Information Security and Privacy

WHAT are the Guidelines?

HOW is it to be done?

WHY is it done?



WHAT are the guidelines

- Be in compliance of Federal/State Laws
  - **Federal:**
    - HIPAA - 1996
    - HITECH - 2009
    - GINA – 2009
    - OmniBus Ruling – 2013
  - **State:**
    - CA Constitution
    - WIC 4514
    - Information Practices Act
      - Civil Code Section 1798.29

18 Individual Identifiers

1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)
3. All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
4. Telephone numbers
5. FAX number
6. Email address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Any vehicle or other device serial number
13. Device identifiers or serial numbers
14. Web URL
15. IP address
16. Finger or voice prints
17. Photographic images
18. Any other unique identifying number, characteristic, or code

Terms/Definitions

- **Protected Health Information (PHI):** Data are "individually identifiable" if they include any of the ***18 types of identifiers*** for an individual or if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual.

- **"Individually identifiable health information (IIHI)" (**as defined by the Code of Federal Regulations (45 C.F.R. § 160.103), is information, including demographic data, that relates to:
  - the individual's past, present or future physical or mental health or condition,
  - the provision of health care to the individual, or
  - the past, present, or future payment for the provision of health care to the individual

Terms/Definitions

- **Medical information,** as defined by the Information Practices Act (Civil Code section 1798.29), means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

- **Health insurance information,** as defined by the Information Practices Act (Civil Code section 1798.29), means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

Terms/Definitions

Personal "Notice Triggering" Information as defined by the Information Practices Act (Civil Code section 1798.29) is more narrowly defined as unencrypted computerized data, specifically:

- Name (plus) one or more of the following:
  - SSN
  - DL number/State ID number
  - Financial account number, or
  - Medical or health insurance information
- State policy is to notify in cases of breaches of notice-triggering information, no matter what format



Three Categories of Safeguards

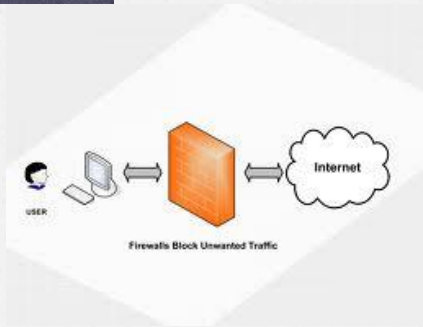
- Administrative Safeguards



- Physical Safeguards

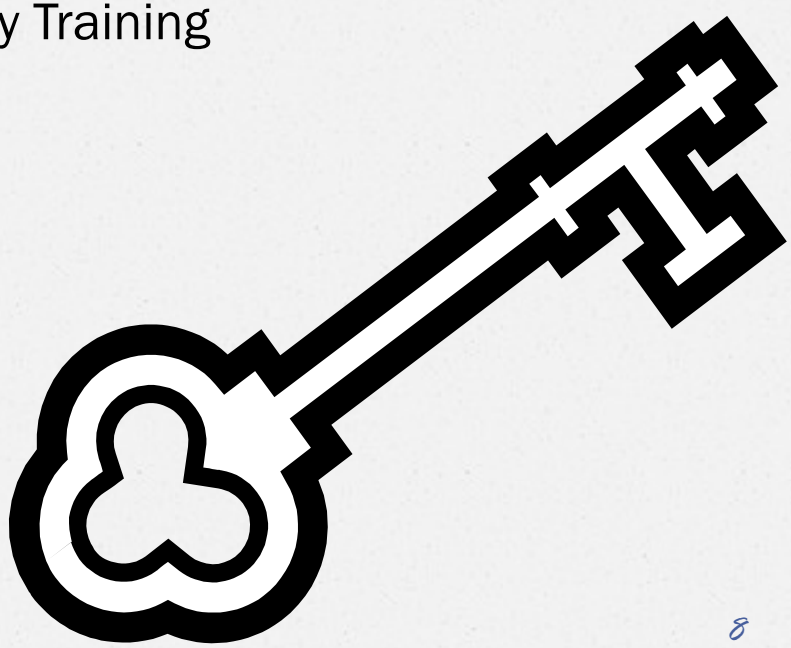


- Technical Safeguards



Administrative Safeguards

- Implement policies, procedures, and processes
- Implement Privacy and Security Training
- Review/update annually



Physical Safeguards

- Implement physical barrier.
  - Store confidential files in locked cabinets
  - Use card keys
  - Properly destroy physical and electronic data
    - Use locked security bins for confidential shredding
    - Do not leave confidential papers at printers, copiers and fax machines
    - Do not leave confidential papers unsecured
  - Confidential information should not be left unsecured at any worksite (e.g., office, home, hotel, remote location, etc.), or at any time when in transit between work locations (e.g., airplane, train, automobile, restaurant, etc.).



