INFORMATION SECURITY TRAINING: CONTRACT EMPLOYEE

Designed for Pathways Community Mental Health

2017

The goal of this training is to acquaint you with the basics of information security and the HIPAA Security Rule.

The topics of this training include:

- **HIPAA & HITECH**
- **Passwords and Pass Phrases**
- **ELMER Security**
- **Reporting Security Incidents**

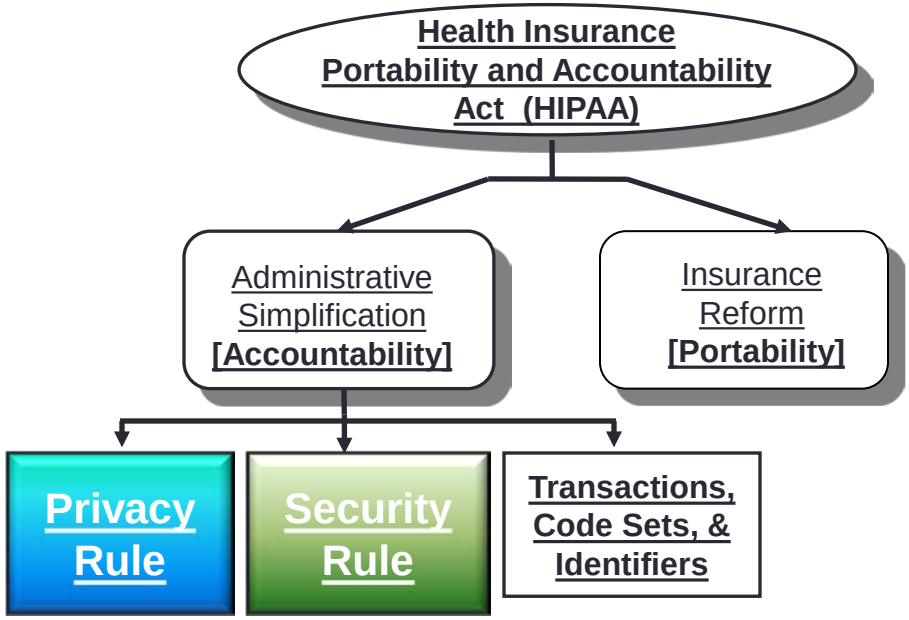
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA is a federal mandate dealing with a variety of issues. The original goal was to make transferring from one health insurance plan to another easier as people changed jobs or became unemployed. To make it easier to share information between healthcare providers, HIPAA required healthcare providers and payers to submit transactions (e.g. patient claims) in a standardized electronic format. As information becomes easier to transmit, it also becomes easier for the information to be lost, stolen or abused.

Digitizing patient records allows for efficient transmission of information but comes with associated risks. HIPAA requirements for reasonable and appropriate security of patient information are critical to maintaining the confidentiality, integrity and availability of this information.

Virtually all healthcare organizations that engage in electronic transactions are required to comply with HIPAA. These organizations are referred to as “covered entities” under HIPAA. Pathways meets the criteria to be considered a covered entity.

Contractors that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity are considered a **Business Associate.** **The organization you work for is considered a Business Associate of Pathways.**



On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act of 2009. A portion of the bill created the Health Information Technology for Economic and Clinical Health Act (HITECH). The HITECH Act substantially expanded the HIPAA Privacy and Security Rules and increases the penalties for violations of HIPAA.

Three important HITECH requirements are:

1. HITECH established mandatory federal security breach reporting requirements for HIPAA Covered Entities and their Business Associates. Covered entities now must notify each person whose unsecured PHI is disclosed in a breach. Under certain circumstances, a breach may involve notifying the local newspapers and television broadcasters of the incident. The U.S. Department of Health and Human Services has established a list of breaches of unsecured protected health information affecting 500 or more individuals. The list has been nicknamed the "Wall of Shame". You can view the list here: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

2. Under the HITECH Act, Business Associates are directly subject to the administrative, physical and technical safeguard requirements of the Security Rule, as well as the requirements to maintain policies, procedures, and documentation of security activities in the same manner that such sections apply to the covered entity.

3. Establish new criminal and civil penalties for noncompliance. The act provides a four tiered system for assessing the level and penalty of each violation. Penalties quickly escalate from a minimum of $100 per violation with a $25,000 max per calendar year to $50,000 per violation and $1.5 million for the calendar year. The Feds appear to be **very** serious about issuing penalties under HITECH.

Civil and criminal penalties for violation of the HIPAA security rule apply to a Business Associates in the same manner as they apply to a Covered Entities.

