Creating a Trusted Environment: Reducing the Threat of Medical Identity Theft

HIMSS Privacy & Security Task Force
June 2012

Neither HIMSS, the authors or editors of this white paper accept any liability for actions taken by readers of this document or their organizations.

The information provided to you in this document is not intended to be legal advice or to provide recommendations for an organization's specific circumstances. Please consult a lawyer or other appropriate expert for professional assurance before taking any action.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper examines the ways in which individuals and entities involved in the delivery of healthcare services, supplies and equipment can effectively safeguard their patients' Protected Health Information (PHI) without inconveniencing the patient or disrupting workflows. Healthcare providers and emerging Accountable Care Organizations, health plans, financial institutions, health IT vendors and others represent some of the effected communities. This paper will consider the risks and recommend mitigation strategies for a variety of work environments, including point-of-service, electronic health information exchange, and cyberspace. It also will discuss ways in which provider and vendor risk, and personal, physical, administrative and financial security may be addressed. It was written for those who have a basic understanding of privacy and security laws, and may be especially helpful for those new to administrative duties involving PHI or individuals interested in refreshing their knowledge of mitigation strategies against threats to PHI, particularly in an electronic environment.

Medical identity theft has been called one of the fastest growing crimes in America. Its impact can range from simple inconvenience to legal woes, financial devastation, even death. According to a report released from the Ponemon Institute, a privacy and security research firm, medical identity theft is a $30 billion a year crime in the United States[1] – and growing. The past five years have seen an 800 percent increase in the number of incidents reported[2]--and those are just the ones we know about. Among individuals surveyed for the Ponemon study, only half said they reported the theft to authorities. A full 50 percent said they did not report their medical identity stolen, often because they knew the person who had perpetrated the crime or because they did not think any personal harm had been done to them.

The perception of "no harm done" may be a reflection of the length of time it frequently takes for an individual to become aware their medical identity has been stolen. By the time the victim becomes aware of the crime, the level of harm can be devastating. A video circulating on YouTube[3] tells the story of a woman who nearly lost custody of her four children after a woman who had bought the victim's medical identity from a thief gave birth to a drug-addicted baby and was reported to authorities.

In another example, a woman opened her mailbox to find a bill from a local hospital for the amputation of her right foot. When she walked into the surgeon's office and showed them that her right foot had obviously not been amputated, she discovered her identity had been stolen by someone who had used her Social Security number, her address and her insurance ID number to have the surgery. Although she was able to clear her name in this instance, when she was hospitalized for a hysterectomy a year later, she discovered that medical identity theft is the gift that keeps on giving. The nurse reviewing her chart commented, "I see you have diabetes." She doesn't; the medical identity thief's information had become intermingled with her own. "I now live in fear that if something ever happened to me, I could get the wrong kind of medical treatment." she said.[4]

Medical identity theft can take many forms: it may involve the large-scale theft by computer hackers, as recently experienced by the Utah Medicaid office[5] where the breach is believed to have been committed by someone located in Europe; it is a crime of opportunity that can happen when your wallet is stolen and the thief uses your insurance card; or a friend or family member who has access to your personal information may use it with or without your knowledge to gain access to care. Protecting our own personal health information is the first line of defense against medical identity theft. Healthcare providers are the second. They not only have a moral obligation to play this role; there are state and federal laws that require them to do so.

This white paper represents the collaborative effort of HIMSS members across a broad spectrum of enterprises whose day-to-day activities demand their attention to these topics, including representatives from the healthcare, banking, insurance, cyberspace and risk mitigation industries.

This report will evaluate risk and mitigation strategies under two major sections. One section will provide an overview of concerns related to two of the three fundamental areas of security management which are critical to managing identity theft—physical and administrative security. This section should help orient the reader not already familiar with the security landscape. Other important topics, such as technical security, are beyond the scope of the present paper and is covered in-depth in many publications. The National Institute of Standards and Technology website (www.nist.gov), in particular, has many excellent papers and security management tools available for free download.

The second major section of this paper will explore risk management issues in specific areas of opportunity for identity thieves. These areas include provider/vendor relations, electronic health information exchanges, cyber security, point of service security and financial security. The sections will have some purposeful overlap as needed with the broader sections. This will aid readers looking for guidance in addressing such concerns and responsibilities in their own organizations.

INTRODUCTION

The Ponemon Institute estimates the cost of medical identity theft at $30 billion a year[6]. As ominous as that figure is, the costs associated with medical identity theft go far beyond its measurable economic impact. When a person's medical identity is stolen, it is stolen for the purpose of being used. The person using the stolen identity will never have the same medical history as the victim, and may not even share the same blood type.

Healthcare is a "high touch" and time-sensitive service. Patients and providers may need immediate access to treatment rooms, prescription medication and personal health information (PHI). Consider the implications should the victim require emergency medical care. Records become intermingled. Examples of the types of questions this might raise include: What if the victim has a medical condition or allergy not noted in the most recent treatment documents associated with the care received by the individual who stole or "borrowed" the victim's medical identity? What are the legal, economic and reputational risks for the provider?

Finally, what are the chilling effects of story after story of medical identify theft and data breaches on the progress toward the "trusted environment" which is the foundation of leveraging electronic health information exchange, electronic health records, comparative effectiveness research and predictive modeling to improve outcomes. Perhaps most troubling, and in contrast to financial identity theft, there is simply no sure-fire way to remediate medical identity theft. Once a theft is detected, a compromised patient will never be sure that the issue will not resurface, potentially in a life-threatening manner.

Physical security is a broad term that addresses the basic need to keep PHI safe from those who would attempt to steal it or use it inappropriately. A foundational step in providing physical security is ensuring administrative security. To the extent possible, those who will have access to PHI should be carefully screened. Once screened, all those with access to PHI should be trained to understand how to protect this information and the consequences of failing to do so. Administrative vigilance is crucial to ensure that these procedures are continually enforced and monitored.

Healthcare delivery is in the midst of being redefined. It is no longer simply a matter of physically going to the doctor's office. Online portals, smartphones, tablets, kiosks, in-store clinics—the delivery of healthcare is now an ongoing feast of vulnerabilities for identity theft. The ability to authenticate an individual's identity and verify that identity each time they access service is now more important and complex than ever. Further, if we want to encourage the patient's direct engagement in their care, processes must not deter patient access. The risk of a given transaction must be assessed with an appropriate level of authentication or verification determined. The results should be carefully monitored, evaluated in terms of effectiveness and consumer satisfaction.

In terms of Accountable Care Organizations (ACO), Patient-Centered Medical Homes (PCMH) and Health Information Exchanges (HIEs), the goal of the electronic medical record is to make it possible for a provider to have the patient's full medical picture in front of them at the time of the interaction. Achieving this goal requires that the data be accessible across a cyber-network to both patients and providers. The more we share data, the more it will be an irresistible target for organized and sophisticated identity thieves. Virtual sharing of PHI requires a foundation of multi-factor authentication that supports compliance, information, security and operational functions. Fortunately, affordable and strong biometric-based solutions are being implemented today.

Lastly, there has been a paradigm shift in the profile of healthcare as a target for identity thieves, including cyber criminals. As healthcare currently represents 18 percent of gross national product (GNP), the way we think about prevention needs to shift radically[7]. While the bulk of identity thefts and breaches will continue to be "inside" jobs, there also exists a threat from a new breed of outside players—organized crime organizations, hackers and foreign entities. In April 2012, the Utah Department of Health experienced a security breach compromising the PHI of nearly 200,000 Medicaid recipients when eastern European hackers broke into an inadequately protected computer server.[8]

We tend to think of these threats as something the government "deals with," but that would be a mistake. With the explosion in cloud computing, responsible parties must constantly be cognizant of these threats and put in place procedures to address these vulnerabilities proactively. In cloud computing, the websites and applications used are not stored on the user's computer hard drive, but instead stored on a remote server that allows access online. While this greatly improves the convenience of accessing data, it dramatically reduces direct control over its security.

