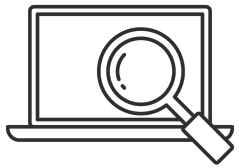
EVOLVE
Security

Secure Mechanisms for Data Handling in Healthcare

About Us

Evolve Security



CONTINUOUS PENETRATION TESTING

APPLICATION SECURITY

SECURITY ACADEMY

Brian Liceaga

- Penetration Testing
- Security Architecture
- Cloud Security
- DevSecOps
- Instructor

Agenda

- Preface
  - Let's hear about you
  - Data Breach Fatigue
  - Security Basics
- The Five Step Plan
  - Data Handling Examples

Data Breach Fatigue

- US data breaches in 2017: **1,002**
- US data breaches in 2016: **1,093**
- US data breaches in 2015: **780**

40%

In 2016, healthcare/medical industry represented 34.5% of data breaches. In 2017, this dropped to 26.3%.

Source: Identity Theft Resource Center (ITRC) and CyberScout

Totals for Category:	**Business**	**# of Breaches: 495**	**# of Records:**	**5,669,711**
		% of Breaches: 45.3	**%of Records:**	**15.5%**
Totals for Category:	**Educational**	**# of Breaches: 98**	**# of Records:**	**1,048,342**
		% of Breaches: 9.0%	**%of Records:**	**2.9%**
Totals for Category:	**Government/Military**	**# of Breaches: 72**	**# of Records:**	**13,869,571**
		% of Breaches: 6.6%	**%of Records:**	**37.9%**
Totals for Category:	**Medical/Healthcare**	**# of Breaches: 376**	**# of Records:**	**15,942,053**
		% of Breaches: 34.4	**%of Records:**	**43.6%**
	Totals for All Categories:	**# of Breaches: 1093**	**# of Records:**	**36,601,939**
		% of Breaches: 100.0	**%of Records:**	**100.0%**

2016 Breaches Identified by the ITRC as of:	**1/18/2017**

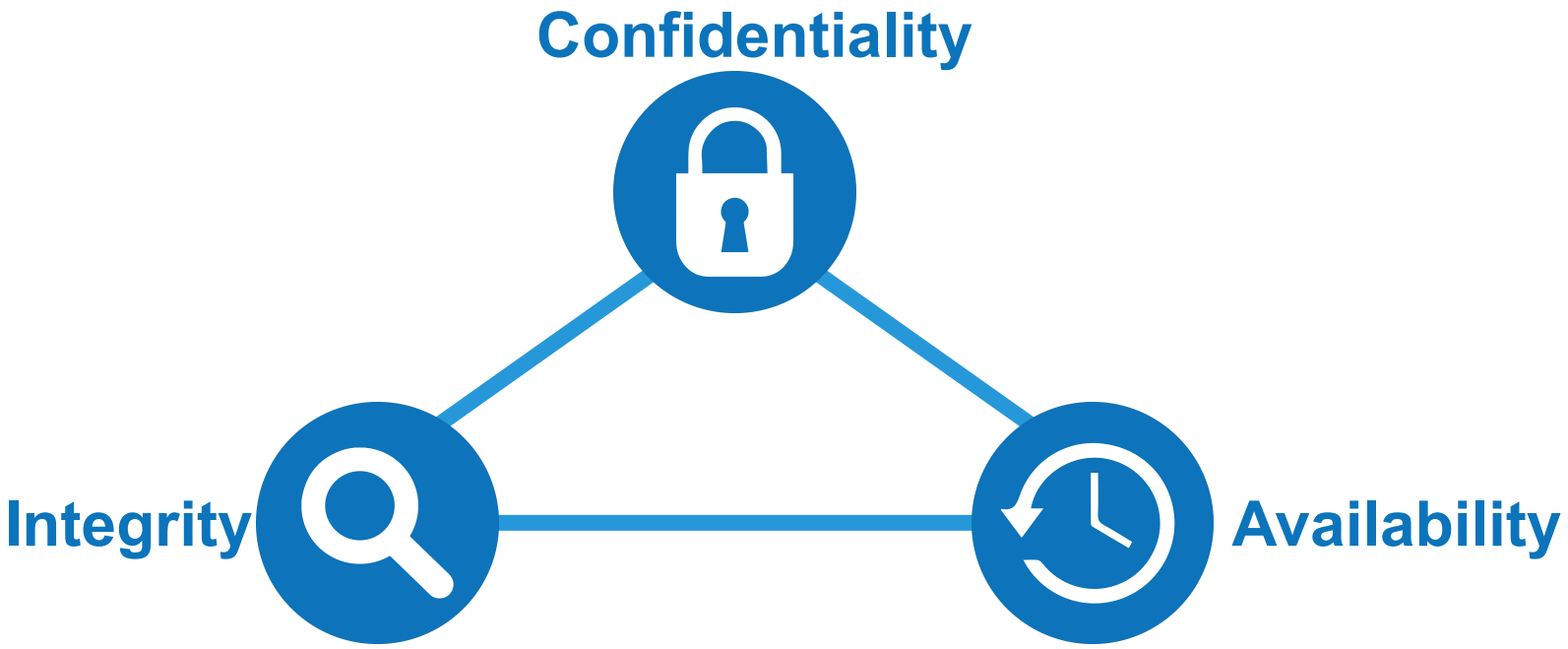
Total Breaches:	**1,093**
Records Exposed:	**36,601,939**

