WILL THE REAL DR. JOHN SMITH PLEASE STAND UP?
A LOOK AT THE LATEST TRENDS IN HEALTH CARE FRAUD

The health care industry is the biggest target of identity theft on both a national and international level. It also has a human face. Government mandates look to make us healthier, safer and secure—no easy task when confronted with the ethically challenged. This session will present the latest trends in health care fraud, including a look at deceptive practices, medical identity theft, and how to prevent existing and evolving schemes. It will also explore these fraudulent practices from the perspective of the Affordable Care Act and its relevant directives.

You will learn how to:
- Protect your personal health information (PHI).
- Avoid and prevent health care fraud.
- Assess the trends of health care in 2015.

REBECCA BUSCH, RN, CFE, CCM, CPC
President and CEO
Medical Business Associates Inc.
Westmont, IL

Recognized as an expert in her field, Rebecca S. Busch has developed data management practice standards for emerging CDOs, medical data scientists, and auditors that ultimately support and defend complex issues impacting the bottom line. She currently provides technical investigative, audit, and review expertise to various government agencies and expert testimony on health-related issues in both state and federal court. She attributes her company’s success to the development and implementation of a unique analytical work-flow process, “Interactive and Iterative Behavioral Model, System, and Method for Detecting Fraud, Waste, and Abuse,” which identifies all critical tasks, conditions, and standards that promote a stable, dynamic, and scalable health care business.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
**Impact on the Insured**

Health care fraud creates victims. Fraud can result in:

- Being subjected to unsafe or unnecessary medical procedures
- Medical records being compromised
- Insurance information used to submit false claims
- Ineffective, unsafe drugs/remedies prescribed
- Unproven treatments/supplements prescribed
- Fraudulent diagnostic tests (not approved by the FDA) utilized
- Loss of benefit days/capping of insurance benefits

How can a simple decision evolve into a complicated matter? Consider this example. A family member (Joe) lends his insurance card to his brother (John) who has no insurance for surgery. A new hospital system is using a biometric reading of the palm to associate all of John’s data points under his palm biometric reading, which really is associated with Joe. Prior to surgery, John cancelled and informed the hospital that he really was not who he said he was. Why did he ‘fess up to the situation? He realized that all of his records would be associated with his brother, Joe, and he feared that his brother maybe subjected to services that he did not really need.

Another example: Your identity is sold to an individual who did not want his health care issues associated with his name. However, the blood type of the victim and the blood type of the perpetrator are different. What is the impact? Potentially, death if the victim receives the wrong blood type.

This list goes on—individuals need the right information with the right person in order for health care providers to prescribe the right treatment!
WILL THE REAL DR. JOHN SMITH PLEASE STAND UP?
A LOOK AT THE LATEST TRENDS IN HEALTH CARE FRAUD

Deceptive practices/scams, medical identity theft, and corrupt, unsecured data are some of the major players driving the latest trends in health care fraud.

Health care is a tempting target for thieves. Medicaid doles out $415 billion a year; Medicare, the federal scheme for the elderly, doles out nearly $600 billion. A study done in 2012 estimated that fraud (and the extra rules and inspections required to fight it) added as much as $98 billion, or roughly 10 percent, to annual Medicare and Medicaid spending—and up to $272 billion across the entire health system.

Federal prosecutors had over 2,000 health-fraud probes open at the end of 2013. A Medicare “strike force,” which was formed in 2007, boasts of seven nationwide “takedowns.” In one of the latest, in May of 2014, 90 people, including 16 doctors, were rounded up in six cities—more than half of the perpetrators were in Miami, the capital city of medical fraud. One doctor is alleged to have fraudulently charged for $24m of kit, including 1,000 power wheelchairs.

Fraud-fighting has intensified—run jointly by the Department of Health and Human Services (HHS) and the Department of Justice. Between 2011 and 2013, they recovered $8 for every $1 spent. Obvious billing fraud instances such as durable medical kits and home visits were reduced. Home-health fraud got so bad that a moratorium was called on enrolling new providers in several cities. Since tighter screening was introduced under the Affordable Care Act, 17,000 providers were stripped of their license to bill Medicare.

NOTES

In ensuing slides, we will see that fraud migrates from state to state, town to town. Fraud mutates as well. As old scams are discovered, new and better ones crop up. Scams now need to be more sophisticated to succeed. Doctors, pharmacists, and patients now act in league. Scammers overbill for real services rather than charging for nonexistent ones, so now they are harder to spot.

Some criminals are switching from cocaine trafficking to prescription-drug fraud because the risk-adjusted rewards are higher. The money is still good, the work is safer, and the penalties are lighter. These criminal gangs are often bound by ethnic ties: Russians in New York, Cubans in Miami, Nigerians in Houston, etc.

