



SECURITY & PRIVACY AWARENESS

Keeping our data safe

WHAT YOU
ALWAYS WANTED
TO KNOW BUT
WERE AFRAID TO
ASK



WHY ARE WE HERE?

WHY DO WE CARE?

- The Department of Developmental Services (DDS) is committed to providing leadership that results in quality services to the people of California and assures the opportunity for individuals with developmental disabilities to exercise their right to make choices.
- These disabilities include intellectual disability, cerebral palsy, epilepsy, autism and related conditions. Services are provided through a state-operated **developmental centers and a community facility**, and contracts with 21 nonprofit **regional centers**. The regional centers serve as a local resource to help find and access the services and supports available to individuals with developmental disabilities and their families.



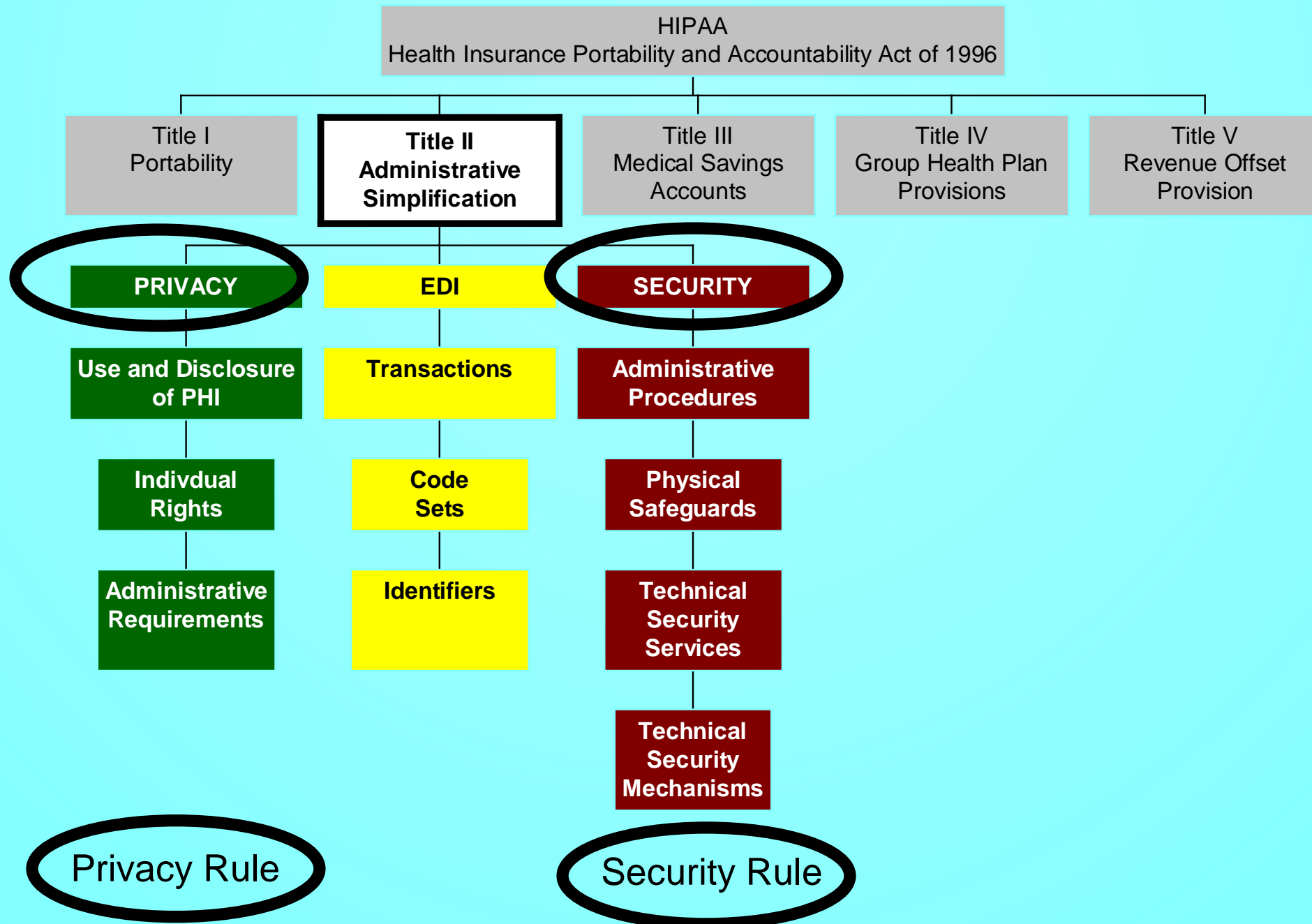
WHAT ARE THE GUIDELINES

Federal:

- 1996 - HIPAA
- 2009 - HITECH
- 2009 - GINA
- 2013 - Omnibus Ruling

State:

- California Constitution
- Information Practices Act - 1977
- WIC 4514
- Comprehensive Computer Data Access and Fraud Act (Penal Code 502)
- California Consumer Privacy Act (CCPA) January 1, 2020





WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

ACRONYM SOUP



PHI – Protected Health Information (*19 Identifiers*)