Totals for Category:	**Business**	**# of Breaches: 527**	**# of Records:**	**149,238,244**
		% of Breaches: 52.6	**%of Records:**	**91.5%**
Totals for Category:	**Educational**	**# of Breaches: 98**	**# of Records:**	**1,112,151**
		% of Breaches: 9.8%	**%of Records:**	**0.7%**
Totals for Category:	**Government/Military**	**# of Breaches: 49**	**# of Records:**	**5,767,061**
		% of Breaches: 4.9%	**%of Records:**	**3.5%**
Totals for Category:	**Medical/Healthcare**	**# of Breaches: 264**	**# of Records:**	**4,234,355**
		% of Breaches: 26.3	**%of Records:**	**2.6%**
	Totals for All Categories:	**# of Breaches: 1002**	**# of Records:**	**163,132,648**
		% of Breaches: 100.0	**%of Records:**	**100.0%**

2017 Breaches Identified by the ITRC as of:	**9/13/2017**

Total Breaches: 1,002
Records Exposed: 163,132,648

CIA Triad



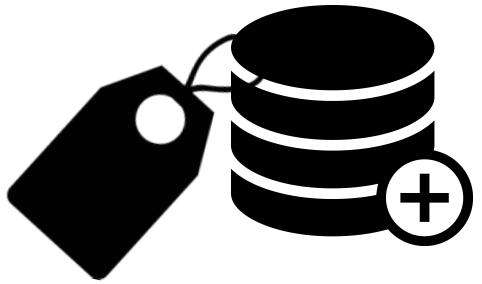
CIA Triad Examples

- **Confidentiality**
  - Access controls and cryptography
- **Integrity**
  - Protection: access controls and cryptography
  - Verification: hashing and message digests
- **Availability**
  - Fault tolerant architectures, redundancy, business continuity, disaster recovery