“Medical identity theft incidents rose more than 20% in fiscal year 2014 compared to the year prior.”
—FierceHealthIT

Stealing patients’ identities is lucrative. Medical records are worth more to crooks then credit-card numbers. And, unfortunately, it takes longer for victims to notice that their medical information has been stolen. The Government Accountability Office has recommended that the CMS remove Social Security numbers from Medicare cards to prevent fraud but they have yet to do so.

Individuals should be reviewing their claims data annually to evaluate if bills have been sent in their name for services they have never received. Of those unknown providers, copies of medical records should be requested in order to validate the commingling of any health information that does not belong to the individual. Remember that HIPAA allows an individual to request amendments of their records for incorrect information associated with their name.
There are four types of identity theft:

- **Individual identity theft**: an intent to use another’s individual identity to commit, aid, or abet any unlawful activity. Common themes include access to financial assets or creating false credit lines to access cash or property. Often results in compromised credit reports, loss of assets, and significant disruption of day-to-day life.

- **Medical identity theft**: an intent to use another’s individual identity to commit, aid, or abet any unlawful activity within health care. Common themes involve getting access to unauthorized health care services. Often results in the creation of false health information under the individual’s name and additional debt for payment of services never rendered.

- **Professional identity theft**: an intent to use another’s professional identity to commit, aid, or abet any unlawful activity. Common themes involve using a doctor’s identity to submit a false claim. Often results in significant compliance issues for the licensed victim and their business practice to respond and clean up the false use of their professional license.

- **Synthetic identity theft**: an intent to use another’s corporate professional identity to commit, aid, or abet any unlawful activity. Often results in real and false information combined to create a new identity. Perpetrators will take the combination of false and real information to create these new identities, and at times the new identity can result from totally fabricated information. Often results in identities to obtain credit, open deposit accounts, and obtain driver’s licenses and passports.
“Financial identity theft might wound your wallet … but medical identity theft can kill you.”
—Bankrate.com

Effects of medical identity theft:
- Insurance capped out due to other fraudulent use and benefits exhausted
- Erroneous information added to medical record
- Fictitious medical records created
- Wrong medical treatment leading to patient becoming uninsurable
- Employment denied due to failed physical exam because of erroneous documentation in medical records
- Physical risk to patients of injury (submitting to unnecessary procedures) or even death

---

In 2015, IRS officials are warning of identity thieves targeting tax refunds.4

“Identity thieves may attempt to run off with your tax refund before you ever take the time to file your taxes. NBC 5 has learned this type of theft has caught many taxpayers by surprise and could lead to months of frustration for those expecting an otherwise fast refund. It is not exactly known how identity thieves gather the information they need to file fraudulent tax returns, but tax experts said the perpetrators may be stealing Social Security numbers and other personal information.”

A middle school teacher filed his taxes early to pay some bills and educational classes with his refund. Unfortunately, an imposter had stolen his refund. Taxpayers who file online may receive a rejection notice claiming that their information has already been submitted. Victimized taxpayers will eventually receive their refunds—but only after a long wait!

The IRS estimated paying about $5.8 billion in fraudulent refunds while preventing $24.2 billion from falling into the wrong hands during the 2013 tax filing system.

February 2015—Daphne Maria Patterson was arraigned on federal charges of health care fraud and aggravated identify theft. She allegedly stole patients’ and their family members’ identities and billed insurance providers for services she did not render. Patterson, a registered nurse practitioner and owner of Healthier U 4Ever Wellness Center in Stone Mountain, Georgia, filed false claims with United Insurance Company for various allergy tests and

treatments that the patients never received. In addition, she used her access to steal family members’ identifying information to seek further reimbursement from United for services she had not rendered to patients she had never seen. In total, Ms. Patterson obtained more than $1 million from the insurance companies on the basis of her false claims.5

- Mechanism of theft: authorized access to patient data; however, unauthorized use of information

Physicians can be victims too. In 2011, an international “crime boss” pled guilty to racketeering in connection with an FBI indictment charging 44 alleged members of a crime ring with the “largest single Medicare fraud ever charged.”6 Reportedly, the organization’s activities spanned 25 states, operated in 118 phantom clinics, and billed at least $100 million in fraudulent claims.

These fraudsters used the physicians’ unique identifiers to bill Medicare for services that were never performed in clinics that did not exist. Often, the services billed did not match up with the physician victim’s medical expertise or licensure.

Physician identity theft can be devastating for the physician victim and result in severe financial losses for the federal government.

---


Physician identity theft occurs in two common scenarios:

- A physician’s identity is used to open a phony clinic and bill for services never rendered.
- A physician’s identity is used to order fraudulent prescriptions, medical equipment, or medical devices.

