

# Identity Theft in Healthcare

**Presented by:**

**Donna Gilley, CCP, CHC**  
**LBMC Healthcare Group, LLC**  
**[Dgilley@lbmc.com](mailto:Dgilley@lbmc.com)**  
**615-309-2376**

**Wynelle Paige, RHIA, CCP**  
**Compliance Advisory Coalition**  
**[mwpaige@charter.net](mailto:mwpaige@charter.net)**  
**865-621-2095**

# Identity Theft – What is it?

- The National Crime Prevention Council (2005) defines identity theft as “occurring when a person knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit or to aid or abet any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law”

# Identity Theft - Statistics

- One of the fastest growing crimes in the US
- Healthcare consumes one is seven dollars and is growing at a rate of six times greater than the rest of the economy
- 12.7% (27M) of adults report they have been the victim of identity theft
- According to Blue Cross Blue Shield – over 85 BILLION (of the 1.7 trillion) dollars was lost to health insurance fraud in 2003 alone
- On average, it takes 175 hours of work for a victim of identity theft to clear their good name

# Identity Theft - Statistics

- The Federal Trade Commission (FTC) reported more than 635,000 complaints related to fraud and identity theft in 2004
  - FTC identity theft complaints online ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft))

# Identity Theft

Healthcare organizations are particularly vulnerable to identity theft crime due to the wealth of patient personal, demographic, and financial information that is collected, transmitted, and maintained in the course of operations.

# How Does It Happen?

- Theft of wallets, purses, or mail from patients
- Accessing computer information/PHI through hacking
- Dumpster diving or collecting trash containing PHI
- Stealing records or information while on the job
- Thieves “trolling” the obituaries

# How Does It Happen?

- Employee Access
  - Access information under the pretext that it is a legitimate use of PHI
  - Access information through legitimate means and then divert the information for criminal purposes

# Two Types of Identity Theft in Healthcare

- **Medical Identity Theft**

- An individual steals another person's identity to gain access to healthcare

- **Theft of Patient Identity  
(PHI Theft)**

- An individual steals another person's identity from information gained from a healthcare entity

# Medical Identity Theft

- Almost always perpetrated by a friend or relative who has lost or does not have insurance coverage

# Medical Identity Theft

## Who gets hurt?

- The “real” patient
  - Financial
    - » May impact lifetime maximums, and/or annual coverage caps
    - » May be asked to cover co-pays and deductibles for services never received
    - » May impact coverage premiums or the ability to obtain future coverage if the thief has certain diagnoses

# Medical Identity Theft

- The “real” patient

- Clinical

- If the thief has certain medical conditions, such as drug allergies, the patient may be denied life-saving medications because the provider believes the medical record to be accurate
    - Once the medical record is “mixed” with the information from 2 different individuals claiming to be the same person, it can be Very difficult for clinicians to separate conditions, medication lists, allergies, etc

# Medical Identity Theft

- The Hospital, Nursing Home, or other healthcare entity
  - Once the theft is discovered, the payor (if they have paid the claims), will seek repayment
  - Even if the theft is caught, the chances of getting reimbursed for services rendered is incredibly narrow
  - With healthcare margins more narrow than ever in history, facilities with only a very few thefts can be hit hard financially

# Medical Identity Theft

- The Insurance Company

- If the theft is not identified, the insurance company will unwittingly pay for services they would not be responsible for ordinarily – Many times these are treatments for the terminally ill, mental health services and other expensive and/or extensive treatments.

# Medical Identity Theft

- Companies and Individuals (You and I)
  - As the cost of national healthcare rises, so do insurance premiums, co-payments, and deductibles
  - Insurance companies may be less willing to cover certain diagnoses and/or services causing honest consumers to have to pay more out of pocket.