Physical Safeguards – (continued)

- **Basic Safeguard Tips include:**
  - Electronic storage media shall be kept locked
  - Keep locked doors secured (do not prop open)
  - Report unauthorized people in restricted areas
  - Never share codes, passwords, identity cards, or keys



Technical Safeguards

- Protection of Health Information depends on <u>everyone</u> being conscientious
  - Software applications designed to limit access
  - Implement minimum password standards
  - Use anti-virus and anti-malware protection
  - Enforce the principle of least privilege
  - Use auditing software that tracks and monitors access
  - **ENCRYPT** all end user devices (USB, laptops, etc.)

Technical Standards

- Federal Standards -
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53
  - Federal Information Processing Standards (FIPS)
- California State (and Business Associates)
  - State Information Management Manual (SIMM)

HIPAA Mandated Technical Safeguards

(continued)

Technical Safeguards: *"the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."*

Simply Put: *Technological solutions are required to protect ePHI.*

- Examples include Access Control, Ensuring Data Integrity and secure data transfer over the network.
- All electronic transmission of PHI must be appropriately encrypted. (ePHI)
- Protected Health Information residing on any form of electronic media or computing device must be encrypted if stored or taken off-site e.g. Backup CDs, DVDs, external Hard Drives, etc.
- Encryption must be achieved through software approved by the DDS Information Security Office.

Example: File Encryption Applications:

- 7-Zip (Windows)
- GNU Privacy Guard (Windows, Linux & Mac)
- AxCrypt (Windows)
- Credant-2-Go (Windows)
- WinRAR (Windows)
- PKWare SecureZip (Windows, Linux, IBMi)
- WinZip (Windows, Mac, Android, iOS)
- S.S.E. –Secret Space Encryptor (Android)

Example: Full Disk Encryption Applications :

- Microsoft BitLocker (Windows)
- EndPoint Encryption by TrendMicro (Windows, Linux & Mac)
- Full Disk Encryption by CheckPoint. (Windows & Mac)
- SDE – Symantec Drive Encryption (Windows & Linux)
- Dell Data Protection, formerly known as Credant (Windows)
- TrueCrypt (Linux & Mac, Windows version pending source code audit)

Encryption

- **IS NOT** STRONG PASSWORDS
- Encryption is putting data or a message into a coded form.
- Encryption protects data against loss or misuse.
- Encryption prevents a breach
- Encryption saves you $$$$
- It is the (HIPAA) law



The Cost of a Breach

- Fines are increasing: When HIPAA was first enacted, the maximum penalty for a HIPAA violation was $250,000. Now the maximum penalty is $1.5 million (criminal fine limits)

- Fines (civil) can now be levied by each State's Attorney General



Costly Breaches

- Min-**$50K** Max-**$250K**

  (**per individual**)
- The number of individuals affected
- (1,000 * $50K = $$$$$$$$$)
- Federal reporting is a lengthy process



Examples of Sanctions

- **Incident:** The HHS Office for Civil Rights (OCR) began its investigation following a breach report submitted by WellPoint. The report indicated that security weaknesses in an online application database left the electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet.

- **Penalties:** The managed care company WellPoint Inc. has agreed to pay the U.S. Department of Health and Human Services (HHS) **$1.7 million** to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.



