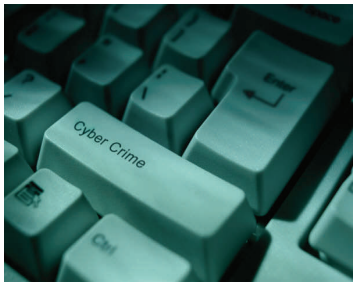
Risk Rx

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

Vol. 6 No. 4 October—December 2009

UF HSC Self-Insurance Program



Preventing Medical Identity Theft

Jan Rebstock, RHIT, LHRM, CPHRM

As telemedicine and electronic patient records (EHR) become more commonplace, so does the threat and incidence of security breaches by hackers and attackers. The transition to electronic health records is a national priority under the HITECH Act and while the EHR is expected to improve timely health care, and prevent medical errors, it also exponentially increases the opportunities for medical identity theft. The Federal Trade Commission estimates that 250,000 to 500,000 people have been victims of medical identity theft since 2003.[1]

Whether for the purpose of general or medical identity theft or other fraudulent intent, large complex data bases are attractive to cybercriminals and inside perpetrators because the crime is often easier to accomplish, the numbers make it more lucrative and it 's harder to detect.

What is Medical Identity Theft?

Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity- such as insurance information- without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. [1]

Medical identity theft is also more lucrative than general identity theft; a stolen Social Security number is estimated to have a street value of $1 per identity while stolen medical identity information averages $50 per identity. [3]

The potential negative impact of medical identity theft is significant and broad-based for both patients and providers. Perhaps one of the most harmful ramifications is the fraudulent alteration of a patient's medical information which could result in a patient receiving the wrong treatment and having a deadly outcome. To make matters worse, these kinds of errors are not easily discovered as many patients do not have copies of all their medical records and may not become aware of a problem until they have a reason to scrutinize them. Even when medical identity theft is discovered, it is extremely difficult to correct erroneous information that may have already been released to other medical providers, medical clearinghouses or insurers. Additionally, victims can be faced with credit card harassment by debt collectors, loss of or difficulty finding employment, denial of insurance and even wrongful allegations of criminal activity. Providers are also victims, perhaps having to return money to insurance companies, face potential litigation and civil penalties as well as deal with negative press and consumer confidence.

Some examples of Medical Identity Theft [4,1]:

- One week after a woman's child was born, she received a bill for $94 from an unknown clinic in the name of her newborn son where the painkiller Oxycontin had been prescribed for the infant's work-related back injury.

- Another mother of 4 was notified by a social worker that her baby tested positive for methamphetamines and as a result, the state planned to take away all of her four children. The mother hadn't been pregnant for 2 years but her stolen driver's license had ended up in the hands of a meth user who gave birth using

the mother's name. Despite hiring a lawyer to sort out the damage to her legal and medical records, the records had been circulated electronically and the mother's record contained the thief's blood disorder and emergency medical contact number.

- One woman was surprised to have her insurance company reject her claim for a $189 gynecological visit and found that another woman had already used her name to pay for the one allowed annual checkup.

- A Pennsylvania man discovered that an imposter used his identity at five different hospitals to receive more than $100,000 worth of medical treatment. At each hospital, the imposter created medical histories in the victim's name.

- An office coordinator at a Cleveland clinic in Florida printed out 1,100 patient records, then sold them to her cousin for $5-$10 per patient.

- A Colorado man had his medical identity stolen by a man who received multiple surgeries in his name. The victim did not have insurance and lost property and his business as a result.

Suggested Facility Prevention Strategies:

- Perform regular facility assessments, testing and surveillance of technology security
- Regularly evaluate and update data encryption, firewalls and intrusion detection programs and systems
- Include information about medical and other identity theft in new hire and annual employee educational training programs
- Assess the placement, accessibility and visibility of computer monitors, fax machines and medical records

Suggested Individual Prevention Strategies:

- Secure personal information in your home and shred documents that contain confidential information such as your health insurance ID number or social security number instead of throwing them in the trash
- Read explanations of insurance benefits of treatment received for accuracy
- Exercise your right to a free annual copy of your credit report from the three major credit bureaus and review any unpaid medical bills
- Observe your surroundings when providing/displaying insurance or other personal identifying information
- Maintain an up to date copy of your medical records
- Do not give personal identifying information to telemarketers or door-to-door solicitors

Some actions you can take if you are a victim of medical identity theft:

- Place a fraud alert on your credit report by calling the toll free numbers for any of the three consumer reporting companies; TransUnion- 1-800-680-7289, Equifax-1-800-525-6285 or Experian-1-888-397-3742.
- Notify the police and complete an identity theft report
- File a complaint with the State Attorney General's office, State Insurance Department and the Identity Theft Data Clearinghouse operated by the Federal Trade Commission
- Notify your health care providers and demand that providers or insurance companies correct erroneous information or append and amend records to alert users to inaccurate content.
- Notify your heath insurance company

Preventing medical identify theft requires a multi-faceted organizational approach to ensure that ade-

quate technical, physical and individual security safeguards, policies and procedures are in place. While data networks may help tie the world together, those ties need to be strong enough to prevent or at least deter information crimes.

