HIPAA

- **Privacy Rule:** Protects the privacy of individually identifiable health information, known as protected health information (PHI)

- **Security Rule:** National standards for the security of electronic protected health information

- **Breach Notification Rule:** Requires covered entities to and business associates to provide notification following a breach of unsecured PHI

- **Patient Safety Rule:** Protects identifiable information being used to analyze patient safety events and improved patient safety

What is HIPAA?

The Health Insurance Portability and Accountability Act, enacted in 1996, which requires healthcare providers / facilities to abide by certain regulations pertaining to patient information

Contoso
Pharmaceuticals

KNOWLEDGE QUIZ

Which of the following is NOT a best practice for privacy and security?

A) Keeping fax machines in areas that are not generally accessible

B) Keeping consumer records and other documents containing PHI out of sight

C) Documents containing PHI do not need to be shredded

D) Keeping medical records rooms locked/secured

Contoso
Pharmaceuticals

Key Terms

Protected Health Information (PHI)

- Any number of patient identifiers
  - Social Security Number
  - Telephone and Address
  - Diagnosis
  - Health Plan Beneficiary Number
  - Date of Birth
  - Medical Record Number

Covered Entities

- Any health care providers, health plans or clearinghouses that electronically transmit medical information
  - Billing
  - Claims
  - Enrollment
  - Eligibility Verification

Contoso
Pharmaceuticals

SOCIAL MEDIA VIOLATIONS

HIPAA violations perpetrated by individuals on social media breach both the Privacy and Security rules. In many cases, employees don't realize their behavior is violating HIPAA because of perceived security on social networks or a lack of understanding around HIPAA's definition of privacy.
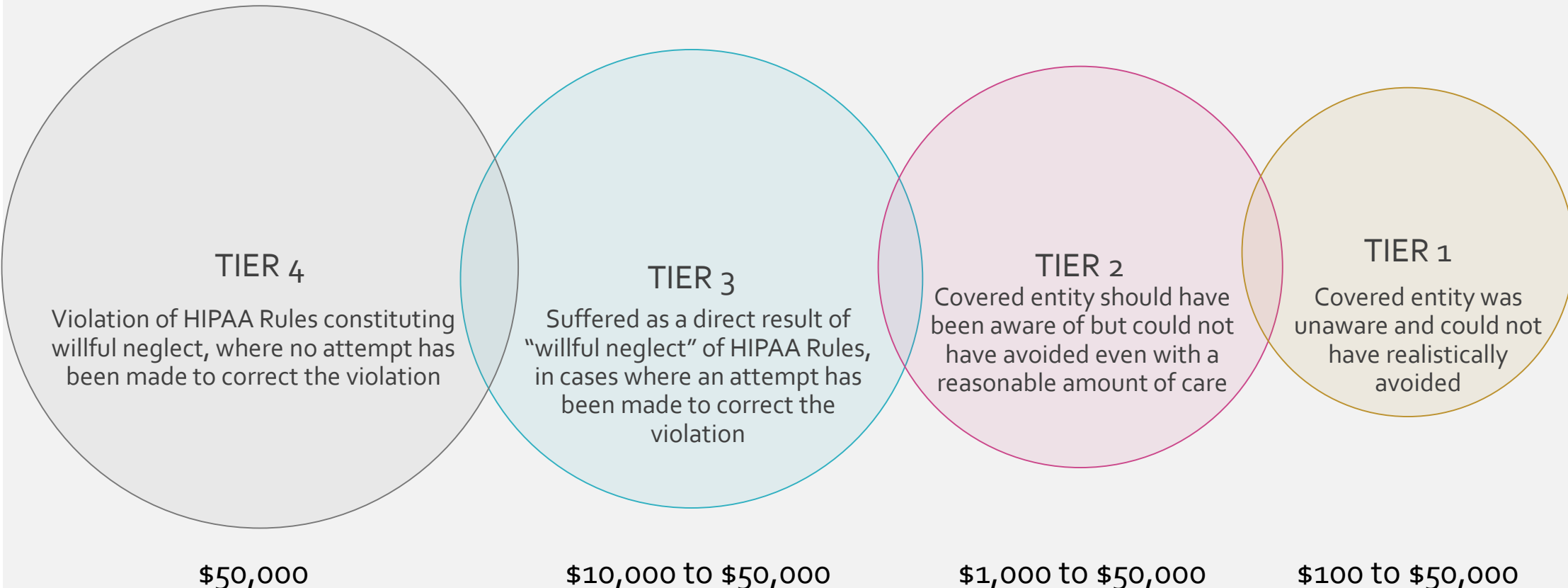
Contoso
Pharmaceuticals