Five Step Plan

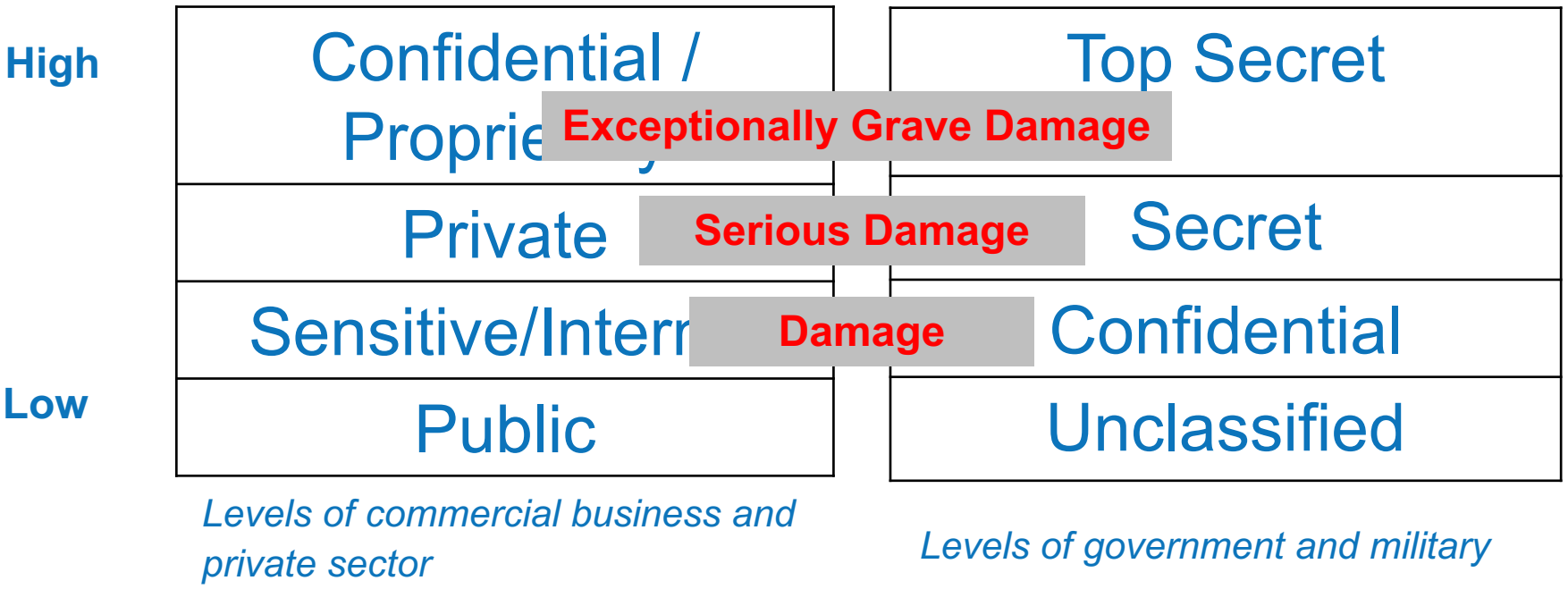
1. Create a policy!
   - Define tiers/classifications of data based on sensitivity
   - Define the necessary precautions for each classification
2. Be knowledge about applicable legislation and regulatory requirements
3. Stop proliferating and start tokenizing
4. Training and awareness
5. Have a response plan (and practice it!!!)