Although medical identity theft is a serious and increasingly common occurrence, there are best practices and solutions, both established and emerging from across the business spectrum that can serve as powerful tools in its prevention. A proactive approach will help to prevent the economic, reputational and patient harm that results from medical identity theft and data breach, as well as support the trusted environment necessary to drive affordable quality healthcare.

PHYSICAL AND ADMINISTRATIVE SECURITY OVERVIEW

PHYSICAL SECURITY

Controlling physical access to patient data, particularly unauthorized access, is an important consideration for healthcare organizations. Physical access involves individuals gaining access to such areas as offices, files, workstations and the loss or theft of portable devices, such as laptops or cell phones among other areas where PHI may be found.

In the 2012 HIMSS Analytics' *Security of Patient Data*[9] report, commissioned by Kroll Advisory Solutions, 56 percent of those respondents who indicated their organization experienced a breach within the past 12 months reported the source of breach was due to unauthorized access by an employee. One-third was due to wrongful access of paper-based patient information, while another nine percent involved improper destruction of paper-based records. A surprising 2 percent cited a second-hand computer from which data was not removed as the source of the breach. Only 3 percent of breaches involved a network breach by an outsider.

The Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."[10] The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) further expands HIPAA's requirements to include PHI in paper records. The physical security requirements include standards on the following: facility access controls, workstation use, workstation security, and device and media controls.

The Security Rule covers major elements of security compliance for most healthcare organizations, although there are certain state laws that also include physical security requirements. For instance, Massachusetts statute 201 CMR 17.00[11] applies to any business that owns licenses and/or receives, maintains, processes or otherwise has access to personal information about a resident of Massachusetts. The law requires such businesses to implement a comprehensive security program for the security, integrity and confidentiality of paper and electronic records. The requirements do include a provision to place reasonable restrictions upon physical access to records containing personal information and storage of such records and data in locked facilities, storage areas or containers.

Although many view the purpose of these requirements to be the protection of an individual's privacy, it also provides critical elements for guarding against medical identity theft. Physical security safeguards have the greatest impact in preventing medical identity which is intended to keep data safe from external as well as internal threats, and to avoid the accidental loss of information.

RISK CONCERNS

The lack of robust safety measures in the medical environment heightens concerns related to physical security of information and medical identity theft. Healthcare organizations are data-rich and provide a "high-touch" environment for data. It is not unusual for many different individuals to access PHI throughout the process of providing care.

For these reasons, insider threats can be particularly challenging. Identity thieves who gain access through employment with a healthcare organization have many means at their disposal for the theft of valuable PHI. Malicious intent is not always behind a data breach. The 2012 HIMSS Analytics study found that 45 percent of respondents indicated that lack of staff attention to internal polices put data at risk. This represents a fourteen percent increase from the 2010 HIMSS survey. Clearly healthcare organizations must place much greater emphasis on educating their employees about the need to protect PHI to reduce the number of incidents based on human error, negligence and poor judgment.

Specific high-risk problems found in healthcare settings include:

- *Unauthorized access to open workstations by both employees and outside individuals.* An open workstation can be taken advantage of by anyone—patients, cleaning crew or outside vendors or employees not authorized to access certain sensitive information
- *Unauthorized access to file storage cabinets or closets by employees and outside individuals.* Although the HIPAA Security Rule provisions are largely focused on electronic PHI, organizations should not overlook paper files in their offices. Even if the provider has converted to Electronic Health Records (EHRs), there is likely to be paper generated within the office—copies of forms or identification brought in by patients, faxes, etc.
- *Loss or theft of physical media or devices.* These include laptops, mobile phones, tablets, backup tapes, thumb drives, CDs, basically any device or media that can store electronic data. Loss of physical media accounts for a large portion of data breaches within healthcare; an analysis of the information reported to the U.S. Department of Health & Human Services for breaches impacting more than 500 patients reveals that nearly 51 percent of breaches were due to lost or stolen desktop computers, laptops and portable electronic devices[12]

MITIGATION STRATEGIES

Although there are several vulnerabilities that put patient data at risk, there are proactive solutions to address them. The following highlights common practices organizations adopt to ensure PHI is protected from theft or loss:

- **Ensure visitors do not have physical access to workstations or equipment that stores or accesses PHI.** Securing workstations is vital in any setting, large or small. This includes implementing a "clean desk/clean screen" policy. Employees should store paper files, mobile devices and electronic media in locked cabinets when not in use; and should "lock" computers any time a workstation is unattended, using a strong password.
- **Exercise proper disposal of paper records, hardware and devices**. For larger institutions, the disposal of old or outdated media storage will likely fall to the IT department; however in small to medium-sized offices employees may self-store data on

CDs or other storage devices; often lacking knowledge of the correct protocol for safely discarding this equipment once it has become old or outdated. Offices of all sizes should keep an inventory of physical property involved in the use of PHI, which includes, not only computers and storage media, but also printers, cell phones, fax machines, cameras, keys, access cards, and landline phones. A periodic audit of media assigned to employees will also help in determining what needs to be disposed or preserved. Files containing sensitive information should be disposed via document shredders or locked trash receptacles. Dumpster diving remains a method for identity thieves because many healthcare organizations neglect this vital step.

- **Maintain physical security records to deter unauthorized access to sensitive data (security cameras, access badge logs, sign-in sheets, etc.).** Physical security record-keeping can be vital in the event of a data breach. Access logs, sign-in sheets, footage from security cameras—all of these will aid in determining exactly how a security breach occurred. In fact, they may be the only clues to determining the cause of a breach, and whether sensitive data was stolen. Small offices often lack access to these types of security measures; or they are not used to the fullest extent—usually with no customization beyond the manufacturer's settings of the software and equipment. No matter the office size, organizations should look to evaluate their competence in this area, as these records could be used to establish risk exposure (i.e., how often unauthorized personnel access the area).
- **Use a maintenance log to track equipment and facility repairs (i.e., repairs that would affect physical security).** Any regular maintenance performed by cleaning crews, building services personnel, authorized contractors or vendors should be documented. Documented employees and approved servicemen may be allowed unescorted access to permitted areas on the premises (with the exception of network server rooms, records rooms, or other restricted-access areas) provided appropriate background checks have been performed. In larger environments, these individuals should be provided identification badges, to be worn in full view while on the premises. Any keys or access cards issued to maintenance must be tracked and their use should be audited periodically. If keys are lost, locks should be replaced immediately, and the office manager or security manager should be contacted immediately to ensure protocol is followed.

ADMINISTRATIVE SECURITY

The HIPAA Security Rule defines administrative safeguards as "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."[13] Such safeguards are key to mitigating identity theft. The HIPAA administrative security requirements include:

- Security management policies and procedures (including risk analysis and risk management).
- That a security official be assigned to develop and implement security policies and procedures.
- Workforce security measures (authorization, clearance and termination procedures).

- Guidance on information access management and security awareness training.
- Incident response policies and procedures; recommended data backup and disaster recovery processes (including testing and analysis).
- Suggested periodic evaluations.
- Outlines guidance for business associate contracts.

Administrative safety measures taken by covered healthcare entities can have enormous impact on the incidence and prevalence of medical identity theft. Not only do healthcare organizations have the opportunity to improve the prevention and deterrence of data theft, but also to educate employees, patients and third parties about the effects of medical identity theft, how to recognize it, and what steps to take to remediate in instances where identity theft has occurred. With appropriate security protocols in place, if a breach occurs, an organization has a definite plan of action to enable a prompt response, which will also mitigate the overall impact to the population.

