Medical Identity Theft

Recommendations for the Age of Electronic Medical Records

October 2013

Kamala D. Harris, Attorney General
California Department of Justice

Privacy Enforcement and Protection Unit
California Department of Justice
www.oag.ca.gov/privacy

Table of Contents

Message from the Attorney General

Medical identity theft has rightly been called the privacy crime that can kill. When a victim's identity is used fraudulently to obtain medical goods or services, whether the scam involves overbilling Medicare by generating false records of treatment, abusing patient information to obtain prescription drugs like OxyContin, or any other permutation of this crime, the result is the same: medical records become contaminated with erroneous information such as a false diagnosis or inaccurate medical history. This in turn prevents practitioners from effectively treating their patients and endangers the health of the victims. Medical identity theft is thus, above all, a quality-of-care issue.

Medical identity theft also imposes financial harm and administrative burdens on victims including hospitals, insurers and particularly patients, for whom it is often stressful, complicated, time-consuming and costly just to obtain copies of their medical records let alone to correct inaccuracies in their records resulting from fraud. Unfortunately, many health care providers do not have adequate means to respond to patient reports of errors in their records.

The recommendations set forth here will help to prevent, detect and mitigate the effects of medical identity theft. In developing our recommendations, we consulted with experts in the fields of medical records administration, health informatics, information security and patient privacy, as well as with health care providers. We appreciate their contributions and commitment to addressing the problem in their organizations and in the industry.

The Affordable Care Act has escalated the migration to electronic medical records. With this migration, the health care industry has an opportunity to focus on medical identity theft as a serious quality-of-care issue and to learn from other industries that have experience in detecting and responding to fraud in electronic transactions. I urge the industry to take action during this window of opportunity.

Sincerely,

Attorney General Kamala D. Harris

Executive Summary

Medical identity theft corrupts medical records with erroneous information that can lead to incorrect diagnosis and treatment, and is therefore a quality-of-care issue that directly impacts the core mission of the health care industry.

One form of medical identity theft, accounting for nearly half the victims, should begin to decline as the Patient Protection and Affordable Care Act takes effect. Nearly half of victims report having shared their own identifying information with a relative or friend to allow that person to obtain medical services, according to a survey recently released by the Ponemon Institute. By extending coverage to many who are now uninsured or underinsured, the Affordable Care Act should help to stem the increasing rate of medical identity theft.

Unfortunately, victims of medical identity theft often lack rights and resources comparable to those available to address financial identity theft, such as free annual access to records, flags on compromised identities and records, easy access to records suspected of containing fraudulent information and correction of information resulting from fraud. With the Affordable Care Act's mandate to move to electronic medical records, the health care industry has an opportunity to develop best practices to address remaining medical identity theft issues.

The California Attorney General is offering *Medical Identity Theft: Recommendations for the Age of Electronic Medical Records* as a best practices guide for health care providers, payers, health information organizations and policy makers. The guide focuses on the impact of identity theft on the integrity of medical records, which poses the greatest risk to victims and is often unaddressed by existing procedures and remedies.

Key Recommendations

For Health Care Providers

- Build awareness of medical identity theft as a quality-of-care issue within your organization.
- Make patients aware of medical identity theft, which includes using someone else's medical ID or sharing theirs and its potential consequences.
- Deploy technical fraud prevention measures such as anomaly detection and data flagging, supported by appropriate policies and processes so that all red flags are appropriately investigated.

- Implement an identity theft response program with clear written policies and procedures for investigating a flagged record. Train staff in all relevant departments on these policies and procedures.
- Offer patients who believe they may be victims of identity theft a free copy of the relevant portions of their records to review for signs of fraud.
- When an investigation reveals that a record has been corrupted by medical identity theft, promptly correct the record. Use a procedure appropriate for the circumstances, such as removing the thief's information from the victim's record and placing it in a separate "medical identity theft file," or leaving the thief's information in the victim's record but flagging it as not belonging to the victim.

For Payers

- Make Explanation of Benefits statements patient-friendly. Include information on how to report any errors that are discovered.
- Notify customers who have been identified as victims of medical identity theft by email or text or other agreed upon timely method whenever a claim is submitted to their account.
- Use automated fraud-detection software to flag suspicious claims that could be the result of identity theft.
- When medical identity theft is confirmed, the first priority should be correcting the patient's claims record to eliminate the possibility that benefits could be capped or terminated.

For Health Information Organizations

- Build system capabilities that can assist in the prevention, detection, investigation and mitigation of medical identity theft.
- Adopt policies and standards that recognize the possibility of medical identity theft. Include specific policies relating to medical identity theft as part of privacy and security policies and procedures.

For Policy Makers

- When collaborating on the development of standards and software for electronic health records and health information exchange, consider the policies and procedures recommended in this guide. The recommendations could also form the foundation of standard policies for industry self-regulation.
- The U. S. Department of Health and Human Services should include a medical identity theft incident response plan as a certification requirement or as one of the best practices

they are currently developing for health information organizations or exchanges and Accountable Care Organizations.

