of transactions and communications. Financial entities use automated systems to conduct such privacy and security functions as monitoring behavioral spending patterns, identifying anomalies, verifying consumer identities, and gathering data about the individual to continue to strengthen the consumer's profile. These tools could function similarly in the health care industry.

Using technology to recognize inconsistencies in services requested and delivered, for example, can be used to detect fraudulent use of individuals' identities. Systems could review transactional records and detect such anomalies as the appearance of treatments for chronic conditions not previously diagnosed; increases in prescriptions that may indicate drug-seeking behavior; or attempts to receive care at multiple locations, all remote from the individuals' residences. These types of alerts would allow for further investigation to ensure that the consumer receives the appropriate care, and inconsistencies can be identified and handled appropriately.

This section discusses some types of technology advancements that can be explored or implemented to handle medical identity theft.

4.3.2 Auditing/Monitoring

Because an increasing number of health care transactions are conducted electronically, auditing and monitoring can be an effective method for detecting medical identity theft. When numbers of transactions are large, stakeholders may prefer to conduct some form of automated auditing and monitoring. The potential, under-explored uses of technologies like these were discussed among Town Hall participants.

In the information security context, the terms "auditing" and "monitoring" are often used interchangeably to refer to any automated process for reviewing information system activity and user activity within information systems.[24] The HIPAA Security Rule contains three separate provisions for conducting information system activity reviews,[25] monitoring logins,[26] and

[24] To some, "monitoring" refers to ongoing, continuous activity, whereas "auditing" may refer to activity conducted periodically or in response to specific events, such as the appearance of suspicious activity or a security breach.

[25] Specifically, to "regularly review records of information system activity, such as audit logs…." See HIPAA Security Rule, Sec. 164.308(a)(1)(D).

maintaining audit controls.[27] While distinct, these activities all involve reviewing electronic records of system and user activity and taking appropriate action if warranted.

Auditing provides several advantages to participants in health care transactions who may be concerned with detecting medical identity theft. Auditing can provide a means of detecting medical identity theft soon after its occurrence. Automated auditing may be especially effective in detecting anomalous high-volume activities, as when a single individual accesses an unusually large number of records in a single day. In this latter case, the activity may indicate what is sometimes called "wholesale" medical identity theft, where an insider downloads and sells many records. If auditing detects these events, data stewards may be able to take future corrective action by (for example) setting restrictions on the number of records that can be accessed and downloaded by individuals in particular roles within a preset period.

Auditing and monitoring are best implemented in conjunction with other controls. Access controls such as role-based access, for example, limit access to information based on individuals' roles and responsibilities. In a role-based access environment, auditing and monitoring can more easily identify the point of failure that may have resulted in a privacy or security breach. Another approach to maximizing the effects of auditing and monitoring is to provide staff notice that their actions are being monitored. Notification alone can serve as a deterrent to staff that would otherwise be willing to access and exploit PHI. In this sense, auditing and monitoring may serve as a prevention measure as well as a detection and remediation measure.

In addition, a number of federal initiatives are in place that are designed to detect and prevent fraud within the Medicare and Medicaid programs. The Zone Program Integrity Contractors (ZPIC) have been created to perform program integrity functions for Medicare Parts A, B, C, D; Durable Medical Equipment; Home Health and Hospice; and the Medi-Medi program. Similarly, Congress recently mandated, and the CMS is currently implementing, the Medicaid Integrity Program (MIP). MIP represents CMS' first national strategy to detect and prevent Medicaid fraud and abuse in the program's history. There are two broad operational responsibilities under this new program: reviewing the actions of those providing Medicaid services; and providing support and assistance to the states to combat Medicaid fraud, waste, and abuse.

One of the fundamental components of these anti-fraud programs is to identify program vulnerabilities that may be susceptible to unscrupulous activity, and to isolate aberrant items related to those vulnerabilities. Given that the combined Medicare and Medicaid enrollment in these programs is more than 104 million beneficiaries, the ZPIC and MIP efforts represent an existing opportunity to mine claims and enrollment data against algorithms designed to detect possible cases of medical identify theft.