RISK CONCERNS

Risk concerns surrounding administrative safeguards include:

- ***Insider threats**.* Insider theft in the healthcare industry is fairly high. Employees have ready access to highly valuable personal identifiers, providing the opportunity to steal, sell or use patient PHI. Third-party vendors, contractors, and temporary employees, who may not receive the same level of training as full-time, regular employees also often have access to the same valuable data. Workers can be exploited by external parties, such as through social networks. This is very difficult to stop and can be one of the most effective ways a hacker may employ to gain access to your system.
- ***External threats**.* This is a growing problem within the healthcare industry. In healthcare, where data thieves are typically after rich data sets of PHI, external parties are typically looking for weaknesses in security that can be exploited.
- ***Inadequate policies and procedures**.* The guidelines set forth by an organization are the first line of defense in the protection of data, but very few healthcare companies have policies strong enough to adequately protect data. According to the 2012 HIMSS Analytics: Security of Patient Data report, 49 percent of respondents agreed their risk analysis noted a deficiency in their organization's security plan.[14] Often this reflects a lack of on-going risk review and analysis—threats and technologies change. As the business grows it is important to periodically assess the effectiveness of previously established policies and procedures. Process development goes hand-in-hand with employee training. In the latest HIMSS Analytics report, 45 percent of respondents cited lack of attention to policy as the item that puts data most at risk.
- ***Inadequate analysis of existing logs and records to determine threats**.* When a breach of data occurs, security logs, which could have been used to determine who gained access to the secure area and what sensitive information was accessed, may have been deleted or were never collected to begin with.
- ***Business associates (BAs).*** These third parties are an extension of the covered entity itself, inasmuch as they share in the use of PHI to perform day-to-day operations. If a BA's organization policies and procedures are not current or contain weaknesses overlooked by the covered entity, the BA can pose a major vulnerability for a data breach.

- ***Cloud services**.* Cloud-based computing and data storage is fast becoming a preferred choice in healthcare as it allows users to reduce the amount of files stored on their physical servers while also offering increased processing capabilities at a reduced cost. The security of a cloud service provider must be scrutinized, and because this is new technology for many organizations, it deserves special attention. Companies should complete their due diligence to understand what security measures the cloud service provider has in place to protect sensitive data. If this does not occur, they may not be prepared to handle a third-party breach involving the cloud provider.
- ***Known breaches of data and patients' increased susceptibility to medical identity theft.*** Depending upon the circumstances, a breach can put patients at considerably higher risk of harm, especially if the breach was perpetrated by an insider. Often cases involving employee data breaches go undetected for a significant amount of time, affording the perpetrator more of an opportunity to either sell the data to a third party (making it even more difficult to trace) or use the patient's identity for themselves. For this reason, it is important to consider the risk of harm related to the affected population—some of whom may be at a greater risk level than others and may require special assistance or remedies to safeguard their information.

MITIGATION STRATEGIES

Because medical identity theft is one of the more complicated and problematic types of identity theft, it is important for healthcare facilities to educate patients on the care and security of their own medical and billing records. Patient-focused solutions that can help mitigate threats and support remediation include:

- ***Privacy and security training***: Training is the cornerstone of any successful privacy and security program. HIPAA requires training of all new and current workforce members, including contract, temporary and volunteer workers, with access to PHI. Covered entities can and should take into consideration role-based utilization of PHI and customized training to fit with scenarios the employee is most likely to encounter. A number of employees will need only basic training, while others will require a more in-depth understanding of their role in security to ensure PHI is safeguarded.
- ***Employee screening***: A stringent background screening program includes a criminal records search, residence history trace, credit check, drug test and a search for aliases. The report should encompass all jurisdictions of residence in the previous seven years.
- ***Inclusion of sanctions in policies and procedures***: HIPAA calls for organizations to have a sanction policy that will "apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity." While companies may have sanctions as part of their security policies and procedures, they are not always well understood by employees. It is important for organizations to clearly state what types of disciplinary actions an employee can face for violating security policies and procedures, and provide examples.
- ***Notice of privacy practices***. HIPAA requires all covered entities to present a notice of privacy practices to any person served. Distribution of this notice provides additional information to patients concerning medical identity theft. According to the Department of

Health & Human Services (HHS) website[15], medical providers must describe "the individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity." Since this notice is provided to all patients, it offers a good avenue to provide information on what a patient can do if he or she suspects identity theft. To decrease the possibility that the identity theft information could get overlooked as part of the privacy notice, a covered entity could create a separate document for the medical identity information and simply include it with the privacy notice.

- ***Accounting of disclosures***. When notifying patients of their rights under HIPAA (and also their means to investigate potential identity theft), a covered entity (under HIPAA these include healthcare providers, insurers and electronic transaction clearinghouses) should include information about the individual's right to an accounting of disclosures. This can help the patient identify the person with whom the information was shared.
- ***Patient access to medical records***. Often physicians and hospitals misinterpret the HIPAA Privacy Rule, refusing access to files suspected of fraudulent activity under the guise of protecting the thief's right to privacy. The Federal Trade Commission[16], *even in cases of identity theft*, gives the patient the right to obtain copies of their medical records. Victims of medical identity theft also retain the right to have falsified information amended and/or have an explanation of dispute placed in the file to avoid future complications.

In addition to these security measures, employers can ensure that staff members are trained to recognize common signs of medical identity theft in day-to-day operations, such as a discrepancy in patient identity information and how to respond.

Other signs that may indicate medical identity theft include:

- The covered individual received an Explanation of Benefits statement listing services or treatments they never received.
- The covered individual received a bill for services or equipment they never received.
- An unpaid medical bill has been sent to collections by the medical provider, but it is not related to any service received by the covered individual.
- The patient is denied health insurance benefits or prior approval for a procedure because the health insurer has claims history for that individual indicating the benefit in question has been exhausted, but this is the first time the patient is attempting to access the benefit.
- A physician notes inaccuracy in historical information in medical record based on information being provided by the patient during current encounter.

There are also some easily overlooked considerations that will directly affect employees' ability to safeguard patient data:

- ***Access restrictions for employees***. Organizational data security requirements should include role-based access to PHI determined by job function and including access only to that which is necessary to perform duties. Employees should be required to provide authorization any time the data is accessed. This includes all devices available to the employee – workstations, laptops, cell phones, etc. Any terminated employee's access privileges must be terminated within 24 of leaving the organization. Keep in mind special access scenarios—for instance, regular teleconferences.

- ***Review of activities***. According to the Verizon 2011 Data Breach Investigations Report[17], less than 1 percent of the breaches analyzed was discovered through log analysis; even though in 69 percent of the cases the breach was detectable though log evidence. Logs are an important part of any forensic analysis and a careful log analysis can also help organizations detect suspicious activity. The HIPAA Security rule requires covered entities to regularly review information system activity through records such as audit logs, access and security incident tracking reports. Unusual or abnormal occurrences recorded within the logs can often indicate signs of a data breach. For instance, detecting malware might involve looking for unusual communications or traffic in places not normally expected, as the malware "calls home" at scheduled intervals. Logs are also essential in determining what, if any, PHI was infiltrated from the organization's databases.
- ***Documented incident response plan***. All healthcare organizations must develop and implement an actionable incident response plan, thoroughly test the plan and perform frequent reviews to ensure updates are made in a timely manner. Testing may include a tabletop drill, in which all stakeholders are brought together for a dry run of the response plan in the face of a mock breach scenario
- ***Social media policy***. Social media is increasingly provides an opportunity for external threats. In some instances, external sources may use information on social media sites to launch a social engineering attack against employees. In other cases, it is the employees themselves who commit privacy violations by divulging sensitive information on social media channels. A social media policy should include clear guidelines on proper social media use for employees, as well as the consequences of non-compliance.
- ***Business Associates*** (BAs). Both HIPAA and HITECH mandate requirements for a BA agreement to ensure the privacy and security of the covered entity's sensitive PHI. These requirements should be included as obligations within the BA Agreement. Some obligations, such as background screening, are not specific requirements of HIPAA, but an organization may choose to include these provisions. Important questions to ask a BA include:
    - How will data be: stored, accessed, shared or transmitted?
    - What is the data retention policy (e.g., what will happen to the data when this relationship ends)?
    - Does the BA have a comprehensive privacy awareness training program for employees?
    - Does the BA have an incident response plan in place that establishes procedures for notifying you as soon as a breach has occurred?
    - Who are the BA's subcontractors, and how will PHI be disclosed to them?