Introduction

Medical Identity Theft

Medical identity theft is defined as the fraudulent use of an individual's identifying information in a health care setting to obtain medical services or goods, or for financial gain. The crime may be perpetrated by an outsider using the stolen identification of another or by an insider abusing access to patient information. This type of identity theft first received widespread attention in a report published by the World Privacy Forum in 2006.[1]

There are two primary ways in which medical identities are misused. The first is consensual: An individual may knowingly provide his or her identity to someone else in order to allow that person to obtain medical goods or services. A 2013 study by the Ponemon Institute found that nearly half (47 percent) of medical identity theft victims shared their identifying information with someone they knew. The most common reasons cited by survey respondents were that the family member or friend did not have insurance or could not afford to pay for the treatments.[2] This type of medical identity theft should decline as the Patient Protection and Affordable Care Act extends health care coverage to many who are now uninsured or underinsured.

Medical identity theft also occurs when the victim does not know the perpetrator, as the result of lost or stolen identification or of an insider abusing access to records. For example, a Seattle woman discovered that her newborn son's Social Security number had been stolen when she received a bill addressed to her son from a clinic prescribing him OxyContin for a work-related back injury.[3]

An insider may use access to patient medical records to perpetrate a fraudulent billing scheme. In one case, a psychiatrist entered false diagnoses of drug addiction, depression and other psychiatric disorders into the records of individuals who were not his patients. He did this in order to submit false bills to insurers. One of the victims discovered a false diagnosis of severe depression in his records after he had applied for employment.[4] Criminal enterprises also perpetrate elaborate billing scams, often with Medicare as the target.

The impact on the victim's medical records is, of course, dangerous regardless of the motivation behind the use of the information and regardless of whether the fraud was perpetrated by a relative or by a stranger.

Medical identity theft is often underreported, as it is difficult to detect or misreported simply as health care fraud without taking

into account its impact on patients. Nevertheless, it is clearly a significant problem. The World Privacy Forum estimated the number of victims in 2003 as between 250,000 and 500,000, based on the Federal Trade Commission's (FTC) Clearinghouse and Identity Theft Survey data for that year.[5] In a 2008 report, the U.S. Department of Health and Human Services cited a figure of 250,000 victims, based on FTC survey data from 2006.[6] More recently, the Ponemon Institute calculated that there were adult 1.84 million victims in 2013. This constitutes a 21 percent increase over the previous year.[7]

The impact of medical identity theft on patients can be devastating. The Ponemon study extrapolated an average cost of $18,660 for the 36 percent of medical identity theft victims who had to pay out of pocket. The total value of out-of-pocket costs incurred by U.S. victims was estimated at $12.3 billion.[8] More importantly, in addition to leading to loss of benefits and unwarranted financial obligations, medical identity theft can corrupt health records and put the health and safety of the patient at risk.

While knowledge of the crime has grown, adequate means for preventing, detecting and remedying the problem are not always in place. Potential and actual victims of medical identity theft lack rights and resources comparable to those available to address financial identity theft. Such rights and resources include free annual access to records, flags on compromised identities, easy access to records suspected of containing fraudulent information and prompt correction of information resulting from fraud.

By mandating a transfer to electronic medical records, the Affordable Care Act offers the industry an opportunity to address these problems. The responsibility for preventing, detecting and mitigating medical identity theft lies primarily with the health care industry, although patients can also help. The industry must evaluate its current practices for privacy protection and data security and implement appropriate counter-measures against medical identity theft. Strategic use of technology can help prevent, detect and mitigate the harmful effects of the crime. Importantly, providers must correct compromised records and thereby eliminate the persistent risk that erroneous medical information poses to victims' health and quality of care. Although consumers can take steps to help prevent and detect medical identity theft, victims cannot correct compromised records on their own.

We also note that errors in medical records that are not the result of medical identity theft can pose the same risk to patient

safety. Many of the recommendations in this guide are applicable to the detection and correction of those errors, as well.

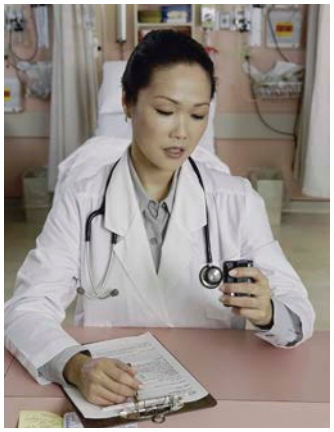
Nature and Scope of this Guide

In July 2012, the Attorney General created the Privacy Enforcement and Protection Unit, with the mission of protecting the inalienable right to privacy conferred by the California Constitution. The Privacy Unit enforces state and federal privacy laws, and develops programs to educate consumers and businesses on privacy rights and best practices.

While personal information stolen from medical records, such as a name and Social Security number, may also be used to commit other forms of identity theft – for example opening credit accounts – financial identity theft is not the subject of this guide. The guide focuses on the unauthorized use of personal information in health care settings and, in particular, on the impact on medical records.

The recommendations offered here are not regulations, mandates or legal opinions. Rather, they are intended to contribute to the development of best practices for health care providers and related organizations to follow in managing patient information in ways that promote and protect individual privacy interests.

In developing this guide, we were fortunate to be able to draw on the knowledge of experts from the fields of medical records administration, health informatics, information security, health care providers and patient privacy. Their contributions were significant and we are grateful to them all.[9]



Key Terms

The following definitions are for key terms as used in this guide.