Auditing and monitoring was generally acknowledged by participants at the Town Hall as an appropriate and effective measure. Participants on the Town Hall panel discussing laws, policies,

[26] Login monitoring is defined as maintaining "[p]rocedures for monitoring log-in attempts and reporting discrepancies" (HIPAA Security Rule, Sec. 164.308(a)(5)(ii)(C)). HIPAA does not explicitly require that the actual monitoring be automated, although an automated approach would seem to be the most effective method of detecting inappropriate attempts at gaining electronic access. The login monitoring requirement is an addressable implementation specification of the Security Rule.

[27] Covered entities must "[i]mplement hardware, software, and/or procedural mechanisms that record and regularly review records of information system activity, such as audit logs…." See HIPAA Security Rule, Sec. 164.312(b).

and procedures cited these approaches with approval. Participants noted, however, that this is one of the more technical approaches to the problem, and many stakeholders do not fully understand the options and solutions available to implement these types of protections.

- **Potential Action:** Identify best practices for auditing and monitoring that are applicable to medical identity theft.
- **Potential Action:** Explore opportunities to tailor auditing and monitoring for identifying medical identity theft in the Medicare and Medicaid populations using existing contract vehicles.

4.3.3 Patient Authentication

Many stakeholders in medical identity theft have noted that patient authentication can be one of the simplest yet most effective methods in preventing medical identity theft. Patient authentication consists of ensuring that patients receiving services are the individuals they claim to be. Currently, few providers require any strong evidence of patient identity at the point of service. Patients are often asked to provide only verbal assertions of identity and coverage. However, technology solutions such as biometrics, smart cards, or electronic patient records may be able to assist providers in verifying patients’ identities based on past histories, demographics, or facial photographs. The potential use of patient authentication to combat medical identity theft was part of the theme of health IT that emerged at the Town Hall event.

Patient authentication can address medical identity theft at a number of points in the health care delivery chain. Identities can be verified when patients seek medical care; when they make claims for insurance payments; or when they request copies of their medical records. Town Hall participants noted that these approaches will not prevent all instances of medical identity theft but may be a helpful deterrent.

However, in some cases patient authentication practices can render medical identity theft victims worse off. For example, if medical identity thieves present forged or stolen credentials and they are accepted, medical identity theft victims can be hard-pressed to prove they were not the recipients of the services provided. Patient authentication mechanisms must anticipate these potential conflicts and identify ways to resolve them.

Although verifying a patient’s identity at the point of service will not combat all forms of identity theft, it can help to reduce the risk of imposters receiving services. Town Hall participants and others have noted that a relatively low-burden method of patient authentication such as asking patients to present photo identification may serve as an effective safeguard against some forms of medical identity theft. Some health care facilities that request to see identification have noted that some attempted medical identity thieves seem to be effectively deterred by requests for identification. Other low-tech approaches concern asking the patient to demonstrate knowledge of their demographic information, previous services received, or a password. These latter approaches, however, are perhaps too easily circumvented by a medical identity thief, and therefore do little to deter them while making health care access slightly more difficult for all patients.

Some health centers have implemented biometrics for patient authentication. The Advanced Ambulatory Surgical Center in Chicago, for example, uses a biometric identity management solution that scans each patient's index finger using high frequency sound waves. The fingerprint scan associates the individual with his or her pre-existing medical record.[28]

Another technological approach to patient authentication involves smart cards. This approach is currently in use at Elmhurst and Queens Hospitals in Queens, New York. The Smart Card Alliance notes, "Each patient in this network carries a card that contains data such as the patient's name, address, emergency contacts, allergies, current medications, and recent lab results."[29] To verify their identity, patients' cards are scanned similar to the way credit cards are scanned. Therefore, a medical identity thief cannot assume the patient's identity unless the thief has the individual's smart card as well as knowledge of the personal identification number (PIN) often used in conjunction with smart card technology. These protections will prevent potential medical identity thieves from using another's identity in cases of nonconsensual medical identity theft.[30]

- **Potential Action:** Develop metrics and studies to assess the effectiveness of various types of new patient authentication practices combined with cost-benefit analyses to determine the appropriate threshold for investment and implementation.