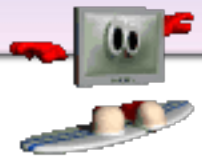
Pathways has always upheld strict privacy and security policies.
It is critical that Pathways' Business Associates also be vigilant in protecting the confidentiality of consumer information.

Each user is assigned a unique user ID and password. The credentials are assigned to the individual and that individual ONLY.

It may seem like a good idea to share credentials with a co-worker that has not been assigned access to an application. However, that would undermine the key security principle of accountability. The computer system's auditing would indicate all activity conducted under your user ID to be attributed to you. In other words, you may take the blame for their conduct.

To safeguard **YOUR** computing account, **YOU** need to take steps to protect **YOUR** password.

When choosing a password:



- Don't use a word that can easily be found in a dictionary. Words commonly found in a dictionary can be cracked in minutes.
- Don't share your password – protect it the same as you would the key to your residence. After all, it is a "key" to your identity.
- Use eight characters at a minimum which should contain Uppercase letters (A-Z), lowercase letters (a-z), and numbers (0-9).

- Your personal passwords (e.g. hotmail, Facebook, on-line banking) should be different than the passwords you use at your job.

A Pass Phrase is a good alternative to complex password

A pass phrase uses words to create a sentence—like phrase. For example, "*UP summers r great*" is an 18 character (including spaces) pass phrase containing upper and lower characters. Unlike passwords, pass phrases can't be found in the dictionary and are much harder to guess.

Tips for Pass Phrases:

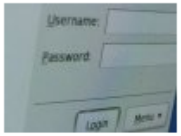
- Misspelling or abbreviating words adds complexity to the pass phrase
- Pass phrases should not contain famous quotations from literature, movies, etc.

The Pathways' Information Security Team recommends using pass phrases or complex passwords in all Pathways systems, including ELMER.

How I'd Hack Your Weak Passwords

by JOHN P.

+1 21



If you invited me to try and crack your password, you know the one that you use over and over for like every web page you visit, how many guesses would it take before I got it?

Let's see… here is my top 10 list. I can obtain most of this information much easier than you think, then I might just be able to get into your e-mail, computer, or online banking. After all, if I get into one I'll probably get into all of them.

1. Your partner, child, or pet's name, possibly followed by a 0 or 1 (because they're always making you use a number, aren't they?)
2. The last 4 digits of your social security number.
3. 123 or 1234 or 123456.
4. "password"
5. Your city, or college, football team name.
6. Date of birth – yours, your partner's or your child's.
7. "god"
8. "letmein"
9. "money"
10. "love"

Statistically speaking that should probably cover about 20% of you. But don't worry. If I didn't get it yet it will probably only take a few more minutes before I do…

Hackers, and I'm not talking about the ethical kind, have developed a whole range of tools to get at your personal data. And the main impediment standing between your information remaining safe, or leaking out, **is the password you choose**. (Ironically, the best protection people have is usually the one they take least seriously.)

http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/

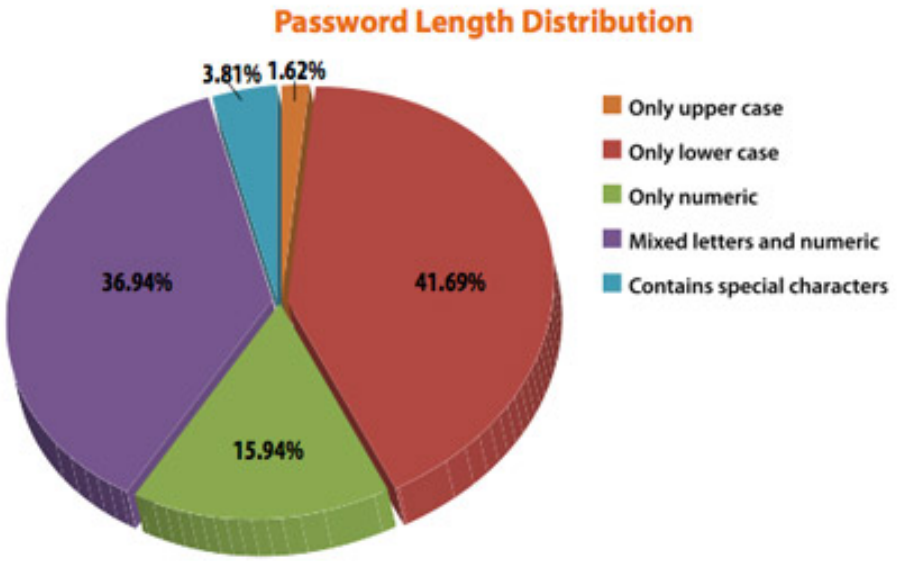
Analysis of 32 million breached passwords

Posted on 21 January 2010.