Business associates are entities under contract to health care providers that handle medical records on behalf of the providers.[10]

Detection means using manual and technological means to identify past, present and attempted medical identity theft. Detection includes determining what information was involved and how, when and where it was stolen and used.

HIO is a health information organization that manages and oversees health information exchange (HIE) functions. Such an organization is considered a business associate of its member health care providers.

Medical identity theft is the fraudulent use of an individual's identifying information

in a health care setting to obtain medical services or goods, or for financial gain.

Medical record is a permanent record that contains identifiable medical information, and is intended for use in decision-making relevant to a patient's health coverage, diagnosis and treatment. Medical information is identifiable when it includes a patient's name, Social Security number, address, insurance number or other identifier that links to an individual. A medical record can be in paper or electronic form and can be maintained by payers, providers and/or business associates.

Mitigation is the process of assisting victims of medical identity theft in repairing the damage once the problem has been discovered. Victims can be individuals, providers or payers. Mitigation involves minimizing the risks and costs to all victims and doing everything possible to restore medical and financial records to the status quo ante.

Payers include insurers, third-party bill payers, government health plans such as Medicare and Medicaid and self-insured health plans.

Prevention means ways to stop medical identity theft from occurring, with a focus on preventing its impact on patient medical records.

Providers include hospitals, clinics, small practices, pharmacies and diagnostic facilities like laboratories and imaging centers.

Recommendations for Health Care Providers

This section describes problems that health care providers face as the result of medical identity theft and recommends measures to assist in the prevention, detection and mitigation of the crime.

The overall recommendation for all health care providers is to build awareness of medical identity theft and implement an identity theft response plan. The plan should include a team prepared to respond to any evidence of medical identity theft. In larger provider organizations (such as medical centers, hospitals and multi-facility clinics or diagnostic centers), the team, which might be headed by the privacy officer, should include representatives of corporate-level administration, information technology, information security, compliance, finance (billing), security, human resources, clinical departments, labs and imaging and patient registration. The team of a smaller provider (small to medium practice group, single facility clinic, lab or imaging operation) should include individuals concerned with front-office reception, office management (records, billing, human relations) and information technology, as well as the practitioners. Business associates should be included in your response plan when appropriate.

The team should develop and implement policies and procedures for the prevention, detection and mitigation of medical identity theft. The recommendations here are offered for inclusion in providers' medical identity theft response plans.

Prevention

This section covers suggestions for health care providers on how to prevent inaccurate information from entering medical records as the result of medical identity theft.

Know Your Staff

Pre-employment background screening and appropriate access controls—including cutting off system access by terminated employees—can curb internal misappropriations of medical identities.

Recommended practice: Exercise care in hiring individuals who have access to patient information or medical records. Employee background checks can help in identifying candidates with a criminal history and should be a standard part of the hiring practice. Screen temporary hires and volunteers as well.

Recommended practice: Include effective role-based access controls as a component of your information security program. Such

controls should be built into electronic health record (EHR) systems. Access limits should apply to paper as well as electronic records.

Know Your Patient

Recommended practice: Require patients to show a copy of their health insurance card (if not paying in cash) at registration. Consider requiring a photo ID and training employees to check whether the photograph and descriptive details (such as race, gender, height, weight and hair and eye color) match the ID. Whenever practical, embed a patient photo in the EHR or supplementary database. Do not scan a government-issued ID, such as a driver's license and incorporate the scanned data into the medical record. Doing so would add unnecessary personal information to the record that increases the risks of identity theft.

Recommended practice: If a patient requiring emergency care presents a questionable ID or no ID, the patient must generally be treated. Make sure there is a place in the intake record to note this and take further steps to validate the patient's identity. One simple additional step could be to ask the patient which doctor she saw last.

Basic Patient Education

Recommended practice: Educate patients about their right to review and request corrections to their own medical records.[11] Provide clear instructions to patients on how they can get a copy of their records. Use the principal languages of your patient population in brochures available at registration counters and on your website.

Recommended practice: Make patients aware of the crime of medical identity theft. Clarify that using someone else's medical ID or sharing theirs is a crime and highlight the potential dangers. This might be done with a poster visible at registration.

Recommended practice: Clinical Care Summary documents may have a role in preventing medical identity theft.[12] This document contains both clinical and individual identifying information. Include a clear caution at the top of the page, encouraging the patient to protect the confidentiality of the information. If the document includes the patient's insurance ID number, it should be truncated or better yet, not shown at all. When handing the patient a copy at the end of a visit, ask the patient to verify the accuracy of its information. A patient who receives an electronic document should also be asked to verify the information. This can be a way to detect and promptly correct errors in medical records.

Detection

Detecting medical identity theft can be a manual or technological process—or both—in which providers and patients have a role to play. Early detection allows for action to reduce the risk to quality of care and patient safety.