4.3.4 Incident Response

While prevention and detection of medical identity theft are important, both can minimize but not eliminate the possibility of its occurrence. All stakeholders, therefore, should at minimum be aware of the existence of medical identity theft and have a plan in place to respond to it appropriately when it occurs. As with other appropriate controls, maintaining an incident response plan poses no new burden to HIPAA-covered entities, which are required to implement policies and procedures for incident response and are further required to "identify and respond to suspected or known security incidents; mitigate to the extent practicable, the harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."[31] In advance of an incident, best practices include assembling an incident response team with an appropriate set of skills to handle the incident, including executive management, IT staff, compliance specialists, privacy and security specialists, communications and public relations staff, and records management specialists. Smaller entities may not be able to maintain full-time positions for these functions but are still able to develop a response plan in advance of an incident to ensure that its response will be as rapid and effective as possible. All entities may also benefit by documenting incident response roles, responsibilities, policies, and procedures, to ensure consistency, efficiency, and clarity. Staff new to the organization or their roles, for example, can learn their roles quickly and share an understanding with existing staff if these responsibilities are clearly and accurately described in policies and procedures documentation.

- **Potential Action:** Develop model incident response plans for medical identity theft based on current best practices. Ensure the model plan is adaptable and scalable to health care providers, insurers, health information data processors, and other stakeholders, and to entities of various sizes with differing staff and other resources.

[28] Akridge, Jeannie. "Closing the safety loop with auto patient ID." *Healthcare Purchasing News,* January 2005.

[29] Smartcard Alliance. "Smart Card Applications in the U.S. Health Care Industry." *Smartcard Alliance Newsletter,* February 2006. Retrieved November 2008, http://www.smartcardalliance.org/newsletter/february_2006/feature_0206.html.

[30] Ibid.

[31] HIPAA Security Rule, Sec 164.308(a)(6)(i)).

4.4 POLICIES AND LAWS

Many existing federal laws require organizations to take actions that will address medical identity theft as well as other forms of privacy and security concerns. In order to comply with these laws, many of these organizations must also develop internal policies to implement these requirements more specifically.

4.4.1 Organizational Risk Assessment

One technical approach to addressing medical identity theft is its inclusion in risk assessment methodologies that are critical to the effective development and implementation of health information systems. Risks assessments are required under both HIPAA (for HIPAA-covered entities) and the federal information security management act (FISMA, for federal agencies),[32] although organizations covered by these laws may need to develop specific, internal policies for their implementation.

Risk assessment can assist stakeholders in developing appropriate policies and infrastructure to address prevention, detection, and remediation. A risk assessment is a process used to identify and assess factors that may threaten the success of a program or achievement of a goal. A more precise definition of a risk assessment – one which is binding on most federal agencies and that is often voluntarily used in the private sector as well -- is given by the National Institute of Standards and Technology (NIST): “the process of identifying risk to agency operations, agency assets, or individuals arising through the operation of the information system.”[33] The risk analysis process can help to define preventative measures to reduce the likelihood of risks occurring, and to identify solutions for addressing occurrences to mitigate their effects. A recent survey sponsored by HIMSS states that “[i]n order to secure electronic medical information, it is necessary for health care organizations to actively understand the kinds of risks that their organizations might face. [Many respondents to the survey] are meeting this challenge head on, as demonstrated by the three-quarters reporting that their organization conducts a formal risk assessment.”[34]

Not only is a risk assessment a requirement of the HIPAA Security Rule,[35] it is the groundwork for a strong privacy and security program for health care providers. Risk assessments can be conducted at the program level but are also necessary and effective to determine whether the privacy and security controls of a particular IT system need to be modified or enhanced.

[32] FISMA requires that federal agencies ‘‘(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through … assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;” FISMA< 44 USC 3544(a)(2).

[33] NIST Special Publication (SP) 800-30. *Risk Management Guide for Information Technology Systems,* July 2002, provides guidance, mandatory for federal agencies on how to conduct a risk assessment.

[34] HIMSS. HIMSS Security Survey Sponsored by Booz Allen Hamilton, October 2008 (available at http://www.himss.org/advocacy/d/HIMSS_SecurityReport102408.pdf).

[35] See HIPAA Security Rule, Sec. 164.308(a)(1)(ii)(A). Note that the HIPAA Security Rule uses the term “risk analysis.” The specific requirement, however, is to “[c]onduct an accurate and thorough *assessment* of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information” (emphasis added). The HIPAA Security Rule also requires that the risk analysis address administrative, physical, and technical safeguards. See 45 CFR Parts 160 and 164, subparts A and C.

In an early phase of conducting a risk assessment, analysts must identify as many possible sources of risk as they are able. In the health care industry, however, medical identity theft is not universally understood as a significant risk and is not consistently included in risk assessments.