Physicians can experience financial loss due to taxes on earnings never received and obligations to return overpayments to payers for items or services never provided.7

In March of this year, one of my staff was provisioning the doctors into the meaningful use program at a major metropolitan hospital. She was walking a doctor through the process of granting proxy for meaningful use. CMS requires entering the physician’s Social Security number. He only wanted to give the last four digits and went on to tell the story of how, when he went to file his tax return, someone had already used his Social Security number. He stated that it has been a long battle verifying his identity to even file his taxes. He said it was a long process—and a major hassle.

- Mechanism of theft: Think of all the traditional functions from an internal audit perspective that require a physician’s identity. Credentials when entering to practice at a provider setting; maintaining licensure; volunteer work; CMS requirements for meaningful use … the list goes on. Each operational requirement can also become a mechanism of theft of the information.

The data strategy for an organization should include the management of PHI and individually identifiable information along with licensure data.

---

On the flip side, how can you know your provider? Physicians are all too happy to provide their credentials and information about their practice. Be sure to research a doctor’s credentials to be sure he or she is competent to take care of you.8

When vetting a doctor online:9

- Read physician reviews on medical sites (Healthgrades) and non-medical sites (Angie’s List) for an overall rating based on patient reviews, info about training, plus metrics such as time spent per patient, office wait time, and customer service.
- Look for patterns in the reviews to get a sense of a doctor’s patient style.
- Try to find any measures of how a provider treats his or her patients on Medicare sites.
- Check the safety and patient satisfaction data where the provider practices.
- Check your insurer’s website for physician and cost information.

How simple is it to look up a doctor’s license? [https://nppes.cms.hhs.gov/NPPESRegistry/NPIRegistryHome.do](https://nppes.cms.hhs.gov/NPPESRegistry/NPIRegistryHome.do). Just plug in their names and see if they have the licenses to provide the services that have indicated.

“Do No Harm” isn’t their motto.10

---

Most common types of fraud:

- Billing for services never rendered—using genuine patient data or data obtained via identity theft
- Falsely billing for a higher-priced treatment than was actually provided (upcoding)
- Performing medically unnecessary services to generate insurance payments
- Misrepresenting non-covered treatments as medically necessary (widely seen in cosmetic surgery)
- Falsifying a patient’s diagnosis to justify unnecessary services
- Unbundling—billing each step of a procedure as if it were separate
- Billing a patient more than the co-pay for services paid in full or pre-paid by the insurer
- Accepting kickbacks for patient referrals
- Waiving co-pays or deductibles and overbilling the insurance carrier or benefit plan

These are classic schemes that continue to occur. However, keep vigilant on new and emerging trends!

“California Doctor Sentenced for Role in Medicare Scam”

- Location: Los Angeles, California, Dr. Kenneth Thaler
- Consequences: sentenced to 12 months in prison; ordered to pay approximately $11 million in restitution
- Mechanism of theft: used marketers to recruit homeless patients
- Scheme: admitted homeless patients to the Tustin Hospital and Medical Center after they had been driven

---

from “Skid Row” in downtown Los Angeles as part of a Medicare fraud scheme

- Volume: 60 patients per month

The key to understanding, detecting, and mitigating health care fraud is to fully assess the mechanism of theft. These are the actionable steps of how a fraud is operationalized. Simply put: How were they able to do it and/or access the victims?

Again, doctors, pharmacies, and patients are collaborating to defraud the government and medical insurers.

- Elderly patients may receive kickbacks to sell their details to a pharmacist. The pharmacist then provides them with drugs they need while billing Medicare for costlier ones.
- Paid recruiters scour nursing homes for accomplices.
- Some pharmacies pay wholesalers to produce phony invoices.
- Some pharmacies bribe medical workers for leftover pills.
- Clinics (pill mills) are targeted to provide prescriptions for painkillers that will be resold on the street.
- Fake patients claim injuries and ask for scans and/or provide urine samples to justify their visits.
- Pharmacies prepare false billing. When investigated, their invoices don’t match their inventory.

Pharmaceutical fraud is growing at an accelerated rate for introduction of counterfeit and diverted medications. The data points are separate from group health care claims and are therefore more difficult to detect on a timely basis.

August 2014—Ringleader Babubhai Patel was sentenced to a 17-year prison term in 2013. Patel, a pharmacist and businessman from Canton, Michigan, owned and/or
controlled 26 pharmacies and several home health agencies in that state, but he concealed his involvement in many of these facilities through the use of straw owners. He and his associates recruited a number of pharmacists—mostly from overseas—to staff his pharmacies and help facilitate his scheme to defraud the government (more than $60 million to Medicare and Medicaid) and private insurers. There were bribes and kickbacks and thousands of illegal doses of sought-after drugs like oxycodone and hydrocodone.\(^\text{12}\)

- Mechanism of theft: Corporate infrastructures were utilized to mask activities.