# Medical Identity Theft – What can facilities do to protect themselves?

- Always ask for Photo ID before services are rendered
- If the ID does not match the medical record (can happen due to marriage/divorce, etc) ask for a second piece of identification with the same name

# Medical Identity Theft – What can facilities do to protect themselves?

- If the patient does not have photo ID, take a picture of them using a webcam
  - Explain it is for their safety, both financial and clinical
- If the patient is unwilling to have their picture made or returns to their vehicle to retrieve ID and does not return, you will know that something is suspicious

# Medical Identity Theft – What can facilities do to protect themselves?

- Make sure your charity care or medically indigent policy is well publicized to potentially eliminate the desire to commit medical identity theft
- Make sure patients know it is against the law to “Share” their insurance coverage
- When an identity thief is caught, make sure you prosecute to the fullest extent of the law.

# Medical Identity Theft – What can facilities do to protect themselves?

- Discreetly post names in registration areas (completely out of public site) to alert staff of a potential issue
- Share information with other providers (be careful to stay within legal limits!!!)
- Make sure you have a policy in place to cross reference a “stolen” identity medical record and the “real” identity’s medical record

# Medical Identity Theft – What can facilities do to protect themselves?

- Post a notice at the bottom of patient statements indicating that the patient should notify the business office immediately if they did not receive the care listed on the statement

If a patient lets us know they are a victim of identity theft and it may include their healthcare, what should we do?

- Flag the medical record
- Tell them to place a fraud alert on their credit reports
- If their insurance card has been stolen, have them call their insurance company immediately
- Suggest they complain to the Federal Trade Commission
- Tell them to file a police report
- Remind them to shred anything they receive at home with personal information that they wish to dispose of

If a patient lets us know they are a victim of identity theft and it may include their healthcare, what should we do?

- Suggest they order the free FTC guide “When bad things happen to your good name” at [www.ftc.gov/bcp/online/pubs/credit/idtheft.htm](http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm)

# PHI Theft from a Healthcare Entity - Statistics

- Most legal cases, except for theft by a family member, are the result of an employee or Former employee theft
- Some cases involve the employee selling the patient information
- A few cases involve compromised information systems either by hackers or by outright theft of computers (if a laptop is secure, the physical theft should not result in access)

# PHI Theft

## Who gets Hurt?

- The “real” patient
  - May impact lifetime maximums, and/or annual coverage caps
  - May be asked to cover co-pays and deductibles for services never received
  - May impact coverage premiums or the ability to obtain future coverage if the thief has certain diagnoses

# PHI Theft

- The “real” patient
  - The thief may give stolen name during an arrest and when they do not show up for court, a warrant is issued

# PHI Theft

- The “real” patient
  - The thief may gain false identification
  - The thief may get a job or file fraudulent tax returns under the stolen identity
  - The thief may open credit card or other accounts and not pay the bill
  - They may open a bank account and write bad checks
  - They may buy a new car in the stolen name

# PHI Theft

## Who gets hurt?

- The healthcare facility
  - Can ruin reputation as a quality provider and drive patients elsewhere

# PHI Theft - What can we do to protect our patient's information?

- Maintain HIPAA standards for privacy and security
  - Storing confidential information appropriately and limiting access
    - Minimum necessary – has it been updated since implementation?
- Keeping computer monitors turned so the view of the screen is limited, or use screen covers when confidential patient information is displayed.

# PHI Theft - What can we do to protect our patient's information?

- Employee (even temp & volunteers) education
- Automatic logouts, etc

# PHI Theft - What can we do to protect our patient's information?

- Keep computer passwords and logons secure.
- Use shredders or locked shredding receptacles-not trash cans-to discard patient information.
- Fax correctly, checking to make sure the number is accurate and the fax is received by the authorized person.
- Use encrypted e-mail for sending patient information outside the system.
- Avoid discussing patient information in open areas that can heard by others

## PHI Theft – What can we do to protect our patient's information?

- Criminal background checks on ALL employees
- Physical plant security – locked doors, minimum access, etc
- If you accept credit card payments, make sure receipts are secure
- Do not keep credit card information in the medical record

What to do if it happens to  
YOU?

Place a fraud alert on your credit reports, and review your credit reports.