- **Potential Action:** Develop model risk assessment modules for medical identity theft; these modules may require several templates to address the threats and vulnerabilities specific to each stakeholder group. The risk assessment module may, for example, include questions about possible motivations for medical identity theft; the stakeholder's particular environment; an assessment of the likelihood of the frequency of medical identity theft; and the possible impacts on data accuracy, patient care, and costs.

4.4.2 Notification to Individuals

Many Town Hall participants expressed that another effective response to medical identity theft is the practice of notifying potentially affected individuals. This perspective is reflected by the broad adoption of state laws requiring such notification. At least 44 states currently require companies to advise individuals when their records may have been compromised.[36] California was the first state to pass such a notification law, and many of the states that have subsequently adopted comparable laws have used similar language and provisions. Because California recently amended its law to explicitly include health care organizations among those required to notify customers of a breach, many believe that other states will do so as well. Consideration of consumers' needs, including the need to know about such incidents, was a recurring theme at the Town Hall event.

These laws create requirements related to responding to medical identity theft, but it is not known whether they serve a significant deterrent or mitigation effect. One report released in 2008 suggested that these laws have no statistically significant impact in reducing identity theft.[37] Providers are also challenged to develop effective methods of ensuring that notifications are sent to the victim and not to the medical identity thief if he or she has altered the patient's address as reflected in the health record. However, this type of legislation may help to provide an incentive for companies to improve their security controls and also allow consumers to make informed decisions about their individually identifiable information. As it relates to medical identity theft, these laws would increase patients' awareness of the use and disclosure—including inappropriate disclosure—of their health care data. Once patients become aware of these security incidents, they can take steps to monitor their financial and health care records, and more quickly control the financial implications related to the issue.

Town Hall participants also shared that in creating these requirements, legislators and other stakeholders should take precautions so that potential victims are not notified too frequently, as in cases where data has been handled inappropriately, but no identity theft has been detected and is unlikely. If organizations communicate these risks too frequently to consumers, consumers may ignore these notices, or become needlessly concerned. Stakeholders that create policies for delivering these notices should therefore set standards that are neither too restrictive nor too expansive.

[36] National Conference of State Legislatures. State Security Breach Notification Laws as of November 4, 2008, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

[37] Sasha, Romanosky; Rahul Telang; and Alessandro Acquisti. "Do Data Breach Disclosure Laws Reduce Identity Theft?" Seventh Workshop on the Economics of Information Security, Hanover NH, June 25–28 2008.

- **Potential Action:** Determine whether state laws requiring notifications to potential victims of medical identity theft affect outcomes such as more immediate detection; increased stakeholder ability to mitigate effects; or lowered financial costs associated with medical identity theft.
- **Potential Action:** Develop model state legislation for addressing notification to consumers in the event that medical identity theft is detected or strongly suspected to minimize variation among states.

4.4.3 Patient Amendment

Inaccurate patient health records are one potential consequence of medical identity theft. If an individual receives health care using the identity of another, the fraudulent individual's information can become entered in the victim's health record. When victims discover inaccuracies (whether caused in the course of medical identity theft or otherwise), they have the right under HIPAA to request an amendment to their health records.[38] Victims of medical identity theft normally work directly with their provider to have the inaccurate health record reconciled appropriately. HIPAA covered entities must comply with the law, and must also develop policies and procedures setting out how they will accomplish these requirements.

Under the HIPAA Privacy Rule, when a patient requests an amendment to his or her health record, the provider must make it unless the request meets one of a few narrow exceptions. In cases where the provider is permitted to deny the request, HIPAA provides the patient with the right to have a "statement of disagreement" added to the health record. The Rule provides limited guidance, however, on how that amendment must be made. In many instances, state law may place constraints on the provider. Some state laws require that information cannot be removed from a health record, but may only be marked as incorrect. In an electronic environment, however, systems requirements must ensure that this annotated data cannot be misinterpreted, re-integrated, or otherwise continue to affect the data integrity of the health record.

- **Potential Action:** Identify best practices in amending health records that meet the requirements of all state laws regarding health records.