Should concerns arise after a business relationship has been established, a covered entity has the option of performing an onsite audit of the proposed BA's stated policies and procedures. This will provide the covered entity a firsthand glimpse of operations, and may be more successful at understanding the BAs capabilities than any due diligence questionnaire. As part of this review, it would be important to ensure that the BA has a plan for mitigating the effects of identity theft. For instance, if the BA provides billing and collections, it's important to ensure that it knows its obligations under the Fair Credit Reporting Act (FCRA). If an individual verifies through a police report that certain financial charges made to them are the result of identity theft, the FCRA says the associated debt cannot be reported to credit bureaus. [18]

SPECIFIC RISK MANAGEMENT CONCERNS

POINT-OF-SERVICE SECURITY

Privacy and security are often the top challenges of health IT. How the healthcare community safeguards patient information plays a role in patient satisfaction and adds confidence to the healthcare ecosystem's use of technology to solve problems on both an individual and holistic patient scale. Although the technical complexity of exchanging interoperable health records in a secure trusted framework often receives the most attention, the systems and processes used to conduct everyday interactions with patients are just as important. As technology increases the ways in which patients can interact with healthcare providers and an expanded care team, the healthcare community can benefit by recognizing and applying best practices for patient identity management to assure the right outcomes in the most cost-effective manner possible.

RISK CONCERNS

Despite its importance, patient identity verification processes and techniques are inconsistently applied in the healthcare community. Identity verification incorporates processes and technologies to help ensure patient presented information is correct and updated throughout each episode of care. In many front-end patient access processes, office staff acts as gatekeepers by requesting basic demographic information before allowing clinical services. Sometimes this information is copied, validated against trusted information sources, or stored electronically and tied to the patient record; sometimes it is not. Even in those instances where there is a process in place to validate patient identities, the process can be outdated relative to the techniques employed by perpetrators or identity thieves.

The presented information is included in numerous downstream workflows including revenue cycle management and care coordination. Medical identity theft could cause patient identity information to be incorrect thereby affecting claim payments, which may be rejected or denied. Patients may also be subjected to inappropriate treatments. The importance of high quality patient identity verification processes applies across the healthcare landscape as patients enter different care settings and access remote healthcare services.

Verifying the identity of an individual seeking care allows providers to retrieve proper medical records, understand familial, behavioral, and historical factors that may affect diagnosis or treatment, and develop a consistent relationship for condition management. Correctly identifying patients also facilitates efficient administration of healthcare payments, allowing providers to seek reimbursement from health plans and from patients for self-pay balances. Identity verification is one control mechanism against identity theft and identity confusion, acting as a layer of defense along with other physical and cyber-security measures to keep patient encounter information private and safe.   Adding greater rigor to identity verification within patient access processes can be done without adversely affecting business processes. Done well it can streamline operations and deliver greater protection against incorrect information being added to an individual's medical record.

In a common patient identity verification scenario, a patient arrives at the healthcare provider's building and the front-office staff requests information from the patient, including a medical ID card issued by the health plan, the patient's driver's license and a description of the chief complaint. Once the information is presented, the registrar validates the driver's license photo with the physical patient, makes a copy of the front and back of the medical ID card and driver's license and inserts the copies into the patient record. On subsequent visits, the registrar has an opportunity to compare the presenting patient with the picture on the copy of the driver's license to help ensure the patient is who they claim to be.

This process, however, fails to address the need for verified patient information in many situations. For example:

- What if patients do not have medical IDs or driver's licenses?
- What if the presented information is a false identity?
- How does the registrar tie the patient's identity to the photo ID if the patient is new and no previous record exists for comparison?
- What if the patient knowingly or unknowingly presents outdated information?
- What if the patient is attempting to access services or information remotely by phone or the Internet?

In short, these situations compel the application of risk-appropriate methods and technologies that mitigate the possibilities of identity theft, identity mis-matched, and poor information collected during the patient access process. Understanding the risks involved with poor patient verification can set the stage for providers, payers, and patients to mitigate these risks.

Medical identity theft can result in both HIPAA violations and legal liabilities. If a patient is inappropriately identified and medical decisions are made based on incorrect records, the provider may be liable for damages incurred by the patient and the patient's family. Such liability could not only result in legal judgments against the provider, but in the delivery of professional sanctions and the revocation of a provider's license. Appropriate patient verification processes can help reduce this legal exposure and avoid operational problems.

Implementation of electronic medical records health information exchange also impacts an individual's risk for erroneous medical treatment associated with medical identity theft. Diagnosis and treatments are often based in part on the familial history, allergies and previous treatments. Obtaining the wrong medical record can result in additional waiting time for the patient, misguided treatments and a poor patient experience.

If a claim is submitted for the wrong patient and the payer fails to catch the identity mix-up, improper reimbursements can result. Once the patient receives the explanation of benefits (EOB), recognizes a problem and notifies the payer, charge-backs from the provider ensue. This scenario has the potential to exhaust patient benefits if the fraud is not caught, create frustration for the patient when identified and set in motion a long-term ordeal to reconcile and correct medical records with every affected provider that has included erroneous data as part of the record.

MITIGATION STRATEGIES

Providers approach patient identity verification in different ways. Some methods clearly have problems:

- Providers may view the threat of medical identity theft as insignificant or rely too heavily on payers for identity management needs. Providers may erroneously believe that because payers have advanced technology and expertise which includes adjudication systems, large special investigation units, and have access to data analytics, they are equally or better able to identify irregularities during the claims adjudication process that would call out errors in patient identification. This approach fails to address the patient safety, operational inefficiencies and patient satisfaction ramifications that occur before the payer ever has an opportunity to intervene.
- Low-tech, policy and procedure-based approaches to patient identity verification alone are also insufficient because they tend to be inconsistently applied and more difficult to enforce across different patient access settings. To be sufficiently robust, a policy must address registrar actions not only under "normal" circumstances, but also under a variety of exceptional" circumstances. Once the exceptions have been outlined in a policy, the policy can easily become unwieldy for even the most astute registrar to reasonably manage. A successful approach to patient identity verification must attempt to curtail identity theft in a variety of situations that cannot be sufficiently described or enforced with a policy and procedure-based approach.
- A single technology will not solve all patient identity management needs either as technological solutions is easily mismatched to the effective need. As providers and payers sponsor remote access to medical record information, lab results and interactions with the care team through websites, smartphones and tablets, patient identity verification during enrollment and ongoing usage needs to account for the lack of a patient's physical presence with increasing sophistication.

Verification methods should manage risk appropriately for each unique scenario. This may include specific methods for identity verification on-site, through a call center, or through remote access solutions like a patient portal. Standards bodies, including the National Institute of Standards and Technology (NIST), have defined graduated levels of verification hurdles that provide related assurances about a person's identity and his or her authorization to access or transact information.

When a patient visits a clinical setting for the first time or is unable to produce any identification, technology can validate a person's identity by comparing a few demographic factors like name, address and date of birth to trusted information sources that contain the real person's identity elements. In a call center environment or for automated outbound calls, alternatives such as voice authentication help verify the identity of the individual calling in with minimal need for additional information. In a patient portal, verification can be coupled with an automated knowledge-based authentication that presents a dynamic, multiple-choice quiz about the individual's personal history, such as previous addresses, education and familial relationships.

These tools help ensure users are who they claim to be each time they access the medical system. Because a proper name, address and phone number is information that may be easily accessed by any individual, including someone who does not actually own the information, in circumstances when it is imperative to confirm that the person is who they claim to be it is incumbent upon providers to take additional steps. Demographic verification services, knowledge-based authentication and biometrics are some of the tools to be used independently, tailored and mixed with operational policies to counter the risks involved with each scenario.

As methods for perpetrating medical identity theft become more and more sophisticated and electronic access to personal health information becomes more common, the tactics selected by practices, hospitals and payers to protect personal health information and ensure patient safety will need to evolve. The increasing popularity of tablets and smartphones demonstrate that changing technology not only creates new avenues for patients to access information, it also cultivates the need for smarter ways of ensuring that healthcare communities know who they are dealing with.