Step 1:
Create a Data Classification and Handling Policy



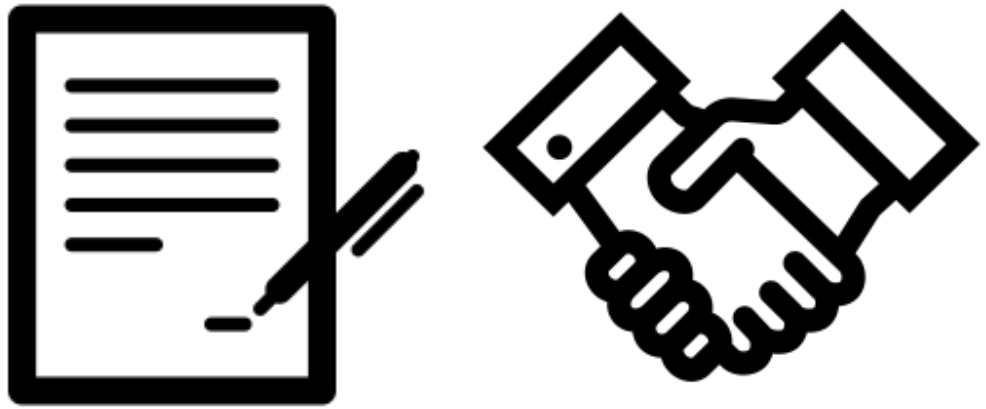
Classifying Data

Define tiers/classifications of data based on sensitivity



Data Classifications

- Agree upon what each classification means and provide examples



Personally Identifiable Information

- PII is any information about an individual maintained by an agency, including
  1. any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and
  2. any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

The Wealth of Health

Protected Health Information (PHI)

- Health information
  - Created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
  - Relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual
- Individually identifiable health information
  - identifies the individual; or
  - With respect to which there is a reasonable basis to believe the information can be used to identify the individual

Ownership and Accountability

- **Ownership** is the formal assignment of responsibility to an individual or group
  - Systems/applications and the data they process

- **Data Owner** – responsible for classifying information for placement and protection within the security solution (high-level manager)
- **Data Custodian** – responsible for the day to days tasks of implementing protections

Handling Data

- Define the necessary precautions and procedures for handling each classification
  1. Access
  2. Display
  3. Storage
  4. Transmission
  5. Disposal

The Goal

Provide the ultimate protection of data (of any medium) throughout its lifecycle!

Especially:

1. At rest
2. In transit
3. When displayed to the user

Image Source: Spirion

Data Handing Policy - Example

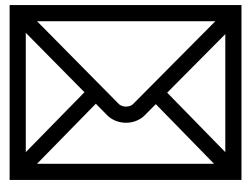
	Confidential/Private	Sensitive/Internal	Public
Access	…limited to individuals with a need to know business justification that have received appropriate approvals…	…need to know business justification and who are bound by a duty of confidentiality…	No requirements
Display	…electronic sensitive personal info must be masked as required by federal, state or local laws or regulations or industry standards…	…limited to individuals with appropriate access…	No requirements
Storage	…electronic sensitive personal info must be encrypted when stored…	…electronic data may only be stored on systems with access control…	No requirements
Transmission	…must be encrypted when sent via a secure connection…	…must be encrypted when sent via a public computer network…	No requirements
Disposal	…electronic device that has been known to have stored data must be wiped using industry standard wiping…	…printed data must be shredded or disposed of in a secure destruction bin…	No requirements

Strong Cryptography

- At Rest:
  - Symmetric encryption using AES 256
  - Integrity hashing with SHA2 or SHA3
- In Transit
  - HTTPS using TLS v1.2
    - Certificates signed using SHA2 (SHA-256) with RSA encryption
  - If required to use other transport protocols (e.g. FTP) be sure use the secure alternative (e.g. SFTP)

Email Security?

- Email is inherently insecure by default
  - Avoid sending sensitive information via email when possible
- Email can be more secure by using
  - End-to-end encryption (GPG/PGP)
  - S/MIME
  - DMARC (DKIM, SPF)



Multi-Factor Authentication

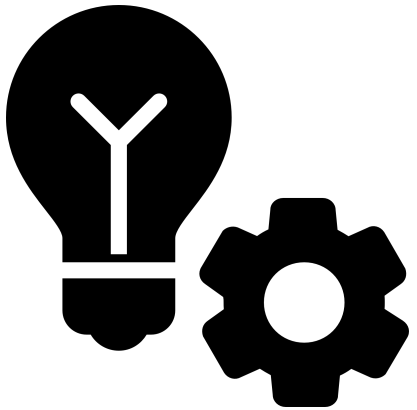
Factor 1 = Something you know

Factor 2 = Something you have

- One-Time Passwords (OTP)
  - Time based (TOTP)
  - Hash based (HOTP)
- Hardware or virtual tokens
- Commercial options available