For more information log on to UF's privacy site: http://privacy.ufl.edu/identity/how.html or Shands Privacy site: https://my.portal.shands.ufl.edu/portal/page/portal/DEPT_CONTENT/DEPT_CORE/Legal/Privacy_and_HIPAA

References:
1. Medical Identity Theft: The Information Crime that Can Kill You, Pam Dixon, World Privacy Forum, May 3, 2006

2. Medical Identity Theft Final Report, Booz,Allen,Hamilton

3. "Mitigating Medical Identity Theft." Journal of AHIMA 79, No. 7 (July 2008): 63-69

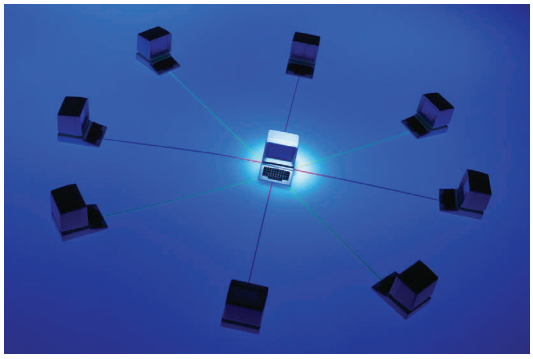
4. http://www.msnbc.msn.com/id/23392229/from/ET/

5. http://www.creditcards.com/credit-card-news/how-to-prevent-medical-id-identity-theft-1282.php

6. Preventing and responding to medical identity theft, Geraldine Amori, Ph.D., DFASHRM, CPHRM, ARM, Journal of Healthcare Risk Management,Vol. 28 No. 2 P. 33

7. http://myfloridalegal.com/idkitprintable.pdf

8. http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm



Legal Case Study: *Florida Department of Corrections v. Lisa M. Abril* (Fla. 2007)

Cristina Palacio, Esq.
Senior Associate General Counsel
Shands Healthcare

The enactment of the Health Insurance Portability and Accountability Act (HIPAA) in 1996 brought national focus on the issue of patient confidentiality. But long before HIPAA, Florida statute and common law both recognized the importance of patient confidentiality. To the extent that those statutes do not conflict with HIPAA, or provide even stronger protection than HIPAA, that law is still controlling today. Moreover, while HIPAA allows for the imposition of government sanctions against a person or entity that violates its provisions, it does not provide a private cause of action. State law, however, does. In *Florida Department of Corrections v. Abril,* we see how a patient can directly recover damages from an entity that inappropriately discloses confidential personal health information.

Facts

In this case, Lisa Abril, a licensed practical nurse at the Hendry County Correctional Institution (HCCI) gave unprotected mouth-to-mouth resuscitation to an inmate. The inmate was known to have hepatitis C, but his HIV status was unknown. Considering herself to have suffered a significant exposure, Ms. Abril sought to have herself tested for hepatitis C and HIV through Continental Laboratory, a lab under contract with the State Depart-

ment of Corrections (DOC) to provide HIV testing for inmates. After the test was performed, a DOC department employee requested information about the test to investigate a concern that the use of Continent Laboratory for testing Ms. Abril's blood was not authorized. In response to the request, Ms. Abril alleged that Continental transmitted Ms. Abril's test results – including a (false) positive HIV test result – to unsecured fax machines in the HCCI office and in the Tallahassee DOC office, resulting in the unauthorized disclosure of the positive HIV test result to a number of DOC employees. Allegedly as a result of the improper disclosure (not the misdiagnosis), Ms. Abril had to undergo treatment for severe depression and post-traumatic stress disorder. Consequently, Ms. Abril filed a civil action seeking damages for, amongst other things, mental anguish and emotional distress as a result of Continental Laboratory's negligent failure to ensure the confidentiality and privacy of her HIV test results, causing the test results to be improperly disseminated to unauthorized personnel.

Analysis

As with all negligence cases, the first question in determining whether Ms. Abril had a viable claim that Continental was liable for negligence was whether it owed Ms. Abril a *duty* of confidentiality. (Note that the case indicates that the DOC has been sued. Ms. Abril's complaint alleged, and DOC did not dispute, that the DOC was liable for Continental's negligence as its agent.) In coming to the conclusion that Continental did owe Ms. Abril a duty of confidentiality, the Court relied on both statutory law and the right to privacy found in the Florida Constitution.