June 18, 2013—Julian Kimble of Missouri City, Texas, was sentenced to 72 months in prison and three years of supervised release, and ordered to pay $3,676,587 in restitution to the Medicare Program.\(^\text{13}\)

All four of his ambulance companies were registered through a third party or straw owner with the Texas Department of Health and none of the companies had ambulances licensed for the types of services they billed.

Multiple beneficiaries were often transported at the same time under the attention of qualified EMT’s.

Co-conspirators were paid $1 million in exchange for agreeing to be transported to different facilities around the Houston area.


Ambulance/Medicare Scams
Dozens of operators of ambulances and ambulates (vans designed to take wheelchairs) have been caught offering kickbacks to patients to pretend they can’t walk. They then qualify for “emergency” pick-ups for which the company can charge $400 per patient.

Consumers should watch out for: 14
☐ One product that does it all
☐ Personal testimonials
☐ Quick fixes
☐ “All natural”
☐ “Miracle cure”
☐ Conspiracy theories

Consumer education is critical to attacking health care fraud on the front lines. Learn when to walk away or get a second opinion. Consumers should learn what questions to ask a provider about their treatment. Does it meet reasonability checks? Further, we should educate consumers on how to protect their identity when interacting with the health care system.

“Meridia Withdrawn from Market after Being Associated with Increased Risk of Heart Attack and Stroke” 15
☐ Mechanism of theft: introduction of products with false claims
☐ Consequence: Fraudulent products not only won’t work, they could cause serious injury.

FDA found more than 100 weight loss products illegally marketed as dietary supplements.

14 “Six Tip-Offs to Rip-Offs: Don't Fall for Health Fraud Scams,” FDA Consumer Health Information/U.S. Food and Drug Administration, March 2013.
NOTES

They contained sibutramine, an active ingredient that was found to increase the risk for a patient to experience a serious adverse cardiovascular event.

Avoid Health Fraud Scams!\(^{16}\)

- Be smart.
  - If it sounds too good to be true, it’s probably a scam!
- Be aware.
  - Learn the most common types of health fraud scams and red flags. Visit www.fda.gov/healthfraud for more information about identifying and avoiding scams.
- Be careful.
  - If the product claims to cure a wide range of diseases, it’s probably a scam.

Protect Your Personal Health Information (PHI)!\(^{17}\)

If you suspect you have been a victim of medical identity theft, contact your medical provider immediately and file a police report before beginning the process of getting your medical record information corrected. Pay special attention to any medical bills that come in the mail, and make sure you are being billed only for services you received. The closer attention you pay to things like this, the easier it will be to spot any fraudulent activity going on.\(^{17}\)

- Biometrics—PSI (Patient Secure Identity) system identifies patients through palm vein recognition, which can be integrated with the electronic medical record.\(^{18}\)

---

16 “Health Fraud Scams . . . Are Everywhere,” FDA Consumer Health Information/U.S. Food and Drug Administration, November 2011.
WILL THE REAL DR. JOHN SMITH PLEASE STAND UP?
A LOOK AT THE LATEST TRENDS IN HEALTH CARE FRAUD

- Smart Cards—holds encrypted patient information—estimated to reduce Medicare fraud by 66 percent—called CareCards in Canada.¹⁹
- Voice-recognition technology—used in Florida. Health workers conducting home visits call in from the patient’s home during each appointment to have their voice pattern matched against the one stored electronically. This has greatly reduced billing for non-visits.
- Analytical and predictive anti-fraud software—CMS has a new predictive analysis system, introduced in 2011, to catch Medicare fraud earlier. It is modelled on tools used by credit card firms.
- Controlling data breaches—This is a question for all organizations along with individuals. From an organizational perspective, it is critical to conduct regular vulnerability assessments for both physical and cyber security protocols. Individuals need to be aware of where they keep their own information, regardless of whether it is in paper format or electronic format. If they access their information electronically, is it being accessed in a secured environment?
- Ongoing legislative solutions—Healthit.gov is a good source to monitor ongoing legislation on HIPAA and PHI updates.

How Bad Data Puts Your Business at Risk

Final Thoughts on Datum
The following is an outline for consideration on managing data.

- Take an inventory of all data elements that are processed within the organization.
- Identify the value and perspective of that data point from a standpoint of:
  - Knowledge
  - Money
  - Business intelligence
  - Security
  - Risk
  - Compliance
- Identify the work flows associated with the datum.
- Create a data strategy.
- Develop an infrastructure to manage and update the data strategy for the organization.
- Operationalize the data assets for the business to protect the organization from illicit use of that data.

---