Use "Red Flags"

Recommended practice: Use "red flags" or other means of tagging discrepancies in appropriate systems and at different contact points with patient and medical records to note a problem that requires

further investigation. Electronic records systems should allow for the flagging of any new issues that come up in the registration process. Unless there is a red flag that clearly disqualifies a patient (such as refusal to show any ID, other than in an emergency room), the provider should proceed to treatment. Providers may want to develop their own flags based on their experience with record anomalies. The following checklists highlight some basic issues that should raise a question.[13]

Red flags at patient registration

- ID appears altered or forged.
- ID photo does not match the person presenting the ID.
- ID information (e.g., surname, physical characteristics, address) does not match information on file.
- Presentation of a Social Security card or number that duplicates one that is already part of another patient's registration record.
- Presentation of an insurance or Medi-Cal card that duplicates one that is already part of another patient's registration.
- Presentation of an insurance or Medi-Cal card with information in the benefit-eligibility checking process that doesn't match that of the person presenting the card.
- Duplicate demographics, such as another patient with the same name, address or telephone number already on record.
- The patient or someone accompanying the patient, states or intimates at any time during the encounter that the patient is using a false identity.
- The patient, law enforcement or a credit bureau notifies you that the patient is a victim of identity theft.
- Note any flag in a previously compromised record to ensure that the identity theft is not reactivated at a later date.

Red flags in billing and records management

- Mail sent to known patient returned despite address verification.
- Complaint received from a patient about a bill for services or products that the patient never received.
- Insurer denies payment because charge is improbable or impossible (for example, appendix removed for a second time).
- Duplicate files appear to exist for the same patient.
- Patient bills are returned as undeliverable but health care charges continue to accrue.

Red flags for professional staff

- Individual presents medical background or information inconsistent with the existing medical record.
- Individual is unaware of basic medical information within an existing medical record.

- Patient denies information within an existing medical record.
- Lab or other clinical test results are inconsistent with information in an existing medical record (for example, colonoscopy results in a record indicate pre-cancerous polyps, but a subsequent test result has no mention of polyps) or with the patient's presentation (for example, a biopsy in the record indicates basal cell carcinoma in a discolored patch of skin on the patient's right cheek, but the patient presenting for treatment does not have discolored skin).

Recommended practice: Train employees to identify discrepancies that need to be flagged. Maintain checklists of issues worth flagging, based on the above lists and your experience with record anomalies.

Respond to a Flagged Record

Recommended practice: Establish clear written policies and procedures for investigating a flagged record and determining if the problem is the result of a registration or operational error or actual medical identity theft. Require all business associates and your downstream vendors to implement red flag policies and procedures. Adopt your own practice-specific versions of the suggestions below for following up on flagged records, based on a risk analysis. Responses to flags may include the following:

- Require an employee who flags a record for error or suspicion of medical identity theft to alert the medical identity theft team leader or security incident response team leader, either automatically through the system with a form that describes the problem or through another chosen means of communication.
- Require the medical identity theft team leader to notify team members from systems and records management, patient registration, patient accounts and compliance of the matter.
- Place affected patient accounts on hold pending the outcome of the investigation.
- Require all departments involved in the medical identity theft or security incident response team to use all manual and technological resources to determine if the problem arose from a registration error (for example, a typo), an operational error (for example, a new file opened by mistake, because a patient's surname changed by marriage or divorce; or the electronic record system merged the medical records of two different patients) or actual medical identity theft.
- If the team has insufficient information to make a final determination, require that

it notify and interview the patient whose record is in question.

- Maintain a database of identities that have been used fraudulently as a tool for future detection.
- Create a central location in your system of records (including an electronic billing or practice management system) to note information captured from a medical identity theft investigation, with a follow-up policy for what to do if this appears. You may have to be creative in developing such a system (for example, an EHR, Practice Management or Patient Administration system where patient information is created, stored and fed into other systems).
- Similarly, identify a place in paper charts of medical records to note information captured from a medical identity theft investigation.

Recommended practice: Train employees to check for and follow up on, red flags at patient registration, during administrative processing, during financial processing (claims submission and patient billing), at periodic audits of electronic health record and patient portal access and during clinical encounters with patients.

Respond to Patient Complaints About Identity Theft

Recommended practice: Establish a regular procedure for following up when a patient has a complaint or question about a bill or about information in a medical record that the patient says is not related to him or her.

- Ask the patient for details, perhaps using a form to capture the information necessary to investigate the complaint. Make sure the patient signs the form.
- Ask for identification from the person making the complaint (such as copies of photo ID, Social Security card, health plan member card).
- Send the complaint to the appropriate department or individual.
- Once the necessary documentation has been gathered, the medical identity theft team should investigate by reviewing the patient's medical records, and other documentation including billing records, business associate stored records and record-access audit logs. Investigators may also compare signatures in the records with new ones requested from the patient. Meanwhile, place financial records on hold.
- If an investigation determines the problem is either an error or the result of medical identity theft, notify the patient and follow your mitigation procedures.
- If someone other than your own patient complains (for example, if someone questions a bill from you for a service he or she did not receive), investigate for medi-

cal identity theft. If the investigation shows that medical identity theft has occurred, rather than just a billing error, notify the complainant of that result and advise her on how to proceed (for example, by contacting her insurer, filing a police report, consulting the consumer information at *www.oag.ca.gov/identity theft*).

