AL-APSES Security Awareness Presentation Text Only

Objectives

Review federal and state regulations regarding PII and PHI

Review responsibilities to prevent breaches of PII and PHI

Review financial and legal penalties for data breaches

Provide guidance regarding best practices

What is PII?

PII = Personally Identifiable Information

This is ANY information about an individual and may consist of name, SSN, place of birth, biometric records, address, age, gender, race, job position, etc. The IP network address of a person is even considered PII.

87% of the population can be identified by date of birth, zip code and gender

What is PHI?

PHI = Protected Health Information

Names, any location smaller than the State, phone/fax numbers, e-mail addresses, service or birth dates, etc.

Any information related to a client’s current, past or future mental or physical health

Any indication of health care treatment

Any indication of health insurance coverage

What is HIPPA?

HIPAA = Health Insurance Portability and Accountability Act

Regulations control how PHI data is stored, transmitted, and accessed to ensure a person’s PHI data is not disclosed to an unauthorized party

What is HITECH?

HITECH = Health Information Technology for Economic and Clinical Health Act

Further strengthens HIPAA with regard to ePHI

What is FERPA?

FERPA = Family Educational Rights and Privacy Act

Ensures a student’s educational data is secure

Grades, behavior, and enrollment are included

Requires written permission to disclose a student’s data to a 3rd party

Any child, even if they are over 18 years old, may have their educational records delivered to their parent as long as they are a dependent student

Be Paranoid!

Always assume someone is trying to get your data or obtain valuable information from you

Most common losses of data

These account for over 50% of data loss:

Laptop computers

Paper documents

USB drives and other portable storage media

Common causes of data loss;

Lost or stolen laptops, tablets, or smartphones

Lost or stolen tape, CD/DVD, or USB storage devices

Lost or misplaced paper containing PII/PHI data

Social engineering (you willingly provide the information)

Accidental release of information

Employee theft

Malware/Viruses

Hackers gaining access to your computer, network, or data storage

Most Commonly Target Industries

Computer (IT)

Government

Financial

Penalties for PHI Disclosure

Civil Penalties:

Up to $50,000 per person for each type of violation

Maximum of $1.5M per year

Criminal Penalties:

Up to $50,000 and one year in prison for obtaining or disclosing PHI

Up to $100,000 and five years in prison for obtaining PHI under false pretenses

Up to $250,000 and ten years in prison for obtaining PHI for personal gain

Example from June 2012

Alaska Department of Health and Social Services settled with HHS for $1.7M for HIPAA violations

Cause of breach was a stolen USB drive from an Alaska DHSS employee’s vehicle. The drive contained consumer data.

Employee of Massachusetts General Hospital took some client billing records home to work on them.

The employee mistakenly left them on the subway.

The hospital was fined $1M

Report Compromised Data

Service providers must immediately report any instance where PII or PHI data was compromised, or might have been compromised, to ADRS within 1 hour of discovery

The one hour notification is mandated by federal statutes

Begin making detailed notes

Get a police report if appropriate

Report the incident to supervisor and ADRS liaison

Common HIPPA Mistakes

Absence of ‘Right to Revoke’ clause on form

Accidental release of wrong patient’s information (two consumers with same name)

Release of too much health information

Failure to adhere to expiration date

Lack of signature

Improper disposal

Unprotected storage or transportation

Failure to provide timely release to consumer

Internal ‘snooping’ of data of friends and family

Posting to Social Networks

Never post/submit anything regarding a consumer to a social media service (e.g., Facebook, MySpace, Twitter, Instagram, etc.)

Even posting a consumer’s condition associated with your name could be a violation of client information

A photo an of x-ray without any other client information might even be regarded as confidential

Don’t post too much information on social media sites. This information could be used to guess your passwords or obtain enough information for identity theft.

Don’t indicate when you’ll be gone; especially on vacation.

Consumer Communication

Use only methods approved by the consumer (phone calls, texting, instant messaging, etc.)

Always encrypt e-mails unless authorized by release

Ensure you are using the correct e-mail address

Never discuss a consumer’s case in social media

Only use authorized telephone numbers

If leaving a voicemail, ensure you dialed the correct number first

It is best to obtain permission to leave voicemails as there could be an unintended party listening

Be careful of the information left on a voicemail or simply ask the consumer to return your call

You can leave a message with someone other than the consumer but leave only limited information

Ensure your phone calls are private

Communicating with Partners

ADRS is currently revising vendor agreements to include requirements for protecting PII and PHI

Make sure that any electronic communications is encrypted

Make sure any physical delivery is properly addressed

Make sure that you have the proper authorization and forms completed

Employee Termination

Employees must turn in all company-owned devices

Employees must ensure they DO NOT retain any documentation, or copies of, regarding consumers whether paper or electronic

Privately owned employee devices must be cleansed of consumer data

ADRS must be notified if employee does not turn in documents and devices containing consumer information

Physical Access to Records

Documents containing consumer information must be secured by double lock system

Data Storage Devices

No unauthorized person, including family members, should be allowed access to any resource capable of storing or accessing Consumer data

Physically destroy CD, DVD, and diskette media

Do not leave your laptop or smartphone in an unlocked vehicle

Do not leave your laptop or smartphone visible in any vehicle

Secure Backups Should Be:

Should be:

Encrypted

Physically Secure

Redundant

Passwords should be:

Everyone should have a password that is known to no one else

Never share your password with anyone and be sure you do not write it down

Always use complex passwords

Electronic Mail Data Protection:

Do not send emails containing PII or PHI information to external email addresses unless it is necessary and encrypted

Do not ‘Remember’ your webmail credentials on any computer

Cloud Storage

Storing PII or PHI information in a cloud service is NOT recommended

If you must use a cloud storage provider at least use multifactor authentication

Storing PII or PHI information in a cloud service is NOT recommended

Smartphone and Tablet Recommendations

Unless necessary, do NOT connect your smartphone to your computer

Use caution when storing any consumer information on your device or memory card within the phone

Consider having a screen-on login (e.g., PIN, password, pattern, etc.)

When using the WiFi hotspot feature, disable when no longer needed

Paper Files:

Paper files should not be left unattended even within the office

Paper files should not be taken out of the office unless absolutely necessary

Any copies of consumer files should be logged

Do not duplicate SSA provided information

Disposal of Paper Media:

Any documents containing PHI, PII or SSA provided data MUST be properly disposed of

The practical method of disposal is shredding

A third-party vendor, like Iron Mountain, may be used provided a record is made of the destruction and they are monitored

Ransomware:

Ransomware encrypts either your entire hard drive or certain files on your computer

May encrypt files on other computers

Demands money to decrypt your files

Prevent by using a non-Admin account

Prevent by executing only known applications

Recover by frequently backing up your data

Malware

Email Spoofing:

Watch out for email ‘Spoofing’

Spoofing occurs when someone sends a message to you that appears to come from someone else

Usually contains a virus infected attachment or link to infected website

Phishing

What had happened was…

Example of recent data breach

Questions