Bookmark and Share

Imperva released a study analyzing 32 million passwords exposed in the Rockyou.com breach. The data provides a unique glimpse into the way that users select passwords and an opportunity to evaluate the true strength of these as a security mechanism.

In the past, password studies have focused mostly on surveys. Never before has there been such a high volume of real-world passwords to examine.



Key findings of the study include:

- The shortness and simplicity of passwords means many users select credentials that will make them susceptible to basic forms of cyber attacks known as "brute force attacks."
- Nearly 50% of users used names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on). The most common password is "123456".
- Recommendations for users and administrators for choosing strong passwords.

"Everyone needs to understand what the combination of poor passwords means in today's world of automated cyber attacks: with only minimal effort, a hacker can gain access to one new account every second—or 1000 accounts every 17 minutes," explained Imperva's CTO Amichai Shulman.

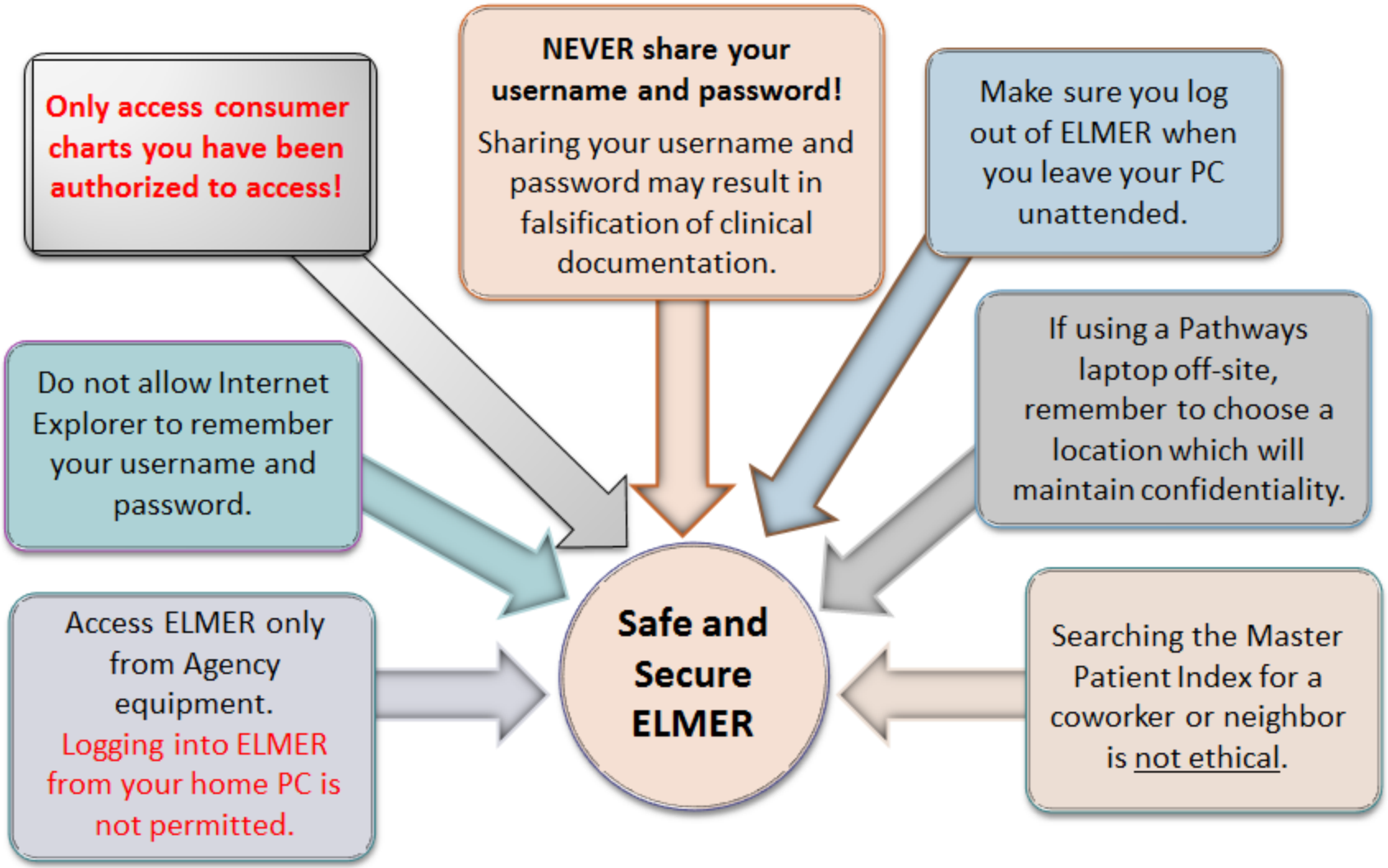
The report identifies the most commonly used passwords:

1. 123456
2. 12345
3. 123456789
4. Password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123

For enterprises, password insecurity can have serious consequences. "Employees using the same passwords on Facebook that they use in the workplace bring the possibility of compromising enterprise systems with insecure passwords, especially if they are using easy to crack passwords like '123456'," said Shulman.