Help Patients Detect Errors and Fraud: Patient Access Rights

EHRs can simplify meeting records requests and improve the role of patients in detecting signs of fraud in their medical records. With the patient's participation, many errors could be detected sooner and potential medical identity theft flagged before the harm escalates. Patients may also have an important role to play in any internal investigation of medical identity theft, by confirming whether information in a record belongs to them.

Recommended practice: Inform patients that they are entitled to access their medical records and to receive copies of the records. Simplify your process for responding to record requests from patients, particularly from a patient who suspects medical identity theft.

NOTE: Some providers have questioned whether HIPAA permits a patient whose record may have been compromised from seeing that record because it may contain another person's personal health information. The Office for Civil Rights endorses and provides a link to guidance from the Federal Trade Commission for health care providers and health plans: "Some medical providers and health plans believe they would be violating the identity thief's HIPAA privacy rights if they gave victims copies of their own records. That's not true. Even in this situation, patients have the right to get a copy of their records."[14]

Recommended practice: Offer patients who believe they may be victims of medical identity theft a free copy of the relevant portions of their records to review for signs of fraud. Give confirmed victims of medical identity theft regular access to their records in order to monitor whether the problem continues with other providers.

Recommended practice: If you support online patient portals that patients can use to access at least summary information about their current health conditions, test results and medications, there should be a clear and easily visible message on the login page, requesting patients to review these records periodically for accuracy and providing some way to report inaccuracies.

Use Technology to Detect Identity Theft and Errors

Recommended practice: Use the audit capabilities of electronic records to aid in detecting unauthorized access by insiders. When such an intrusion is indicated, providers should conduct a follow-up check of records for possible inconsistencies or other inaccuracies.

Recommended practice: Build demand for provider-side detection software, which can improve the detection of medical record errors and fraud beyond the current largely manual process. Currently, there is only a handful of such applications and they are generally only cost-effective for large-scale providers.

Mitigation

Reducing or eliminating the consequences of medical identity theft for patients is the most important goal of any mitigation process. Inaccurate medical records imperil quality of care and a lack of mitigation efforts can bring regulatory intervention, legal action, harm to a provider's reputation and other intangible damage. It is patients, however, who can be harmed most seriously—even fatally—by errors introduced into their records as the result of medical identity theft.

Mitigation Policies and Procedures

Recommended practice: Establish clear written policies and procedures for handling records that your investigations show have been corrupted by medical identity theft. Consider the following steps for inclusion in your mitigation, with adaptations based on your experiences with handling medical identity theft cases and your practice environment.

Correct the record, by whatever procedure is most appropriate and effective for the particular circumstances. Possible actions include the following:

- Remove the thief's medical information from the victim's record and place it in a separate file (linked or not linked) labeled "medical identity theft."
- Leave the thief's information in the victim's record but annotate it clearly as not belonging to the victim.
- Start a new record for the victim, linked to the old compromised record.
- Notify relevant parties: provider billing, insurer, collection agencies and credit bureaus.
- Notify the patient/victim of the outcome of the medical identity theft investigation, steps taken to mitigate the problem and steps the patient can take to protect herself from further harm. Providing a letter on your letterhead will be helpful to a patient in following up with creditors and law enforcement.

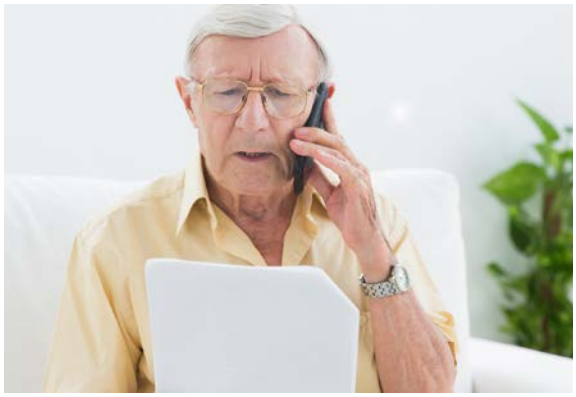
Recommended practice: In addition to the vital step of correcting the medical records, direct the victim to information on how to check and correct any possible impact on his or her credit records. Such information is available from the California Attorney General.[15]

Propagating Corrections Across Record Systems

A complete medical identity theft incident response plan should enable you to correct internal medical and financial records that have been affected by the theft.

Recommended practice: When an amendment to a record results from an investigation undertaken in response to a patient's request, make every effort to inform your business associates and any other parties the patient identifies.[16] When an amendment results from an internal investigation or was initiated by someone other than the patient, help to propagate corrections to a victim's other providers, insurers and any third parties that handle or maintain medical records in their capacity as business associates of the provider. In such cases, it is recommended that providers follow the same process they are required to follow for an amendment resulting from a complaint or request initiated by the patient.

One easy way to alert others to record amendments is to use the Continuity of Care Document, which is shared electronically among providers through a health information exchange.



Recommended practice: If you participate in a health information exchange, follow the established policies and procedures, based on roles and responsibilities described in the data use agreements, to provide corrected and updated information and/or red flags on compromised information to a patient record. This may require reconciling different data handling policies; for example, there may be a different policy for correcting data that originated internally than for data received from an HIE partner.

Recommendations for Payers

Payers for health care services also have an important role to play in the prevention, detection and mitigation of identity theft. Payers are critical in helping victims, who could lose their insurance or see their benefits capped because of medical identity theft. An anomalous transaction or a questioned bill may be the first or only indication of medical identity theft.