ELECTRONIC HEALTH INFORMATION EXCHANGE SECURITY

In both commercial and government sectors, more transactions are occurring in remote channels that force organizations to address enterprise and customer identification management in a whole new way. This is also true for health information exchanges (HIE) that are being designed to provide the secure exchange of electronic health information and EHRs across the entire healthcare ecosystem and ever-expanding geographic regions. A trusted environment for electronic health information exchange will only be possible when those responsible for developing and participating in an HIE create a trusted environment. The implementation of proper security measures is essential to reaching this goal.

RISK CONCERNS

In 2010, the National Institute of Standards and Technology (NIST) published NISTIR 7497 "Security Architecture Design Process for Health Information Exchanges (HIEs)" that presented a layered architecture design process to identify and implement security and privacy in HIEs[19]. The second layer of this approach, classified as "Enabling Services," identified a set of minimum requirements necessary to implement policies for ensuring the secure electronic exchange of health information.

The security guideline provides minimum requirements across the HIE which include:

- Authentication protocols to ensure that an entity is the person or application that claims the identity provided.
- Credential management processes to create and manage the life cycle of the credentials being used for authentication and access control.
- Access controls to ensure that an entity can access protected resources only if the authentication and credentialing management processes indicate they are permitted to do so.

As stated in the guidelines, protecting electronic patient health information is the most critical aspect of developing systems and structures that support the exchange of that information among healthcare providers, payers and consumers using HIEs.

MITIGATION STRATEGIES

Adoption of strong authentication within HIEs will be largely shaped by the need for user access. Consumers, and other non-employee users, tend to challenge most systems by desiring access across a variety of communication channels without using issued authentication devices. This is also true as mobility and personal devices drive the access needs of the payer and provider community. This section will discuss some solution options to help address these challenges for identity-enabling authentication systems such as may be found in HIEs.

The security associated with identity-enabling authentication systems should be built on the basic principle that the process to establish the identity and the process to authenticate a user are distinct, yet interrelated, components of the steps necessary for a secure identity management infrastructure. Since an identity must ultimately be bound to the authentication "token" or method, identity establishment without proper proofing at a determined assurance level can invalidate the integrity of the entire system to manage identities.

HIEs can begin with proofing of the personal identity or "biographical authentication" as the foundation for establishing the identity. Following successful identity establishment, HIEs can enroll or bind the proofed identity to a biometric or token authentication factor for subsequent transactions. Identity proofing or "biographical authentication" can also be used in subsequent transactions if binding of the identity is not desired in the process or if the mitigation of risk presented requires reestablishment or further proofing of the identity.

In addition to personal identity proofing, HIEs also must determine their need for identity authentication for the payers and providers within the system. Some of the users seeking access to an HIE will have credentials associated with professional licensure that can be validated, while others may need to be validated by their organizational and roles-based associations or authorizations.

HIEs will need to balance security, privacy and convenience for users who may access a system through a variety of communication channels. A sample workflow for security identity management is outlined below:

Step 1: Initial fraud screening occurs against elements such as device or IP geographic location, device identification, and unusually high volume transactions.

Step 2: As part of the enrollment the user undergoes an identity proofing process.

Step 3: For continued ease of access, confirmation through another device, such as a mobile phone or biometric capture is completed. This will also be used during password reset processes and as a contact designation to send one time passwords.

Step 4: Identity information and captured print(s) are compared against list of known perpetrators convicted/suspected of identity theft.

Step 5: The account is provisioned and user receives credentials with proper authorizations for future access needs.

Step 6: Based on the results of the authentication method deployed for the credential, HIE access and transactions are either granted or denied.

HIEs must consider a holistic approach to the security of the identity-centric transactions that occur within the system. A holistic solution approach affords a single view of the user from enrollment to repeat access—resulting in more efficient authentication processes and a higher level of security.

In recent years, as mobile device usage has risen, it has become both more difficult and more crucial to authenticate users who conduct transactions using these new devices. In many cases, user names and passwords alone are not strong enough for user authentication. Traditional methods like static challenge questions no longer provide the necessary safeguards for secure account access. User authentication is a foundational service that supports compliance, information security, and operational functions. If internal and external user identities are not properly authenticated, then an enterprise has no assurance that access to resources and services is properly controlled. Everything hinges on the true identity of the user, on the assurance that the user really is who he or she claims to be.

The need to address new business models and systems, emerging regulatory requirements and increased incidence of fraud has driven the growth of multi-factor authentication (MFA). Multi-factor authentication, the process of authenticating a user through at least two independent elements or "factors," employs a combination of any two of the following:

- Something you know: A user name, password, PIN or answers to questions.
- Something you have: A token, access card or key fob (a small hardware device with built-in authentication mechanisms).
- Something you are: Your fingerprint, voice or iris (i.e., biometric).

An access card, for example, can be stolen, but the thief likely wouldn't know the PIN number and he or she certainly wouldn't meet a biometric threshold. By adding these additional layers of security, systems can better protect access to its critical information and resources.

The following are examples of how an HIE could integrate authentication factors:

- ***Something you know example: dynamic knowledge-based authentication***

  There are a number of ways that knowledge based authentication can be incorporated into security processes. Something you know can be a password or numeric pin; however, one of the most interesting emerging approaches is question base authentication with the two main question categories of static and dynamic knowledge-based authentication (KBA). Static KBA refers to "shared secrets," where the question and answer are predetermined and registered by the user. Typically with this method there is no cross-referencing of the correct answer to determine if the information provided in accurate. Instead, the focus is memorization and recall of the registered answer to the selected question(s). Dynamic KBA, on the other hand, does not rely on the registration process; questions are systematically generated, often in a randomized manner, in a challenge-answer method for the user. This dynamic questioning method is more complex than knowledge based and can include out-of-wallet or public record data, financial data, or even data pertaining to specific transaction histories.

- ***Something you have example: one-time password***

  Traditional one-time password measures such as passwords generated through key fobs are not always a practical solution for patients, other non-employee users or mobile workers because of their high cost and requirement to maintain the device within one's possession for secure usage. One-time password capabilities available in a tokenless authentication form offers an effective tool for authenticating constituents for high risk or high value transactions-without the need for an additional hardware. These methods can involve an alphanumeric code via SMS, text, e-mail or phone, allowing the user to receive a one-time password on a device they already have in their possession.

- ***Something you are example: biometrics***

  No single biometric can meet the requirements of all applications. The match between a specific biometric and an application is determined by the operational mode of the application and the properties of the biometric characteristic. Given different applications, environments, users and target enrollees, solution constraints will vary. The effectiveness of a biometric solution relies not only on the modality chosen but also upon on how and where it is used.

There are seven characteristics generally acknowledged to provide guidance for assessing the suitability of a particular biometric trait or modality.

  - Acceptability—the combination of social, cultural and legal impacts that might ease or impede use and adoption.
  - Circumvention—some traits are more vulnerable to circumvention or tampering than others.
  - Collectability—access to biometric readers and capture software, ease of collection and dependence on environmental factors.
  - Permanence—resistance to change with age, disease, injury, weight, stress, clothing, medication, intoxication.
  - Performance—speed, accuracy, enrollment process, scalability, ability to handle searches of one-to-many, one-to-few and one-to-one matches.
  - Uniqueness—usefulness in making clear distinctions between individuals, enhanced by the number of independently varying features.
  - Universality—whether a biometric trait is present in all or nearly all of the given population.

Additionally, other factors may be important such as:

  - Cost: Can the biometric trait be acquired accurately and easily at a low cost under varying operational situations?
  - Industry adoption: What is the adoption rate of a particular modality? Is there adequate research in the space?
  - Legal and privacy compliance: Does the modality meet privacy compliance? Are there potential legal or privacy concerns preventing compliance?

- Vendor adoption: Are there enough vendors with a proven record and historical data for evaluating accuracy and effectiveness?
- Independent testing: Has there been independent testing and studies of the performance and effectiveness of this biometric?
- Interoperability: How adaptable and interoperable is it with existing systems or other vendor solutions?