Example of Sanctions (continued)

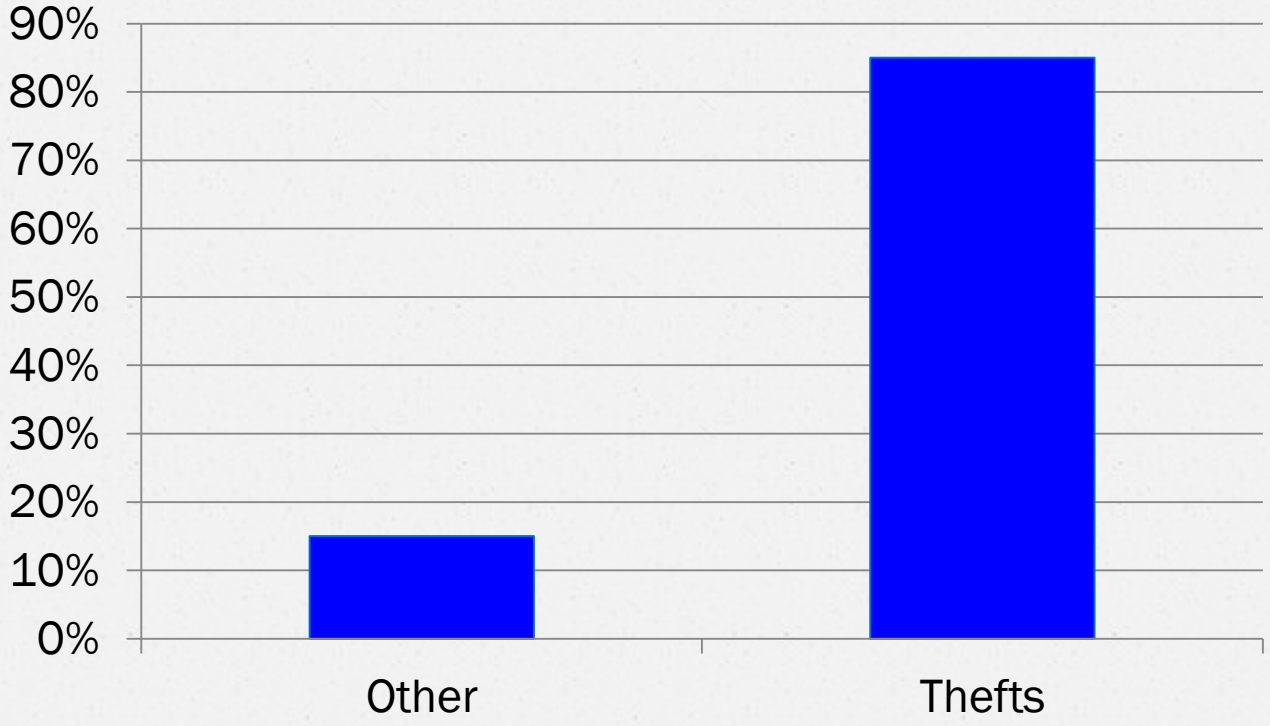
- **Incident:** Cignet, of Prince George's County, MD denied 41 patients, on separate occasions, access to their medical records when requested. This is a violation of the HIPAA Privacy Rule, which requires that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient's request. The company also failed to cooperate with the Office for Civil Rights' investigation.

- **Penalties:** The fine for the initial violation was **$1.3 million** OCR concluded that Cignet's committed willful neglect to comply with the Privacy Rule. The fine for these (civil money penalty) violations was **$4.3 million.**

What's in a name?