Recommended practice: Establish a medical identity theft incident response plan with clear procedures and policies and establish a dedicated team to investigate both consumer complaints about errors and suspicious transactions. There should be detailed procedures for internal investigation, as well as procedures to follow if the claim cannot be resolved internally.

Prevention

Insurers handle an exceptional amount of personally identifiable information, including medical claims history and detailed demographic data. Insurers share all of this information with others, such as physicians' offices and pharmacies and third parties that process claims or collect unpaid debts. Distributing medical information to multiple parties can increase its vulnerability, which can result in medical identity theft and fraudulent insurance claims.

Train Employees and Associates on Medical Identity Theft Response

Recommended practice: Establish reasonable and appropriate data security standards and safeguards—administrative, technical and physical. This includes training employees not only on legal requirements on privacy and security, but also on organizational policies including how to respond to medical identity theft. Obtain satisfactory assurances that your business associates also have appropriate safeguards.

Keep Current on Fraud Trends

Recommended practice: Require your fraud investigation team to keep up with trends in claims fraud. This has implications for both prevention and detection. It may enable you to detect a fraud as soon as it occurs and alert your employees to take certain preventive measures, and to alert any providers who may be affected.

Detection

Make Explanation of Benefits Statements Patient-Friendly

Recommended practice: The Explanation of Benefits (EOB) is among the first documents a patient receives after a medical encounter. If you make your EOBs easy

to understand, you can enable your patients to recognize errors that may be signs of medical identity theft. Use plain language and a standardized format and provide an explanation of "how to read this document" in the statement and on your website. Provide explanations of any abbreviations and codes used. Use the EOB to explain to patients how to report any errors they discover. Be sure to train employees to respond to consumer reports of errors in EOBs.

Recommended practice: Provide information about medical identity theft as part of routine communications with customers. Include advice on how to prevent it (such as keeping insurance cards in a safe place and not sharing them), how to detect it (such as what to look for in EOBs) and how to follow up on errors or questions (where and how to report the error, how to order copies of medical records).

Notify Victims When a Claim Is Submitted

Recommended practice: Implement a process to notify customers who have been identified as victims of medical identity theft by email or text—the best means because it can be in near-real time—or by some other agreed upon method when a claim is submitted to their account. Transmit only the minimum information a customer needs to verify whether the claim is valid, such as the date of service and the provider's name. The notice should provide a toll-free number for the customer to call if he or she believes the claim is in error.

Fraud Detection Software

Recommended practice: Use fraud detection software where appropriate. Such software is likely to be more useful to you than to providers in flagging suspicious claims, including those originating from providers and other internal actors, outside thieves or criminal operators who are gaming the claims systems. There are several different approaches to the automated detection of fraud.

- *Pattern matching* can be manual or application-based or both. You can use a number of criteria to identify patterns that may indicate fraud. For example: Does a provider have several locations in the same or adjacent zip codes and is one patient being treated at more than one or all of them? Are there unusual surges in the overall number of claims—or of certain types of claims, such as claims for particular types of medications—at a location or group of locations that belong to one provider?
- *Predictive modeling* statistically analyzes known frauds in historical claims data and looks for similarities in new claims. Predictive modeling can help

to reduce the false positives, which in turn saves time that would otherwise be spent investigating them.

- *Anomaly detection* looks for outliers in behavioral patterns. Examples would be an otolaryngologist who submits claims for chest X-rays at a much higher rate than similar specialists in the same town or region or a claim for a PSA (Prostate-Specific Antigen) screening submitted to an account belonging to a female.

Recommended practice: Your fraud detection software should flag records to trigger an investigation. While some flags may justify rejecting a claim outright, you should investigate flags whenever possible to determine if there is simply an error in the claim submission or reason to suspect fraud.

Mitigation

If a payer's investigation of a flag or patient's complaint about a billing error confirms medical identity theft, the first priority should be correcting the claims record to eliminate the possibility that the patient's benefits could be capped or terminated.

Recommended practice: In addition to avoiding payment of fraudulent claims and, if possible, recovering on fraudulent claims already paid, act quickly to mitigate the damage to consumers and support their efforts to clear problems related to their credit and pursuit of identity theft claims.

- If the investigation confirms identity theft, notify the insured (if he or she was not the one who reported a billing error) and the provider who submitted the erroneous claim immediately. Notify the provider as soon as you begin investigating the claim.
- When possible, notify all entities, including business associates, that may have received incorrect claims data or other related health information.
- If concluding an investigation requires additional medical information, refer the claim to the provider for investigation, unless the provider is the subject of the investigation.
- While only the provider who submits a claim can modify it, you may request supplementary information about a questionable claim from the provider (a discharge summary, for example). You may also follow up by contacting the provider to discuss the claim further. If you deny a claim, note the reason in a denial code in the EOB. If the reason for denial is suspected fraud, notify the provider directly and recommend that the provider investigate. If you suspect the provider may be involved in the fraud, contact the authorities to investigate.