Two biometric modes that may be most easily incorporated into an HIE security process are fingerprint and voice.

While police and government agencies have used fingerprints to identify the "bad guys" for many years now, organizations are beginning to recognize the value of fingerprint biometrics for more systems requiring stronger authentication for user access. Fingerprint biometrics has become an attractive in-person authentication tool due to its convenience, general familiarity and ease of use and higher level of assurance. Fingerprints are unique to each individual, do not change over time and are easy to collect. And because they are part of the individual, they can be accessed at any time without requiring the customer to carry an additional device or token.

Accuracy of fingerprint biometrics is high and it is capable of real time searches on extremely large data sets without compromising performance. Fingerprint biometrics has been widely adopted in the healthcare industry and several vendors offer a choice of low cost readers. The technology is also well tested by independent agencies (e.g., NIST) and its efficacy is well documented.

Fast and easy to use, electronic fingerprint biometrics can be deployed on-premise or remotely, matching against a hosted database of fingerprints for a system. Fingerprint biometrics also provides a high level of assurance by preventing duplicate enrollments of an individual or fraudulent enrollment under multiple identities.

Voice biometrics is an ideal authentication tool for systems that process a significant volume of anonymous, high risk transactions remotely via a mobile device or within a contact center or telephonic environment. As unique to an individual as a fingerprint, a voice biometric (or "voice print") uses the sound, pattern and rhythm of an individual's voice to determine their identity. Voice biometrics provides a high degree of security with little to no impact on the customer experience.

Voice biometrics is a contactless, non-intrusive and easy to use method of authentication that is widely accepted, especially in remote applications. It is a low-cost solution and easily captured by existing, inexpensive devices (for example, by phone) eliminating any need to purchase additional devices. Voice recognition and verification algorithms are rapidly improving in performance and accuracy.

Identifying and authenticating the true identity of the users, obtaining consent, and properly managing the identities within the system is a constant balancing act between security, privacy and convenience. To be successful, the HIE must develop a risk-based approach to ensure strong authentication of its users. By offering a variety of authentication methods, HIEs will be better prepared to address the remote authentication needs of the various users accessing the system from diverse devices and channels.

CYBER SECURITY

Cyber threats continue to evolve as healthcare implements protection strategies to improve security. With the expanding cyber threat moving from individual acts to nation-state actors, cyber has become increasingly complex. Few experts can even agree on a single approach to cyber security that will improve the national level of information and mission assurance. Vast improvements have been made over the past decade to security standards, security technologies and approaches to deploying security, yet even some of the most sophisticated networks are unable to prevent intrusions and infiltration of data.

Healthcare, including public health, has long lagged behind other sectors in the deployment of both cyber and physical security measures. The ability to openly share patient data could provide insights into alternative treatments or medical opinions that support a change in diagnoses, but doing so requires improvements in current security practices. In large healthcare organizations where information technology funding is high, there is a predominance of both cutting edge health information technologies and security that are influenced by standards most commonly employed in the financial services sector and government. Such organizations tend to take a layered approach to implementing security coupled with a principled physical security program. Large healthcare systems, however, represent only a small portion of total healthcare encounters, leaving the lion's share of care and cyber security to the many organizations and individuals with limited funds.

Information systems coupled with the Internet, have created a paradigm shift away from the traditional brick-and-mortar facility to the delivery of remote healthcare—anywhere, anytime. The implications are that health data once held within a closed community may now be accessible to many, including those outside the United States increasing exposure of healthcare and public health data to cyber penetration and disruptions.

Healthcare is highly diverse and interconnected with other systems such as Social Security, state public health agencies, pharmacies and the Centers for Disease Control and Prevention, among other agencies. Unlike many sectors, healthcare relies on a complex structure of relationships to sustain the provision of care, disease prevention and emergency response. As healthcare and public health become more reliant on technology to improve and extend the provision of care and disease prevention, there is an increasing need to manage the risks to the infrastructure that delivers those services.

Organizational sustainability is now tightly coupled with operational resiliency. Operations increasingly rely on the internet to facilitate, manage, and provide critical services. The dynamics of this growing dependency are intensified by the interconnectedness across industries, services, and international borders. It can be said that just as the economy has moved from domestic to global in scale so too has the networked environment that now subsumes every aspect of business. Moreover, the services that are delivered across the Internet have become increasingly attractive targets. The result is the evolution of a more sophisticated threat environment making it possible to steal one's identity, steal a company's intellectual property, and siphon off tens of thousands of dollars without being detected.

RISK CONCERNS

The proliferation of health IT—mobile devices, telehealth, diagnostics—and cyber physical systems (medical robots) necessitate a more comprehensive examination of the vulnerabilities and consequences associated with cyber threats to the sector. Today, we have only a limited understanding of the speed with which an entire healthcare system might be rendered ineffective; unable to deliver essential services, or of the cascading consequences resulting from attacks to information technology infrastructure. The risks to people, technology, and healthcare operations are inherently interconnected. When security controls fail, the risks to people range from loss of life to financial impacts to identity theft.

Health information can reveal a lot about an individual—their age, ethnicity, where they live, contact information, employment, specific illnesses, among other things. For this reason, the data is referred to as "individually identifiable." How it is used, stored and transmitted is seldom thought about in healthcare settings. This is when it is most critical to be able to share and make use of the data. But data is duplicated, moved and stored in so many ways that ensuring rigid security practices when enforced can be problematic. Examples of technological processes that make data susceptible to intrusions and unlawful use include but are not limited to:

- **Credit, billing and claims processing**: Electronic billing and processing increases the efficiency of billing and payment departments for providers and insurers. It enables real-time financial transactions and can reduce costly overhead. Electronic billing and payment systems interconnect with financial services and must have a high degree of security to avoid theft, fraud or data corruption.
- **Clinical services**: Many, if not most, clinical settings now use information technology and cyber infrastructure to manage patients, to reduce and streamline record-keeping, and to expedite billing. The level of health IT integration changes depend on the particular provider or facility. EMRs are increasing in adoption, but are not always used in real-time. A highly integrated health IT environment can be seen in the model used by Kaiser Permanente. Kaiser has a paperless record system, manages patients through electronic systems that include bar-coded wristbands, and allows doctors to correspond with patients via e-mail. Kaiser also is expanding e-services to include telehealth and telemedicine.
- **Cyber-physical systems**: Medical devices, equipment and imaging systems are a growing segment of networked devices in healthcare referred to as "cyber-physical devices," "cyber-physical systems" or embedded systems. They involve a wide range of devices that can either directly affect patients or provide indirect support. Medical imaging devices require operating systems and are increasingly networked. Some implantable devices, such as pacemakers, include functions to transmit and receive information to provide better patient care. The rapid growth of health IT and cyber-physical systems have opened up a new area of healthcare designed to take maximum advantage of their capabilities.
- **Telehealth**: The growth of health IT and cyber-physical systems has opened up a new area of healthcare that makes broad use of technology and clinical services: Telehealth. Telehealth leverages health IT and communications over the Internet to extend the boundaries and advance patient care. Basic telehealth includes the use of EMRs and e-mails to communicate with patients and colleagues. More sophisticated systems include video conferencing, electronic personal health records that contain all the information of a patient's electronic medical record, as well as other health information, and the ability to share electronic records with others.   Combining certain aspects of telehealth

(videoconferencing, e-mail, EMRs) with cyber-physical systems has allowed for growth in telemedicine. Telemedicine allows clinicians to monitor a patient's status remotely and has significant application in rural populations and in emergency or disaster settings.