4.4.4 Guidelines for Data Protection

Town Hall participants agreed that while much guidance exists on responding to security and privacy breaches, the best solution is to prevent it by implementing appropriate safeguards. Protecting health records against medical identity theft requires a consideration of the many risks that can lead to the problem. As described previously, a risk assessment should precede identifying and selecting safeguards and will help in designing security and privacy programs that are cost-effective and that do not hinder the organization's operations. It is important to properly safeguard this health data because it can be used for quality improvement, public health and research, and may be very necessary for making improvements in health care initiatives. As

[38] "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." HIPAA Privacy Rule § 164.526(a)(1), Amendment of protected health information. Some limited exceptions to the requirement apply.

health IT continues to develop, health data will continue to become more readily available.[39] However, it is important to note that if this information is corrupted as a result of a case of medical identity theft, these public health initiatives and researchers may be using incorrect data. The AHIMA refers to this as the "cascading effect" of medical identity theft.

As in the financial services industry, the health care industry handles large volumes of transactional data, and stakeholders have examined the financial sector to obtain privacy and security best practices. The "red flags" approach, for example, has established a protocol for identifying suspicious patterns of activity and determining the appropriate steps to respond to anomalies. Having identified this approach as valuable and effective, the FTC, the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued new regulations called the Red Flags Rules requiring financial institutions and creditors to develop and implement identity theft prevention programs pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003. Such programs must be developed to identify, detect, and respond to patterns or activities that could indicate identity theft. Among other affected entities, "creditors" (as defined by the Red Flag Rules) must comply, and many health care organizations may fall under this definition. Because government entities may defer payment for goods and services, they too fall into this category and have the responsibility to comply with the Red Flags Rules.[40] These new requirements may have a significant effect in the near future on how medical identity theft is detected.

These Red Flag Rules will ultimately encourage creditors and others covered by the requirements to develop more sophisticated and effective identity theft detection programs. Town Hall panel participants noted that this requirement represents mandating of a best practice, and that these creditors and financial institutions will benefit from a program in place that allows them to identify, detect, and respond to the red flags of identity theft. In the longer term, monitoring the success of the red flags selected would also allow businesses to further evaluate their particular operations to determine how identity theft is arising and how to appropriately respond. Stakeholders at the Town Hall were in agreement that this type of approach has the advantage of being scalable and adaptable. Entities can identify their own "red flags" that are appropriate for their size, complexity, and the nature and scope of their activities in conjunction with existing best practices. Businesses could ultimately comply by developing a fairly simple and straightforward Red Flags program.

Another data protection method concerns issuing new account information. Credit card companies have benefited from the ability to reissue new credit card numbers to consumers after their credit card has been compromised by identity theft or fraud. This response prevents any future transactions from occurring on the affected account and can greatly assist with preventing additional harm. Although insurance cards and credit cards function differently and serve a

[39] National Committee on Vital and Health Statistics. Report to the Secretary of the U.S. Department of HHS. *Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data,* December 19, 2007. Available at http://library.ahima.org/xpedio/groups/public/documents/government/bok1_036300.pdf#page%3D1. Website accessed on January 9, 2009.

[40] "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft" June 2008. http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm.

different purpose, insurance companies would benefit from being able to apply this simple, relatively low-cost response.

In some situations, however, insurers do not currently have this option. If the victim is a Medicare patient, for example, the CMS is not able to change the Medicare account number because it uses the digits of the individual's SSN, and SSNs are very difficult to change. Because of this issue, even after a case of medical identity theft has been detected, medical identity thieves are sometimes able to continue to obtain care and submit claims using the same Medicare account number.[41]

In May 2007, the Office of Management and Budget (OMB) directed all federal agencies to develop and implement a plan to eliminate the unnecessary use of SSNs.[42] The OMB guidance was based largely on the findings and recommendations of the President's Identity Theft Task Force. Because the SSN is considered to be the most valued of all possible items of personal information for an identity thief, the President's Identity Theft Task Force recommended that federal agencies reduce the unnecessary use of SSNs. Eliminating the use of SSNs as identifiers by patients and providers can help to prevent additional exposure of this information. Along with reducing the use of SSNs, the Identity Theft Task Force also recommended issuing guidance on the appropriate usage of SSNs and establishing best practices that minimize the use of SSNs.

- **Potential Action:** Develop guidance on best practices from the financial services industry for implementing "red flags" methodologies and other preventive measures specific to medical identity theft.

- **Potential Action:** Survey current use of SSNs and identify methods for reducing the use of SSNs or using other identifiers in their place.