Automation is Key

- Humans are the weakest link in the security chain
  - Errors and omissions
- No more spreadsheets…
- Leverage automation (e.g. HTTPS APIs) at every opportunity



The Value of APIs

- Connecting with Physicians and Patients (Public APIs)
  - Mobile apps, IoT
  - Facilitate the recording and management of physician-reported data
  - Leverage more data points to increase diagnosis accuracy
- Streamlining Healthcare Operations (Private APIs)
  - Private APIs for use by its employees (e.g. predict staff requirements)
  - Facilitate record sharing with hospitals and medical offices

Step 2:
Applicable Legislation and Regulatory Requirements

Common Legislation

- HIPAA
- PCI-DSS
- Privacy Laws
  - EU Data Protection Directive (to be superseded by the General Data Protection Regulation)
  - US has not federally adopted a comprehensive privacy law
- Breach Notifications
  - PII breaches this differs by US state
  - HIPAA covered entities must provide notification of the breach to affected individuals, the Secretary, and sometimes the media

Top Types of Breaches

Breaches affects 500 or more individuals

Type of Breach	Percent of Total
Theft	39.72%
Unauthorized Access/Disclosure	24.48%
Hacking/IT Incident	14.82%
Loss	6.73%
Other	4.02%

* Many breach notifications included multiple types and were listed as a separate “type of breach”
Source https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HIPAA Rules

- Privacy Rule
  - Regulates the use and disclosure of protected health information (PHI) in any medium
  - Covered entities must disclose PHI to the individual within 30 days upon request and when required to do so by law
- Security Rule
  - Covers electronic protected health information (ePHI) by laying out administrative, physical, and technical security safeguards
  - CIA triad protections

Implementing The Security Rule

NIST Special Publication 800-66 Revision 1

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

National Institute of Standards and Technology
U.S. Department of Commerce

Addressing the Technical Parts

- Access Controls
- Audit Controls
- Integrity
- Authentication
- Transmission Security

Step 3:
Stop Proliferating and Start Tokenizing

Fair Information Practices

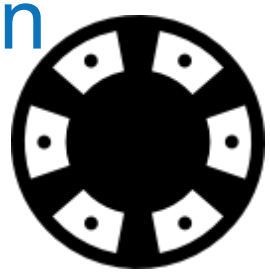
- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitations
- Security Safeguards
- Openness
- Individual Participation
- Accountability

HIPAA De-Identification

- Health information does cannot identify an individual
- Two ways
  1. Remove PHI specific Identifiers
     - Name, email address, phone number, etc. (see appendix for full list)
  2. Statistically calculate the possibility of re-identification is very small

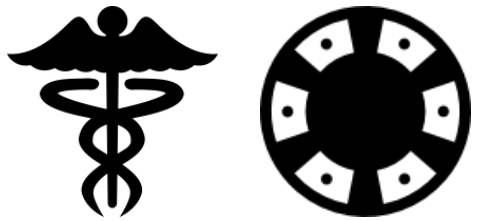
Tokenization

- Substitute a sensitive data element with a non-sensitive equivalent (token)
- Original data mapped from token via the tokenization system
- Benefits:
  - Minimized exposure of sensitive data
  - Very difficult for attacks to uncover original data *
  - Reduced risk in data breaches