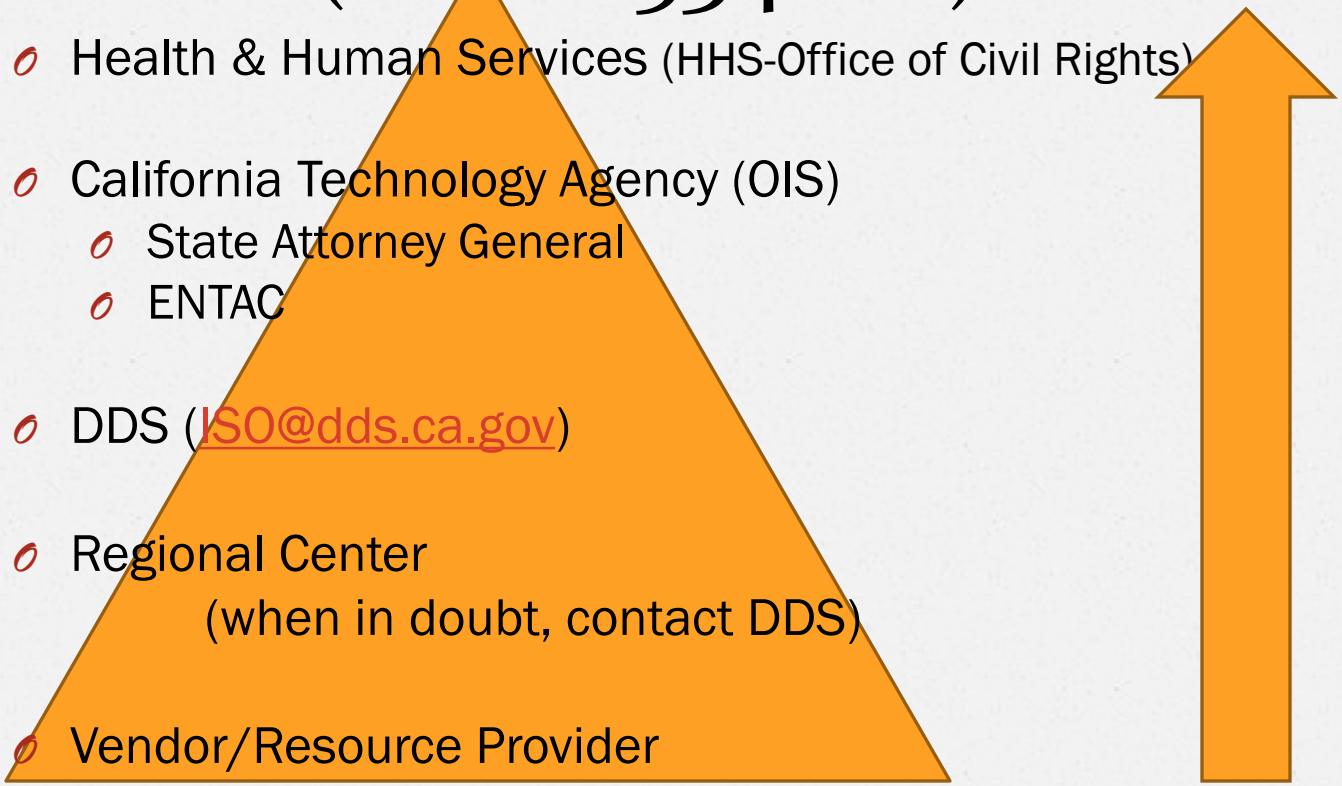
- Covered Entity
- Business Associate
  - 62% of data breaches involved a business associate, according to HHS.gov
- Business Associate of a Business Associate
- Vendor/Resource/Service Provider
- Contractor
- It doesn't matter!

DDS Breaches



Reporting Protocol (SIMM5340-B)

- Health & Human Services (HHS-Office of Civil Rights)
- California Technology Agency (OIS)
  - State Attorney General
  - ENTAC
- DDS (ISO@dds.ca.gov)
- Regional Center
  (when in doubt, contact DDS)
- Vendor/Resource Provider



Whom to contact

Department Developmental Services

1600 9th Street

Sacramento, CA 95814

- DDS Security Officer:
  - ISO@dds.ca.gov (Bryan Johnson)

- DDS Privacy Officer
  - privacy@dds.ca.gov (Elizabeth “Beth” Hibbert)

References

- NASCIO – Heart of the Matter
- NIST – National Institute of Standards and Technology (FIPS)
- SAM 5300 - Information Security
- SIMM – Incident (Breach) Reporting
  - 5340A Incident response instructions
  - 5340B Incident submission form
  - 5340C Notification information and examples
  - http://www.cio.ca.gov/Government/IT_Policy/SIMM.html#5300

Questions

?

Encryption Best Practices & Guidelines-

- Never use RC4 or triple DES (3DES) stream ciphers as they do not provide adequate security.
- Beware of what random number generators (RNG) are selected. Never use “Dual_EC_DRBG”
- Never use the SHA-1 or MD5 secure hash algorithms as they have been compromised.
- Always use a minimum of 128-bit cipher strength. Ideally, 192-bit or higher should be utilized.
- As a general rule, whenever possible use the Advanced Encryption Standard (AES) encryption specification.