KNOWLEDGE QUIZ

What kind of personally identifiable health information is protected by HIPAA privacy rule?

A) Paper

B) Electronic

C) The spoken word

D) All of the above

E) None of the above

Contoso
Pharmaceuticals

HIPAA VIOLATIONS

What happens if you violate HIPAA? That depends of the severity of the violation.

TIER 4
Violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation

TIER 3
Suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation

TIER 2
Covered entity should have been aware of but could not have avoided even with a reasonable amount of care

TIER 1
Covered entity was unaware and could not have realistically avoided

$50,000

$10,000 to $50,000

$1,000 to $50,000

$100 to $50,000

Contoso
Pharmaceuticals

The tiers of criminal penalties for HIPAA violations are:

- **Tier 1:** Reasonable cause or no knowledge of violation – Up to 1 year in jail
- **Tier 2:** Obtaining PHI under false pretenses – Up to 5 years in jail
- **Tier 3:** Obtaining PHI for personal gain or with malicious intent – Up to 10 years in jail

Criminal Penalties for HIPAA Violations

Contoso
Pharmaceuticals

KNOWLEDGE QUIZ

HIPAA security and privacy regulations apply to:

A) Attending physicians, nurses and other healthcare professionals

B) Health information managers, information systems staff and other ancillary personnel only

C) Anyone working in the facility

D) Only staff that have direct patient contact

Contoso
Pharmaceuticals

- Lost and Stolen Devices
- Hacking
- Employee Dishonesty
- Improper Disposal
- Third Party Disclosure
- Release of Information
- Unencrypted Data
- Lack of Training
- Unsecured Records
- Loud Mouths

TOP 10 HIPAA VIOLATIONS

Contoso
Pharmaceuticals

KNOWLEDGE QUIZ

Which of the following is the appropriate person with whom to share patient information even if the patient has NOT specifically authorized the release of information to the individual?

A) A former physician of the patient who is concerned about the patient

B) A colleague who needs information about the patient to provide proper care

C) A friend of the patient

D) A pharmaceutical salesman who is offering a fee for a list of patients to who he could send a free sample of his product

Contoso
Pharmaceuticals

— advice for —

STAYING HIPAA COMPLIANT

when using social media

What can healthcare providers do to help ensure HIPAA privacy and security rules are adhered to when posting online?

Here are five tips to avoid disclosing PHI when using social media.

NEVER POST ABOUT PATIENTS

It's extremely difficult to anonymize patients - even the subtlest identifier could land you and your practice in a lot of trouble.

DON'T TRUST MESSAGING SERVICES

Privacy of messages relies on the recipient keeping the information to themselves and not leaving themselves logged into public or office computers. Best to avoid private messaging altogether.

EDUCATE YOURSELF AND OTHERS

Staff should always be trained and kept up to date with HIPAA compliance best practices and company social media policies.

DON'T MIX WORK AND PERSONAL LIFE

Healthcare professionals should keep their personal and professional lives separate. Interacting with a patient online could result in PHI inadvertently being exchanged in the public domain.

WHEN IN DOUBT, DON'T POST

People can make mistakes in the heat of the moment. Always take a minute, read the post back to yourself, and consider the potential consequences before hitting the 'post' button

scrypt.com

Work confident.™

Contoso
Pharmaceuticals