Recommendations for Health Information Organizations

Encouraged by federal stimulus money and the carrot and stick of Meaningful Use incentives, Health Information Organizations (HIOs), with a few well established exceptions, are just beginning to form and operate. The primary responsibility of the HIO is to manage and oversee the health information exchange (HIE) functions. To do this, HIOs must establish policies and procedures to ensure that information-sharing among health care providers and other participants is designed to protect the confidentiality, privacy and security of the information. HIOs are therefore well positioned to play a role in detecting medical identity theft and preventing its spread. As HIOs develop standards and policies, they should consider how to address medical identity theft.

Build technologies into HIO systems that can assist in the prevention, detection and mitigation of medical identity theft. Depending on your access to the information that is being exchanged, records compromised by identity theft might be identified at the HIO level as they are passed through to providers. HIOs and ACOs should have policies and standards that recognize the possibility of medical identity theft. Include policies relating to medical identity theft in your broader privacy and security policies and procedures. Suggested policies and technology solutions are noted below.

Prevention

Recommended practice: For the most part, HIOs do not currently have the technical ability to receive "red flags" that exist in a provider's records. There is no current specification for such notifications in industry standards HL7, CCD or Consolidated CDA (the next phase of CCD) transmissions between providers.[17] Encourage the addition of such a specification to allow the transmission of flags to indicate compromised records through the HIO to other providers.

Detection

Recommended practice: Make your policies consistent with those of other on-going initiatives, such as health information exchange, ACOs, IDNs and PCMHs,[18] as well as the later stages of Meaningful Use. Now is the time to consider how, in the future, HIOs can extend their usefulness as record aggregators to give patients the ability to access their records from multiple providers. This would allow patients to detect and report errors more easily and

efficiently. Develop a specific patient access and review policy to assist in the detection of identity theft issues.

Mitigation

Recommended practice: Develop the ability to receive and disseminate to participating providers any red flags indicating that a record has been confirmed as being compromised by medical identity theft or is under investigation for suspected medical identity theft. One option is to enable your community Master Patient Index to record the presence of a flag transmitted by a member provider, which could then be further disseminated.

Recommended practice: Without specifications for "red flag" alerts, an alternative practice is to use messaging capabilities to prevent the spread of incorrect medical information. This could automatically communicate system-wide alerts about records known to be compromised by medical identity theft or propagate corrections to known compromised records.

Recommended practice: Provide the ability to create and maintain a flagging audit trail of records wherever medical identity theft has been confirmed. This would assist with mitigation by helping to locate compromised records that have spread across a number of providers, thus facilitating corrections to the records.

Recommendations for Policy Makers

Developing policies and standards for the prevention, detection and mitigation of medical identity theft requires collaboration among all stakeholders in the health care industry. The industry is already collaborating to build a health care infrastructure for the 21st century and the issues posed by medical identity theft should be included in that process. Government policy-making bodies can contribute by providing guidance for dealing with the problems caused by medical identity theft under existing laws and regulations. Policy makers should take advantage of the lessons learned from in a decade of dealing with other forms of identity theft. Policy makers should review proven identity theft policies and procedures in order to identify actions that may be applied to medical identity theft. Other industries with experience with electronic information and electronic transactions, such as financial services, have useful knowledge to share about fraud detection and response.

The issues that should be addressed by policy makers include the following:

- Electronic flagging capabilities
- Certification requirements for systems
- Authentication requirements for users and individual authentication standards for providers, payers and perhaps eventually, patients
- Audit requirements
- Notification and dissemination requirements
- Requirement that an individual who posts a flag conclude the response process and appropriately disseminate the resolution
- Development, as feasible, of standardized data sharing agreements, policies and procedures in support of medical identity theft investigation across enterprises.[19]

The following recommendations are offered for health care industry groups and public policy makers to consider.

Recommendation: Industry groups that are collaborating now on the development of standards and software for EHRs and HIEs should consider the recommendations in this guide as they develop policies and procedures. The recommendations could also form the foundation of standard policies for industry self-regulation.

Recommendation: The Office of the National Coordinator in the U.S. Department of Health and Human Services should include

a medical identity theft incident response plan as a requirement for certification or as one of the best practices being developed for HIOs and ACOs.

Recommendation: The Office of the National Coordinator, in the U.S. Department of Health and Human Services, should include medical identity theft "red flag" recommendations or multiple issue/resolution flag recommendations in Stage 3 Meaningful Use guidelines. Technical standards can enable care delivery organizations and HIOs to share issues and resolutions through

standardized data-sharing "red flag" codes as a part of Meaningful Use requirements.

Acknowledgements

A group of experts in health care and privacy provided invaluable consultation and advice in the development of this guide. Their contributions are gratefully acknowledged.