MITIGATION STRATEGIES

Even well-funded organizations must prioritize their greatest risks (e.g., web servers, messaging or data storage) and identify what mechanisms are available to reduce these risks. This section identifies network infrastructure that is most at risk of exploitation and identifies the threat types and recommendations on remediating system vulnerabilities to an acceptable level. This is not an exhaustive listing of vulnerabilities or infrastructure risks and should be used as part of to a broader security risk analysis of the organization.[20]

Effective risk management programs focus on continuous monitoring of threats and vulnerabilities as well as inform the security controls needed to mitigate risks. Thus, a number of areas outside of IT must be assessed to adequately detect risk and reduce it to an acceptable level. The following areas represent the major categories:

- Insider and outsider threats—hacking, cracking, or attacking.
- Misuse of data—inappropriate sharing of data, intellectual property, trade secrets, classified information.
- Electronic and hard copy data—loss of data, intentional or inadvertent destruction of data.
- Application error—buffer overflows, computational errors, coding errors.
- Identification and authentication—the ability to validate an individual, device, or a process prior to accessing or carrying out an activity on a given system.
- Web application vulnerabilities—Web application vulnerabilities such as SQL injection and cross-site scripting flaws in open-source as well as custom-built applications accounts for more than 80 percent of the vulnerabilities being discovered.

FINANCIAL SECURITY

Managing financial risk in responding to medical identity theft involves reducing or eliminating costs resulting from a security breach. The goals of the financial risk management process are to enhance, understand and articulate the potential financial risk and to increase understanding of the nature of risk relative to peers and organizational objectives. The risk management process involves an objective review, preferably by a third party, of medical identity policies and practices, IT network controls and IT security governance policies and an estimation of tangible and intangible costs related to a breach.

RISK CONCERNS

The costs of medical identity theft can be significant, not only in terms of dollars spent paying ineligible claims since financial gain is often the central motivation for identity thieves, but also for costs associated with notification requirements, reputational damage, regulatory fines and lawsuits. Both individual consumer victims and the organizations though which the theft occurs can be at financial risk. As a result, organizations need to give close attention to these threats, the costs associated with a breach, and remediation options.

Medical identity theft can be especially costly to an organization's clients or customers in very direct ways and these costs can continue for years. This type of theft is closely entwined with financial identity theft since information on medical records may be useful in obtaining unwarranted credit, as well as obtaining medical care or submitting false bills to insurers.

The financial impact to patients may include:

- A loss or downgrade of credit.
- Harassment from debt collectors.
- Employment problems.
- Rejection for healthcare and life insurance.
- The costs of retaining legal counsel, private investigators and others to resolve stolen identity problems.

What is a direct financial loss to an organization's patients can easily become a cost to an organization as well, especially in instances in which the organization has direct involvement in maintaining or transmitting the stolen information or for maintaining safeguards for avoiding the theft. In addition to liabilities resulting from the cumulative direct costs to victims, an organization should consider additional financial risks of identity theft that can be substantial. These include:

- Direct losses to the organization, which may have been duped into providing costly services or payments.
- Regulatory penalties that the government may apply even when clients or customers have not sustained a financial loss. Recently, the Department of Health & Human Services has administered multi-million dollar fines for medical identity security breaches even when there is no indication that anyone suffered a direct financial loss or even that theft was involved with the breach.
- Financial loss due to loss of reputation. Medical identity theft or even unsecured losses of medical information have received widespread publicity in the media. Under HIPAA, organizations that lose information must notify the effected patients, take out newspaper advertisements if the loss affects significant numbers of individuals and may have the organizations name and circumstances of the breach posted on a government website.
- Punitive damages awarded in a trial if the plaintiffs can demonstrate that losses that occurred were associated with a medical identity theft from the organization that was a direct result of the organization's own negligence.

MITIGATION STRATEGIES

To avoid these financial risks, organizations should consider mitigation strategies. These include:

- Consideration of financial risks and losses, both tangible and intangible, when conducting a security risk assessment. Such factors may help determine priorities and trade-offs when evaluating the cost and difficulty of controls to limit potential risks.
- Developing appropriate controls that minimize the risk of identity theft such as:

  a) Confirming patient identity (similar to banking "Know Your Customer" policies that document, train, and implement processes and procedures, including use of such systems such as Trans Union and other demographic search capabilities).
  b) Confirming the identity of the party financially responsible for patient services (spouse, partner, parent, etc.)

- Prior to their occurrence, developing strategies for managing situations involving medical identity theft.
- Obtaining insurance coverage to offset potential financial losses. Standard property and casualty coverage may not be enough to offset the types and complexity of losses resulting from medical identity theft. Therefore, in developing appropriate coverage the organization should consider:

  a) A framework to determine if sufficient insurance coverage currently exists and the scope of additional coverage needed.
  b) Potential carriers willing to insure the risks involved.
  c) An approach to evaluating such carriers including consideration of the carrier's claim process, reputation, and history of offering this type of insurance.
  d) The extent of coverage needed and maximum limits.
  e) A framework for determining covered losses.
  f) A price for the appropriate scope and level of coverage.

Given the potential costs and risks involved and the availability of meaningful and realistic responses, organizations should assure that managing financial risks is a key component of any medical identity risk management program. In summary, it involves understanding the potential costs of medical identity security breaches, both to an organization and to its patients, and developing appropriate responses. Responses involve assessing the risks, developing controls, preparing strategies to respond to breaches, and obtaining appropriate insurance for managing the cost of a breach.

RESPONDING TO MEDICAL IDENTITY THEFT

An online user is checking an online banking statement and notices several unauthorized withdrawals. The user contacts the financial institution and discovers that someone has stolen his/her banking information. The next call should be to one of the three nationwide credit bureaus who will place a fraud alert on the user's credit file, provide a free copy of the credit report to help identify other fraudulent activity, and notify the other two credit bureaus on the user's behalf.

An individual should consider this same scenario involving his or her medical identity. An Explanation of Benefits is received from the health insurance company for services not requested or received. The individual can call the health insurance company and the provider who submitted the claim to dispute the charges, but who should be called to find out if the information has been used with other providers who may not yet have billed for the services delivered? How can additional fraudulent activity be prevented from occurring? How can medical records corrected?

Unlike the financial industry, there are no credit bureau-type services available to provide a single place consumers can go to confirm that their healthcare information has not been used inappropriately, nor is there a single source on which they can rely to help correct their medical records or insurance information when suspicious or fraudulent activity is detected. Instead, when an individual becomes victimized by medical identity theft, it is their responsibility to identify the extent to which his or her information has been compromised and work with the affected healthcare entities to correct erroneous information entered into their medical records, stop collection actions and restore healthcare benefits that were used to pay ineligible claims. To make matters worse, some providers refuse to give victims of medical identity theft access to their medical records to make corrections, citing HIPAA privacy regulations. These providers erroneously believe that it would be a violation of HIPAA to allow the victim to see the thief's medical information, which is now part of the victim's medical file.

These issues might have been avoided had a 2003 identity theft law been interpreted as applying to a variety of industries, including all of healthcare, retained its original language. The law, the Fair and Accurate Credit Transactions Act (FACTA)[21], was intended to curb instances of identity theft. In its original form, it applied to any entity that met the definition of "creditor" as described in the law. A group of regulatory agencies that primarily regulated the financial industry was tasked with creating rules to support the law. The result of their efforts, the Red Flag Rules, reflected the group's area of expertise and focused primarily on identity theft.

The Red Flag Rules require entities subject to FACTA to implement a written Identity Theft Protection Programs "designed to prevent, detect, and mitigate identity theft."[22] The use of the term "creditor" combined with the rules' focus on identity theft created a great deal of confusion about whether or not the rules should apply to healthcare entities, confusion that delayed implementation of the rules until 2010. In December of that year the President signed into law a revision of FACTA that clarified that it would not apply to healthcare providers. The consequence of these events is that although health insurance carriers are required to have an identity theft protection program in place, there is no industry-wide approach to dealing with medical identity theft and no sharing of information between healthcare entities when potential fraud is detected.

Healthcare organizations do not need to wait for a mandate to address the issue. Good business practice, especially given the risks identified within this white paper, dictate that healthcare providers, insurers and their business partners voluntarily develop formal policies and procedures for preventing, detecting, and responding to allegations of medical identity theft. We have made recommendations regarding the prevention and detection of medical identity theft elsewhere in this paper. Here we will address how a healthcare organization might respond to allegations of medical identity theft.