One challenge to developing a coordinated response to medical identity theft is that state law varies widely. This issue is important to consider because it may obstruct interoperability when information is shared between varying states and restrict access to certain areas of a patient's record.[43] A recent report of the National Committee on Vital and Health Statistics (NCVHS) explained that many groups, such as HISPC, have done a great deal of work to determine where state laws have clear differences in their rules and guidelines. By taking a closer look at this information, stakeholders involved in mitigating the risk of medical identity theft will be able to identify where current state laws are more stringent than HIPAA and how state laws differ. In addition, NIST has developed its *Security Guide for Interconnecting Information Technology Systems*, which details a "life-cycle management" approach for interconnecting IT systems that are owned and operated by different organizations.[44] These guidelines are also consistent with the requirements listed in OMB Circular A-130, Appendix III, for system interconnection and information sharing. Because information is typically most vulnerable in transit, it may be beneficial for agencies to refer to this framework when developing their systems and tailoring the guidelines to meet their specific needs.

[41] Consumer Union. *Social Security Numbers on Medicare Cards puts Consumers at Risk for Identity Theft*, October 2004.

[42] Social Security Number Reduction Effort. http://www.privacy.va.gov/ssn.asp.

[43] U.S. Department of Health and Human Services, HIPAA Frequent Questions. "Does the Privacy Rule preempt State Laws?" December 11, 2006, http://www.hhs.gov/hipaafaq/state/399.html.

[44] NIST Special Publication (SP) 800-47. *Security Guide for Interconnecting Information Technology Systems*, August 2002. http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf.

- **Potential Action:** Review previous efforts at identifying differences among state laws, as well as guidance on developing broadly-available networks, and describe aspects of a system for interconnecting health organizations that includes functionalities for preventing, detecting, and remediating medical identity theft that also satisfies as many existing requirements and best practices as possible. This effort may include identifying any conflicts among these authorities and recommending best practices where such conflicts exist.

NCVHS also stated that health care stakeholders must understand the appropriate ways of using and maintaining data, and assign proper data stewardship. This is important for ensuring that individuals are aware of how their health data may be used and to build trust throughout organizations. Education and awareness regarding data stewardship is needed to ensure these privacy procedures are in place. Proper maintenance of data can help to prevent the information from being misused for the purpose of medical identity theft or other harm. In response to this issue, NCVHS developed several recommendations for enhanced data protections as they relate to health IT. They state that protections should improve education, quality, communications,

As detailed by the World Privacy Forum[45] and AHIMA,[46] health care professionals have many options for helping to protect the medical records that they maintain and decreasing the number of medical identify theft incidents each year. By taking the necessary precautions and establishing strong data protection processes they can better safeguard and maintain data. Recommendations include administrative, technical, and physical controls, many of which echo the requirements of the HIPAA Privacy and Security Rules but that will have specific effects on medical identity theft.

Many of the items listed above are also echoed throughout NIST Special Publication 800-37, NIST’s *Guide for the Security Certification and Accreditation of Federal Information Systems*. The guidelines provided in that document were developed to help achieve more secure information systems throughout the Federal Government by establishing consistency with the risk assessment process, promoting a better understanding of the risks associated with information systems, and focusing on training and awareness.[47]

- **Potential Action:** Develop guidance for health care providers that reflects a consensus view of best security and privacy practices for preventing, detecting, and mitigating medical identity theft.

As discussed in previous sections, empowering consumers to have a greater role in protecting their identities may have a signification impact on this issue. By taking steps to protect their personal data such as shredding mail, restricting access to their information, and being aware of their rights can help consumers to take a more significant position in data protection.

[45] Dixon, Pam. “Medical Identity Theft: The Information Crime that Can Kill You.” World Privacy Forum. May 3, 2006.
[46] Apgar, Chris et al. “Mitigating Medical Identity Theft.” *Journal of AHIMA*, July 2008, p. 63–69.
[47] NIST Special Publication (SP) 800-37. *Guide for the Security Certification and Accreditation of Federal Information Systems*. May 2004. http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf.

5.0 SUMMARY

Medical identity theft is an issue that has the potential of having significant health care and financial implications for all health care stakeholders. Although the true magnitude of the problem remains to be quantified, the information that is available on current cases is serious enough to demand a look at what can be done now and what can be done in the future to better understand the problem. It is understood that addressing all of these potential actions collectively may not be feasible. They are intended to be suggestions affected organizations can select based on feasibility and correlation to their specific requirements. Table 1 provides a summary of the suggested potential actions that were identified throughout this paper. In light of the fact that there is limited knowledge on this topic, these suggestions cover a broad spectrum of potential actions and stakeholder involvement.