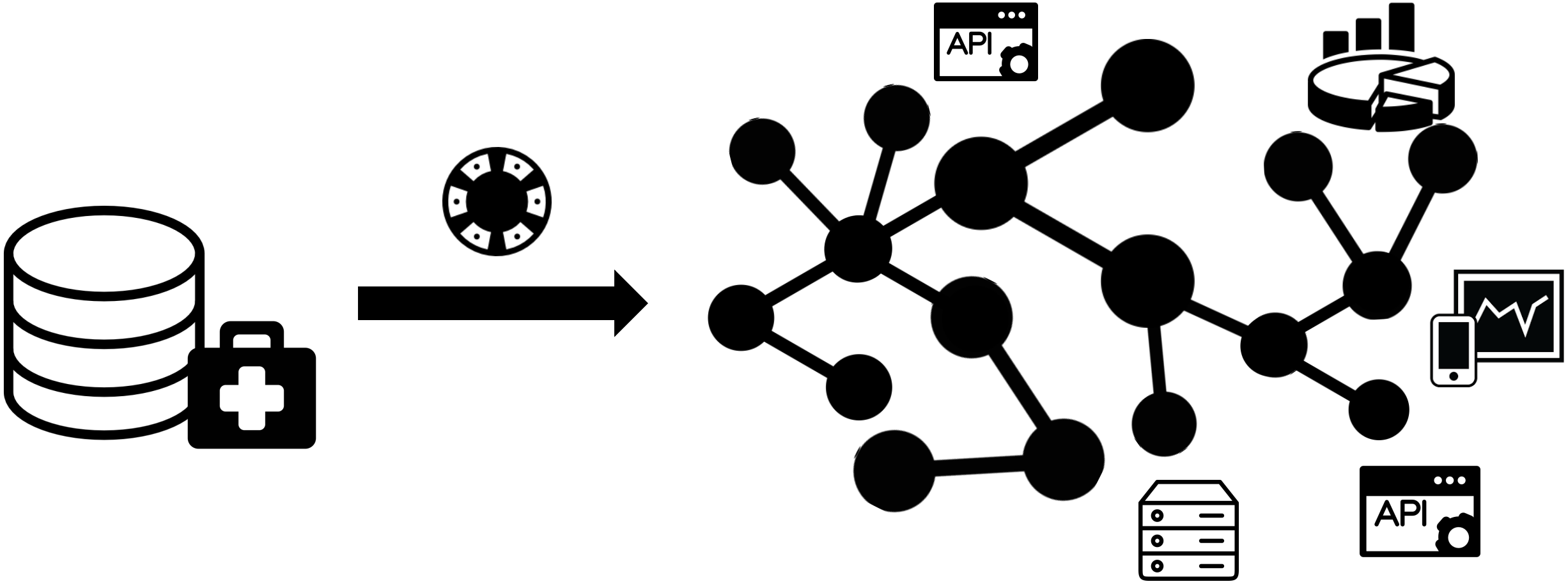


HIPAA Tokenization

- De-identified info can be re-identified provided that
  1. **Derivation:** token is not derived from the PHI/PII
  2. **Security:** mechanism for tokenization is not publically known and tokens are not disclosed



The Power of The Token

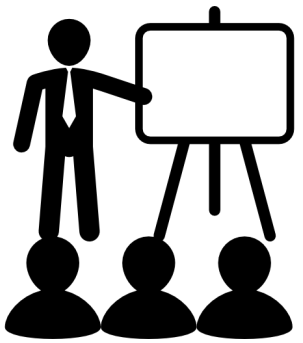


Step 4:
Training and Awareness

Training and Awareness

HIPAA Standard: *Implement a security awareness and training program for all members of its workforce*

- Require all employees to read the data classification and handling policy
- Require HIPAA training for appropriate individuals
- Conduct annual awareness training



Step 5:
Have a Response Plan

Incident Response

HIPAA Standard: *Implement policies and procedures to address security incidents*