Policies and procedures should include, at a minimum, processes for the following activities:

1. Placement of a "flag" on the victim's electronic and paper medical file, alerting anyone accessing the victim's PHI that there has been a report of medical identity theft, the date of the allegation, and, if known, the date the theft occurred.
2. Confirmation that medical care delivered to the patient after notification that the patient has been the victim of medical identity theft was actually received by the patient (note: Legal counsel should provide guidance on the length of time following notification of medical identity theft an entity should continue this practice.)
3. Allowing a victim to review and correct their medical record, including access to electronic and paper versions of the record.
4. Standard tracking of entities with which the patient's PHI is shared; victim should be given a copy of this information to assist them in identifying what records may need to be corrected.
5. Creation of a "Jane or John Doe" file that will allow for the alleged medical identity thief's information to be transferred from the victim's file to a separate file for the alleged thief.

6. Review of accounts receivable activity to proactively identity any claims that may have been submitted for treatment delivered to the alleged thief and which could now be reviewed as ineligible.
7. Notification of government and commercial payers of the submission of ineligible claims and repayment of those claims (Providers and payers may want to consider including a provision in their contracts with one another to address claims that have been processed and later identified as being associated with medical identity theft).
8. Review of internal identification verification processes to determine how they might be revised to protect against future incidents of medical identity theft.

Proactively establishing policies and procedures to address medical identity theft and providing staff with ongoing training of these policies and procedures is in the best interest of both the medical identity theft victim and the entity itself. Formal policies and procedures provide staff the guidance and authority to assist victims in correcting their medical records. They ensure that the provider has the correct information to effectively treat their patient going forward and limit the financial and legal risks for payers and providers associated with the continued processing of ineligible claims.

CONCLUSION

Death and taxes…and risk. There is no getting around the fact that risk is, and will always be, part of the cost of doing business in a world that includes exabytes of data about millions of people as its stock in trade. This information is invaluable to the patients whose care we are entrusted with, and is extremely valuable to those who seek to gain an illegal profit by stealing it. The risk of medical identity theft cannot be allowed to stall progress toward a more transparent and effective healthcare delivery system.

There is also no doubt that there is a cost to every business decision made to proactively prevent medical identity theft. As healthcare shifts to a more business-oriented model in these financially challenged times, we would do well to keep in mind a quote attributed to Warren Buffet, "Lose money for the firm and I will understand; lose a shred of reputation for the firm, and I will be ruthless."[23] Healthcare entities should be ruthless in protecting their hard earned brand and the public's trust in that brand.

This paper presents an approach that balances risk and cost by taking an enterprise view. By involving decision makers with varied areas of expertise and tolerance, or intolerance for risk, proactive and thoughtful plans can be put in place to reduce the risk of medical identity theft to a minimum. Procedures must be implemented should issues occur to ensure quick and effective response as well as methodologies to incorporate lessons learned into best practices.

The digitization and mobilization of healthcare is in its infancy. However, the volume, complexity and frequency of healthcare transactions will only increase in the coming years. The data being driven by medical devices, imaging, and sensors will increase the amount of PHI exponentially. It is high time that critical structures be implemented to ensure resiliency and strategic leadership that will drive each organization's foundational efforts to prevent medical identity theft. This paper should serve as a guide to that crucial and timely effort.

Privacy & Security Task Force White Paper Contributors

John Phelan, PhD, *FY2012 Privacy & Security Chair*
Management & Technology Consultant
Milliman, Inc.

Ed Dodds
Communications Strategist, Web Dev. Writer
Conmergence.com

Lydia Duckworth, CHSS
Information Systems Engineer Lead
The MITRE Corporation

Bill Fox, JD, MA
Principle
Booz, Allen, Hamilton

B.P. Fulmer, B.S.
Managing Partner
Exchange EDI

Sheldon Hamburger
Managing Director
The Aristone Group

Pamela Jodock
Director of Business Development
Commercial Healthcare
LexisNexis Risk Solutions

Brian Lapidus
Senior Vice President, Strategic Partnerships
Kroll Cyber Security & Information Assurance

Richard Marks
President
Patient Command, Inc.

Jeremy Miller
Director of Product Development
Kroll Cyber Security & Information Assurance

Rick Morrison
President
Medical Banking RX

Dhiraj Sharma, MBA, FAHM
Senior Manager, Healthcare Business
WIPRO Technologies

Mick Talley
Director
University Bancorp

About HIMSS

HIMSS is a cause-based; not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare. Founded 52 years ago, HIMSS and its related organizations are headquartered in Chicago with additional offices in the United States, Europe and Asia. HIMSS represents nearly 50,000 individual members, of which more than two thirds work in healthcare provider, governmental and not-for-profit organizations. HIMSS also includes over 570 corporate members and more than 225 not-for-profit partner organizations that share our mission of transforming healthcare through the effective use of information technology and management systems. HIMSS frames and leads healthcare practices and public policy through its content expertise, professional development, research initiatives, and media vehicles designed to promote information and management systems' contributions to improving the quality, safety, access, and cost-effectiveness of patient care. To learn more about HIMSS and to find out how to join us and our members in advancing our cause, please visit our website at www.himss.org.

References

[1] Ponemon Institute Second Annual Survey on Medical Identity Theft. March 2011.

[2] Torrey, Trisha. “The Dangers of Medical Identity Theft.” About.com. 04/26/2012. http://patients.about.com/od/yourmedicalrecords/a/medIDtheft.htm. 05/25/2012.

[3] http://www.youtube.com/watch?v=Y3aPB5Afdks

[4] Biegelman, Martin T. “Unhealthy Procedures: Medical Identity Theft.” Association of Certified Fraud Examiners. 10/09. (http://www.acfe.com/article.aspx?id=342. 05/25/2012).

[5] https://idc-insights-community.com/health/healthcare-transformation/3-massive-security-breaches-in-3-weeks-taking-a-cl

[6] Ponemon Institute Second Annual Survey on Medical Identity Theft. March 2011.

[7] Altarum Institute Spending Brief #12-07: May 2012. DataCenter for Sustainable Health Spending Health Sector Economic Indicators http://www.altarum.org/files/imce/CSHS-Spending-Brief_July%202012.pdf

[8] Henetz, Patty. “Medicaid breach far worse than reported.” Salt Lake City Tribune. 04/06/2012.

[9] 2012 HIMSS Analytics Report: Security of Patient Data commissioned by Kroll Advisory Solutions

[10] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

[11] http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

[12] Ponemon Institute.”Perceptions About Network Security, Survey of IT & IT security practitioners in the U.S.”. http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf. 2011, June

[13] U.S. Department of Health and Human Services Office for Civil Rights. HIPAA Administrative Simplification. http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf. February 16, 2006

[14] Kroll Cyber Security.2012 HIMSS Analytics: Security of Patient Data.http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_-_Security_of_Patient_Data_040912.pdf. April 2012

[15] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html

[16] http://business.ftc.gov/documents/bus75-medical-identity-theft-faq-health-care-health-plan

[17] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

[18] www.ftc.gov/os/2004/11/041119factaappg.pdf

[19] NIST. Health Information Exchange (HIE) Security Architecture. http://www.nist.gov/healthcare/security/hiesecurity.cfm. September 2010

[20] For a comprehensive list of software vulnerabilities users may want to visit http://cve.mitre.org/ or http://nvd.nist.gov/.

[21] Fair and Accurate Credit Transaction Act: http://www.gpo.gov/fdsys/pkg/PLAW-08publ159/pdf/PLAW-108publ159.pdf

[22] Federal Register.Vol. 72, No. 217. http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf. November 9, 2007.

[23] Buffet, Warren. Testimony before the Subcommittee on Telecommunications and Finance of the Energy and Commerce Committee of the U.S. House of Representatives. http://blogs.wsj.com/marketbeat/2010/05/01/buffetts-1991-salomon-testimony/. June 22, 2010.