Table 1: Summary of Potential Actions

Category	Potential Actions In Summary
Leadership	1. Establish a public-private task force, a formation and membership of public and private entities, under government leadership to focus on medical identity theft
	2. Review and analyze the processes used to respond to financial identity theft and consider developing a similar approach for responding to medical identity theft
	3. Develop strategies and an approach, at a national level, to further identify and classify risks related to medical identity theft for all stakeholders, and to address these risks.
Education	1. Conduct systematic, structured scientific-based surveys on the frequency of medical identity theft.
	2. Take a risk management approach, to identify, classify, and potentially quantify the impact of medical identity theft, develop mitigation strategies, and identify tools, techniques, and controls appropriate for specific applications.
	3. Use data analytics to review existing data sets such as claims and collections, and credit reports to provide better estimates about the magnitude of medical identity theft
	4. Identify effective mechanisms and best practices used in the financial industry for educating consumers about medical identity theft
	5. Develop appropriate educational programs about medical identity theft for consumers, health care payers, health care professionals, and law enforcement
	6. Identify existing health literacy programs that can be expanded to include information on medical identity theft to help educate and raise consumer awareness.
	7. Integrate education on medical identity theft as part of employee communications at provider organizations; include information on medical identity theft in patient education materials.
	8. Develop clear, accurate resources for HIPAA covered entities, which clarify how they can comply with the HIPAA Privacy Rule's access requirements in cases of possible medical identity theft.
	9. Evaluate the effects of providing real-time access to patient records on the detection of medical identity theft.
	10. Evaluate the effectiveness of various models of EOBs as a method of communicating with consumers by conducting customer surveys and focus groups. Explore applications currently available to send and manage EOBs electronically.

Category	Potential Actions In Summary
	11. Evaluate existing programs and tools that could serve as a starting point for developing a centralized resource to help support organizations and victims.
	12. Prepare educational materials and guidance for law enforcement officials on the methods in which medical identity theft might occur, impacts, forensics, and prosecution approaches.
	13. Prepare educational materials and guidance for health care organizations about the federal and state agencies that may provide assistance for reporting medical identity theft.
	14. Prepare educational materials and guidance for health care organizations' to explain permissible communications, and limitations on communicating with law enforcement agencies.
	15. Provide local law enforcement agencies with educational resources for documenting and referring cases of medical identity theft appropriately.
	16. Provide patients with information and resources on which law enforcement agencies may be able to assist them in the event of medical identity theft and how they can be contacted.
	17. Identify a single point of entry for victims to report potential cases of medical identity theft that automatically helps them link to the proper authorities and corresponding recovery resources.
Business Processes and Technology	1. Develop communication tools for use among departments within stakeholder organizations to allow for cross-communication, and update business processes to incorporate this communication.
	2. Develop a model for data integrity management using current examples of hospital industry best practices.
	3. Identify best practices for auditing and monitoring that are applicable to medical identity theft
	4. Explore opportunities to tailor auditing and monitoring for identifying medical identity theft in the Medicare and Medicaid populations using existing contract vehicles.
	5. Develop metrics and studies to assess the effectiveness of various types of new patient authentication practices combined with cost-benefit analyses to determine the appropriate threshold for investment and implementation
	6. Develop model incident response plans for medical identity theft based on current best practices.
Policies and Laws	1. Develop model risk assessment modules for medical identity theft
	2. Determine whether state laws requiring notifications to potential victims of medical identity theft affect outcomes.
	3. Develop model state legislation for addressing notification to consumers in the event that medical identity theft is detected or strongly suspected to minimize variation among states
	4. Identify best practices in amending health records that meet the requirements of all state laws regarding health records.
	5. Develop guidance on best practices from the financial services industry for implementing "red flags" methodologies and other preventive measures specific to medical identity theft.

Category	Potential Actions In Summary
	6. Survey current use of SSNs and identify methods for reducing the use of SSNs or using other identifiers in their place.
	7. Review previous efforts at identifying differences among state laws, as well as guidance on developing broadly-available networks, and describe aspects of a system for interconnecting health organizations.
	8. Develop guidance for health care providers that reflects a consensus view of best security and privacy practices for preventing, detecting, and remediating medical identity theft.