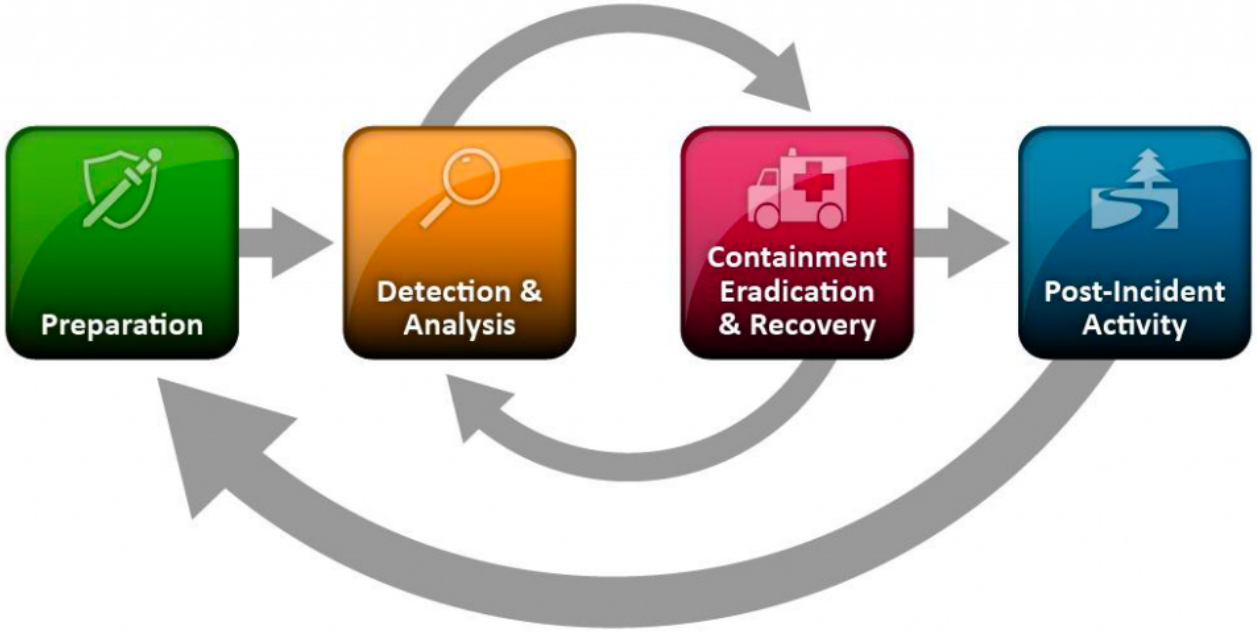


Image Source: NIST

Defining a HIPAA Breach

An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors

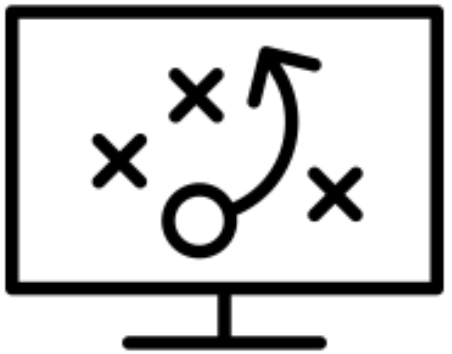
1. *The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;*
2. *The unauthorized person who used the protected health information or to whom the disclosure was made;*
3. *Whether the protected health information was actually acquired or viewed; and*
4. *The extent to which the risk to the protected health information has been mitigated.*

Key Activities

- Determine goals of IR
- Develop and deploy an IR team
  - ad hoc or formalized
- Develop and implement procedures to respond to and report security incidents
- Retrospectives and improvements
  - Incorporate post-incident analysis into updates and revisions

Once More! => The Five Step Plan

1. Create a policy!
   - Define tiers/classifications of data based on sensitivity
   - Define the necessary precautions for each classification
2. Be knowledge about applicable legislation and regulatory requirements
3. Stop proliferating and start tokenizing
4. Training and awareness
5. Have a response plan (and practice it!!!)



THANK YOU!

Contact: Brian Liceaga
Email: Info@EvolveSecurity.io

Evolvesecurity.io

Appendix

18 PHI Identifiers

1. Names
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

References

- http://www.idtheftcenter.org/
- NIST SP 800-122. *GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII).*
- NIST Special Publication 800-66 Revision 1. *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*