The Court began its analysis with Florida Statute section 381.004(3)(f), which provides that:

> "Except as provided in this section, the identity of a person upon whom a[n HIV] test has been performed is confidential and exempt from the provisions of [the public records law]. No person to whom the results of a test have been disclosed may disclose the test results to another person except as authorized [by law]."

Citing to Florida cases that "have long recognized that the violation of a statute may be utilized as evidence of negligence" the Supreme Court found that section 381.004(3)(f) "at a minimum, creates a reasonable standard of care for handling HIV testing results" and that if proven during trial, the allegations made by Ms. Abril could be sufficient to indicate that Continental had acted negligently by violating the duty imposed by section 381.004 to maintain confidentiality of HIV test results and disclose only as authorized by law.

Furthermore, the Court noted that, in addition to the explicit confidentiality provisions of F.S. §381.004, Florida Statute section 483.181(2), which governs clinical laboratories, mandates a lab to report its test results "directly to the licensed practitioner or other authorized person who requested it." The Court cited the clinical lab statute as another indication of the lab's duty to maintain patient confidentiality. Of even more significance in the Shands HealthCare settings, in its analysis the Court specifically referred to F.S. §395.3025 (relating to hospital medical records) as a potential statutory basis for a breach of confidentiality negligence action. F.S. §395.3025 provides that, with limited enumerated exceptions, a patient's medical records are confidential and cannot be disclosed without patient consent. Despite the fact that neither HCCI nor the DOC are subject to F.S. §395.3025, the Court stated that "it [was] apparent that more than one Florida statute may have been breached by the disclosure of Ms. Abril's confidential medical information."

Moreover, the Florida Supreme Court stated that "[t]here is a long tradition of recognizing the privacy interest of patients in confidential medical records." In so noting, the Court quoted from its own decision 5 years earlier in *State of Florida v. Zina Johnson* (Fla. 2002), in which it stated that "[a] patient's medical records enjoy a confidential status by virtue of the right to privacy contained in the Florida Constitution…."

In *Johnson*, evidence obtained from a patient's medical records was used to charge her with DUI manslaughter. Ms. Johnson was the driver in a single-car crash in which her passenger died. She was hospitalized with injuries, and during the course of treatment, blood was drawn. Pursuant to the requirements of F.S. §395.3025(4)(d), the hospital medical records statute, the State attorney tried to notify Ms. Johnson that her records were to be subpoenaed. The rationale behind the notice provision is that a patient should be granted the opportunity to object to the subpoena. Despite several attempts to serve notice to Ms. Johnson, the State attorney was unable to get her correct address (although a check of driver license records or post office forwarding addresses would have yielded it). Unable to fulfill the requirements of the Florida medical records statute, the State attorney instead relied on his general investigative subpoena power, which does not require notice to obtain the records (and which under HIPAA would have been sufficient). Ms. Johnson moved to suppress the evidence obtained from her medical records.

As noted above, the *Johnson* court recognized that a patient's medical records enjoy confidentiality protection through the Florida Constitution right to privacy. But no Constitutional right is absolute, and so the Court analyzed the State's actions under the well established "compelling state interest" standard. That is, that the State may limit a constitutional right for compelling state interests. The Court acknowledged that controlling and prosecuting criminal activity is a compelling state interest. However, it also concluded that the subpoena notice requirement of F.S. §395.3025 is an appropriate legislatively established balance of a patient's privacy rights with legitimate access to medical records for civil and criminal proceedings. Consequently, the Court held that the statute granting the State attorney investigative subpoena power does not override the notice requirement for obtaining medical records pursuant to subpoena under F.S. §395.3025, and the State was not permitted to use the information improperly obtained.

Note that in *Johnson*, no action was brought against the hospital for releasing the medical records pursuant to an invalid subpoena. The Court's reference to F.S. §395.3025 in *Abril*, however, clearly indicates that such a release could be the basis of a breach of confidentiality negligence action against the hospital, or hospital personnel, for improper disclosure of medical records. How that case might look is illustrated by *Suzanne Bagent v. Blessing Care Corporation, d/b/a Illini Community Hospital, and Misty Young* (Ill. App. Ct. 2006). In *Bagent*, Misty Young, an employee of Illini Community Hospital, inadvertently disclosed that Suzanne Bagent was pregnant to Ms. Bagent's twin sister – who happened to be a good friend of Ms. Young's. Ms. Young, a phlebotomist, learned of Ms. Bagent's pregnancy from a fax in the course of performing her duties. Later, meeting Ms. Bagent's sister at the "tavern," Ms. Young asked how Suzanne was feeling. When Suzanne's sister asked what Ms. Young meant, she responded that she thought Suzanne was pregnant; upon further questioning from the sister, Ms. Young disclosed that she had seen the result of Suzanne Bagent's pregnancy test. In find-

ing the hospital could be sued for Ms. Young's disclosure under the *respondeat superior* ("let the master answer") doctrine (providing that an employer may be liable for the actions of her/his employee), the court noted "the importance of the confidentiality of a patient's medical records" and cited to Illinois statutes prohibiting hospitals and physicians from disclosing patient medical information without consent, except, as in Florida, under specifically enumerated circumstances. Ms. Young, while not subject to an action pursuant to the statutes, was potentially liable under a common-law right to privacy theory – much like the Florida Constitutional right to privacy.