Read more here:
http://www.net-security.org/secworld.php?id=8742
http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

In the age of electronic health records, maintaining the security of ELMER is imperative. Here are a few rules to follow:



Reporting security incidents is important so that security problems can be detect, mitigated and prevent

You are responsible for reporting security incidents as soon as possible. All reports need to be communicated to Pathways. Please refer to the Business Associate Agreement for details on how and what to report.

Here are a couple events that require reporting to Pathways:

- When users log into the Pathways network or ELMER with **someone else's** username and password.
- **A privacy or security breach to consumer information.** A breach is considered discovered on the first day a covered entity or Business Associate **knows or should have known about it**. Covered entities and BAs must notify individuals about a breach as soon as possible but no later than 60 days following discovery of the breach. A delay in reporting a breach may result in penalties by the U.S. Health and Human Services.

Snooping in medical records leads to HIPAA breaches, disciplinary actions and often financial penalties for the health care organization.

Nearly 900 notified of new HIPAA breach

By **Erin McCann** | January 26, 2015 | 11:06 AM

Electronic health records not only enable faster access to real-time patient data; they also make it a heck of a lot easier to catch snooping employees who inappropriately view patients' confidential information, as one California hospital has observed this past week.

Officials at the 785-bed California Pacific Medical Center in San Francisco – part of Sutter Health system – notified a total of 844 patients Jan. 23 after discovering a pharmacist employee had been inappropriately snooping on patients' medical data for an entire year.

1,300 patients notified of privacy breach

By **Erin McCann** | August 14, 2013 | 10:52 AM

An Ontario hospital has fired a nurse who was found to have been improperly accessing the protected health information of some 1,300 patients for more than nine years.

The 106-bed Norfolk General Hospital dismissed the employee in March after receiving a call from a former patient who expressed concern that their protected health information was known in the community. The individual was "basically hearing from other neighbors and friends and people in the community things that would be on their medical file," said NGH spokesperson Janine Van Den Heuvel to *Healthcare IT News*.

Malicious Software

Ransomware

Ransomware is a type of malicious software distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker in order to receive a decryption key.

Malicious Software

Ransomware and HIPAA

Ransomware active on computers may compromise the confidentiality and availability of protected health information. In most circumstances, a ransomware attack would require Pathways to report the event to the United States Department of Health and Human Services. Monetary fines and federal audits are used to penalize healthcare providers.

December 2014
U.S. Department of Health and Human Services
Office for Civil Rights

BULLETIN: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software

Anchorage Community Mental Health Services (ACMHS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule with the Department of Health and Human Services (HHS), Office for Civil Rights (OCR). ACMHS will pay $150,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. ACMHS is a five-facility, nonprofit organization providing behavioral health care services to children, adults, and families in Anchorage, Alaska.

Pathways' Business Associates need to be vigilant in protecting the privacy and security of Protected Health Information.

Here are a few resources to help guide your security program:

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- http://www.hcmarketplace.com/prod-7940-EHIPAAB/The-HIPAA-and-HITECH-Toolkit.html
- http://blogs.hcpro.com/hipaa/whitepapers/
- http://www.hcmarketplace.com/prod-7893/Business-Associates-and-Covered-Entities.html

Do you have questions on the material contained in this training? If so, please contact either Matt Maskart or Faye Witte for clarification.

Matt Maskart
Pathways HIPAA Security Officer
Phone #: 906-225-5138
Email: mmaskart@up-pathways.org

Faye Witte
Pathways HIPAA Privacy Officer
Phone #: 906-233-1201
Email: fwitte@up-pathways.org

Information Security Training:
Contract Employee

By signing below, I have read and I understand the contents of the Pathways' Information Security Training: Contract Employee training document. If I did not understand sections of the training, I contacted my supervisor or the Pathways HIPAA Security Officer for clarification.

Printed Name: _____

Date the training was completed: _____

Please print only this page and retain with your staff records. The Pathways' Contract Manager will review this document at the next Site Audit.