# Fraud Alerts

## ➤ Initial

Stays on your credit for at least 90 days, this type is appropriate if your wallet has been stolen or you've been taken in by a "phishing" scam.

## ➤ Extended

Stays on your credit report for seven years, this type is appropriate when you have been a victim of identity theft. Also the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years.

# What to do if it happens to YOU?

- Close the accounts that you know, or believe, have been tampered with or opened fraudulently
- File a report with your local police or the police in the community where the identity theft took place.
- File a complaint with the federal trade Commission.

# Legal Cases

- A victim found that several credit cards, a car loan and car insurance had opened in her name
  - The suspect obtained her information through medical insurance records since the suspect works for a firm that maintains HMO databases

# Legal Cases

- PA woman sued hospital claiming you could clearly read her name and other personal information in an advertisement for Breast Cancer Awareness

# Legal Cases

- Cancer patient was the victim of identity theft perpetrated by an employee of the hospital where he was receiving chemotherapy

# Legal Cases

At one hospital, an employee stole almost 400 patient identities and used them to apply for credit cards.

# Legal Cases

Class Action lawsuit on behalf of 365,000 people due to records stolen from employees car. Negligence claimed.

# Punishment –HIPAA may not apply to individuals ???

- The DOJ on June 1, 05 released a ruling stating that penalties under the HIPAA law apply “covered entities” but “may not” apply to individuals.

# States with the most proactive prevention and/or deterrent laws for identity theft

- California – Governor Schwarzenegger
  - Has an office of privacy protection
    - [www.privacy.ca.gov](http://www.privacy.ca.gov)
    - Increased penalties for “spam”
    - Prohibits prisoners from accessing personal information while in work programs
    - Background checks for state employees with access to medical records
    - Eliminates the requirement for a SSN on power of atty

# States with the most proactive prevention and/or deterrent laws for identity theft

- North Carolina – Governor Easley
  - The NC Identity Theft Protection Act of 2005
    - Prevents businesses from using SSN as customer identification
    - Prohibits selling or displaying customers SSNs to a third party without written consent
    - Requires businesses to notify customers if a security breach occurs
    - Businesses must shred or destroy any records containing customer's personal information.

# States with the most proactive prevention and/or deterrent laws for identity theft

## Michigan – Attorney General Mike Cox “It’s MI Identity” campaign

- Detects theft of identity of seniors living in adult residential care
- Illegal use of a financial transaction device (ATM) – four-yr felony
- Credit report day in 76 residential facilities statewide

# New Developments

## Consumer reporting companies

- Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com);  
P.O. Box 740241, Atlanta, Georgia 30374-0241
- Experian: 1-888-397-3742; [www.experian.com](http://www.experian.com);  
P.O. Box 9532, Allen, Texas 75013
- TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com)  
Fraud Victim Assistance Division  
P.O. Box 6790, Fullerton, California 92834-6790

# Additional Assistance

Federal Trade Commission

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

1-877-438-4338; TTY: 1-866-653-4261

Identity Theft Clearinghouse, Federal Trade  
Commission, 600 Pennsylvania Avenue, NW,  
Washington, D.C. 20580

# Additional Assistance

Remove your name from marketing lists of the credit bureaus (Stop all those pre-approved credit card applications!! – [www.optoutprescreen.com](http://www.optoutprescreen.com))

Federal Do Not Call Registry – [www.donotcall.gov](http://www.donotcall.gov)

Free Annual Credit report for all Americans  
– [www.annualcreditreport.com](http://www.annualcreditreport.com) (DO NOT CONFUSE with [www.freecreditreport.com](http://www.freecreditreport.com) which when used activates a trial membership.

# Additional Assistance

[www.privacyrights.org](http://www.privacyrights.org)

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

[www.fightidentitytheft.com](http://www.fightidentitytheft.com)

[www.usdoj.gov/criminal/fraud/idtheft.htm](http://www.usdoj.gov/criminal/fraud/idtheft.htm)