Chris Apgar, President and CEO, Apgar and Associates, LLC

Robin Bowe, Compliance Coordinator and Privacy Officer, Kern Medical Center

Peter Brown, Member of the Board, OASIS, Editor of the OASIS Privacy Management Reference Model

John Chapman, National Trainer, TBG Fraud Solutions

Pam Dixon, Executive Director, World Privacy Forum

Robert Gellman, Privacy and Information Policy Consultant

Reece Hirsch, Attorney, Partner in FDA and Healthcare Practice, Morgan Lewis & Bockius LLP

Pam Lane, Deputy Secretary of Health Information Exchange, California Health and Human Services Agency

Sokkim Lim, Pharm.D, Specialty Pharmacist, UCSF Department of Clinical Pharmacy

John Macaulay, MD, Health Information Privacy and Security Consultant

Jing Wang MacKenzie, MD, Chief of Staff, ACS Integrated Solutions, Aetna

Dave Minch, President and COO, HealthShare Bay Area

Matt Morris, National Trainer, TBG Fraud Solutions

Dr. Larry Ponemon, Chairman and Founder, Ponemon Institute

Harry Rhodes, Director of Practice Leadership, American Health Information Management Association

Sheryl Vacca, Senior Vice President and Chief Compliance and Audit Officer, University of California

In addition, the project would not have been possible without the excellent work of Lori Hack and Linda Ackerman of Object Health, who drew on their broad and deep experience in health care and privacy to conduct the research, coordinate meetings and working sessions and document the results.

Bibliography and Resources

AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft." Journal of AHIMA 79, no.7 (July 2008): 63-69, available at *http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039058.hcsp?&dDocName=bok1_039058*

Federal Trade Commission, "Medical Identity Theft: FAQs for Health Care Providers and Health Plans," *http://business.ftc.gov/documents/bus75-medical-identity-theft-faq-health-care-health-plan*

Ponemon Institute, "Third Annual Survey on Medical ID Theft," June 2012, available from the Institute, *www.ponemon.org*

U.S. Department of Health and Human Services, Office of the National Coordinator, "Medical Identity Theft Final Report" (2009), available at *http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&cached=true&objID=1177*

World Privacy Forum, "Medical Identity Theft: The Information Crime that Can Kill You" (2006), "Medical Identity Theft: Best Practices and Solutions for Providers" (2007), "Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers" (2008), available at *www.worldprivacyforum.org/medicalidentitytheft.html*

Notes

[1] World Privacy Forum, "Medical Identity Theft: The Information Crime that Can Kill You" (May 2006), available at *www.worldprivacyforum.org/medicalidentitytheft.html*.

[2] Ponemon Institute, "2013 Survey on Medical Identity Theft" (September 2013), page 15, available from the Ponemon Institute, *www.ponemon.org*.

[3] "The Imposter in the ER: Medical identity theft can leave you with hazardous errors in health records," *www.msnbc.msn.com/id/23392229#.T5GxHulWq-8*.

[4] U.S. v. Skodnek, 933 F.Supp. 1108; 1996 U.S. Dist. LEXIS 9788 (D. Mass. 1996).

[5] World Privacy Forum, op.cit, page 22.

[6] U.S. Department of Health and Human Services, "Medical Identity Theft Environmental Scan" (October 2008), page 7, available at *www.healthit.gov/providers-professionals/onc-commissioned-medical-identity-theft-assessment*. Although the FTC's 2006 Identity Theft Survey was based on consumer recollections and was not specifically designed to examine medical identity theft, it was one of the few attempts to measure the frequency of the crime.

[7] Ponemon, op. cit., page 4.

[8] Ibid., page 5.

[9] See the Acknowledgements section for a list of our primary advisors on the project.

[10] The Privacy Rule under the Health Insurance Portability and Access Act (HIPAA) provides a specific definition of "business associate" at 45 CFR § 164.314(a); this has been modified by the HITECH Final Rules at § 160.103 to include specifically HIOs, E-prescribing Gateways and other providers of data transmission services.

[11] For access to records, see HIPAA, 45 CFR § 164.524, California Health & Safety Code § 123110 subdivision (a) and California Civil Code § 1798.32.

[12] Meaningful Use compliance, a set of practice standards in the HITECH portion of the 2006 American Recovery Reinvestment Act, requires giving patients a clinical summary of their treatment within three days of their current visit, either electronically or in paper at the election of the patient.

[13] These checklists have been adapted from the John Muir Health Medical Identity Theft Prevention Program. Similar and additional red flags for health care providers may be found in the World Privacy Forum's "Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers."

[14] The link to the FTC guidance, provided by the Director for Health Information Privacy in the Office for Civil Rights, Department of Health and Human Services, is on the page for the HIPAA Security Rule, *www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/*.

[15] See the "Identity Theft Victim Checklist," from the California Attorney General, at *www.oag.ca.gov/idtheft*.

[16] See 45 CFR § 164.526(c) – (2), on informing the individual, others designated by the individual and business associates, of amendments to a medical record.

[17] HL7 is the global authority on standards for interoperability of health information technology. CCD is a Continuity of Care Document, an electronic document exchange standard for sharing patient summary information. CDA is Clinical Document Architecture, a markup standard developed to define the structure of clinical documents such as discharge summaries and progress notes. Definitions from Search Health IT at *http://searchhealthit.techtarget.com*.

[18] ACOs are Accountable Care Organizations, IDNs are Integrated Delivery Networks and PCMHs are Patient-Centered Medical Homes.

[19] CalOHII has developed the MMPA (Model Modular Participants Agreement) to assist HIOs and participants in writing health information exchange agreements. The MMPA provides alternative terms and conditions for different types of HIOs and is available at *www.ohii.ca.gov/calohi/PrivacySecurity/ToolstoHelpYou/ModelModularParticipantsAgreement.aspx*.