Conclusion and Risk Reduction Tips

The importance of maintaining patient confidentiality cannot be overemphasized. A patient's right to confidentiality of her/his personal health information is supported not only by HIPAA, but also by Florida State law, and the Florida Constitution. As these cases demonstrate, breach of that confidentiality can potentially expose both the hospital and the individual physician or hospital employee to a private negligence action under State law, and to potential sanctions by the Office of Civil Rights under HIPAA.

While familiarizing yourself with the statutes governing patient confidentiality is not practical, knowing the hospital policies relating to patient health information is essential. Those policies can be found in the "Confidentiality" section of Shands HealthCare Core Policies (CP 3 series), as well as CP1.35, CP1.18 and CP1.11; all of which are readily available on the Shands intranet website. And remember, when in doubt, contact Shands Legal Services and/or Privacy Office.

HIPAA - Privacy Regulatory Updates

Heather Noughton -Bokor
CHC. Compliance Specialist
Shands HealthCare Corporate Compliance Dept.

- **HHS / FTC Issues Breach Notification Rules:**

  The Department of Health and Human Services (HHS) issued rules related to breach notification requirements for providers, health plans, and other entities covered under the Health Insurance Portability and Accountability Act (HIPAA). Additionally, the Federal Trade Commission has issued similar rules impacting vendors of personal health records and certain others not covered by HIPAA. These rules serve to implement provisions of the American Recovery and Reinvestment Act of 2009 (ARRA).
  The regulations require prompt notification to affected individuals of a breach of the privacy of their unsecured personal health information. In addition, providers and other covered entities are required to notify the HHS Secretary and the media in cases where a breach impacts more than 500 individuals. Breaches affecting less than 500 individuals are to be reported to HHS annually. Notice obligations are effective for breaches occurring on or after September 24, 2009.

- **Red Flag Rules Delayed Until November 1, 2009:**

  The Federal Trade Commission (FTC) announced an additional delay in the enforcement of the "Red Flags" Rule. The Rule requires those with covered accounts, including hospitals, to implement programs to identify,

detect, and respond to the warning signs ("red flags") that could indicate identify theft.
To give creditors and financial institutions more time to review this guidance and develop and implement written Identity Theft Prevention Programs, the FTC will further delay enforcement of the Rule until November 1, 2009. At the same time, in order to assist small businesses and other entities, the Federal Trade Commission staff will redouble its efforts to educate them about compliance with the "Red Flags" Rule and ease compliance by providing additional resources and guidance to clarify whether businesses are covered by the Rule and what they must do to comply.

- **HHS has delegated authority for enforcement of the HIPAA security rule to the Office of Civil Rights (OCR)**

Security rule enforcement had been handled by CMS, while OCR has handled only privacy rule enforcement. Under the security rule, the OCR will now be able to impose civil money penalties and issue subpoenas.

2010 Joint Commission Hospital National Patient Safety Goals

Debbie Robins,
Patient Safety Officer
Shands Healthcare

While there were many changes to the existing patient safety goals, no new goals were added for 2010.

Several patient safety goals were shifted to chapters within the standards manual including:
- Banned abbreviations,
- Look-alike sound-alike medication requirements (list; segregation; labeling),
- Hand-off communication,
- Fall prevention and
- Early response teams

Of the 20 NPSG's in 2009, 11 were retained in the 2010 version including those related to:
- Two identifiers
- Two-person identification prior to transfusion
- Critical tests results – focus on timeliness of reporting
- Medication labeling
- Anticoagulation management
- Improving hand hygiene
- Reducing multi-drug resistant organisms (MDRO's)
- Central line infection prevention
- Surgical site infection prevention
- Suicide prevention and
- Universal protocol requirements

The requirement for managing a health care acquired infection that resulted in death or serous bodily injury as a sentinel event was eliminated from the NPSG's and the standards.

And last but not least, the safety goal requirements for medication reconciliation continue to be under review by The Joint Commission. As a result, compliance will not be scored during upcoming surveys.

Risk Rx

UF | UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

Send comments and/or article suggestions to: rmeduc@shands.ufl.edu

To see Risk Rx archives, log on to:
http://www.sip.ufl.edu/riskrx.php

Happy Holidays!