EPHI – Electronic protected health information

PII - Personally Identifiable Information

IHHI – Individually Identifiable Health Information

([45 C.F.R. § 160.103](#))

MII - Medical Identifiable Info., - defined by Information Practices Act

([Civil Code section 1798.29](#))

HII - Health Insurance Information

([Civil Code section 1798.29](#))

INDIVIDUAL IDENTIFIERS

NOTE: 2 NOTICE TRIGGERING(NT) ELEMENTS= BREACH

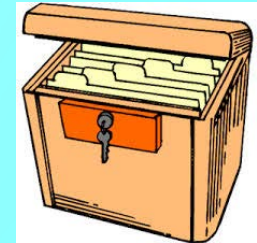
- Names; **(NT)**
- Addresses – all geographic subdivisions smaller than state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the currently publicly available data from the Bureau of the Census:
 - 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 is changed to 000.
- All elements (except year) for dates directly related to an individual (including birth date, admission date, discharge date, date of death and all ages over 89);
- Telephone numbers;
- FAX numbers;
- Electronic mail (email) addresses;
- Social Security numbers; **(NT)**
- Medical record numbers; **(NT)**
- Health plan beneficiary numbers; **(NT)**
- Account numbers; **(NT)**
- Online account username or email address, in combination with a password or security question and answer; **(NT)**
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web URL's;
- IP addresses;
- Biometric identifiers e.g., finger and voice prints, retinal scans, etc.;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code (e.g., UCI)
- **NOTE: In California unauthorized disclosure of an individual's "Name" and any other "notice-triggering" data element (in underlined, bold, RED) is considered a reportable breach.** In the U.S., a Federally reportable breach is unauthorized disclosure of any three (of the 18 individual identifiers) data elements. (Item #19 Vehicle license plate number is not a Federal personal individual identifying data element).

THREE CATEGORIES OF SAFEGUARDS

- Administrative Safeguards



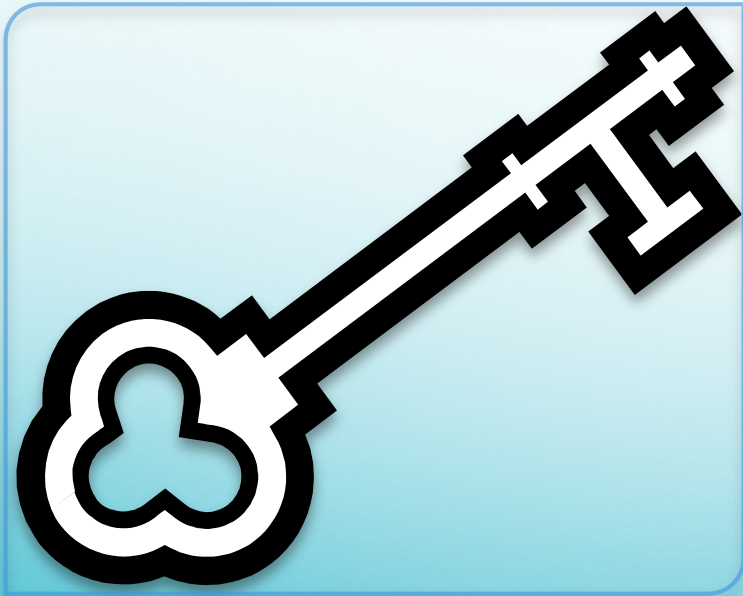
- Physical Safeguards



- Technical Safeguards



ADMINISTRATIVE SAFEGUARDS



- Conduct Risk Assessments
- Ensure Business Associates have an agreement in place
- Implement policies, procedures, and processes
- Implement Privacy and Security Training
- Review/update annually

RISK ASSESSMENT

- Organizational

- Identify assets
 - Information systems, sensitive data
- Potential threats to assets
 - Natural disasters, hacker attack, theft, mis-delivery
- Rate the risk of loss, damage, disclosure
- Put controls in place to mitigate the risk
 - Locked doors, login authentication, MFA, controls, patch management

- Individual

- Identify assets
 - Laptops, Consumer paper files
- Potential threats to assets
 - Theft, accidental loss, mis-delivery, discussing PHI in public location
- Rate the risk of loss, disclosure, etc. (*note: OCR \$50,000 per violation)
- Put controls in place
 - Take laptop/files with you, dispose of data safely, be aware of surroundings

BUSINESS ASSOCIATE AGREEMENTS



- Failure to have Business Associate Agreements with vendors who have access to PHI resulted in recent settlements of \$750K and \$155M!

POLICIES AND PROCEDURES

\$2.5 Million fine - Stolen laptop with ePHI of 1391 individuals

- No risk assessment or risk management processes in place
- No policies or procedures for mobile devices
- Security Rule policies ALL in draft form!

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultrices et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultrices et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

TRAINING

Provide new employee training on all policies and procedures

Review policies annually (update if necessary)

Provide updated annual staff training

PHYSICAL SAFEGUARDS

- Implement physical barriers
- Properly destroy physical (paper) including all notes and electronic data
- Shred paper or use locked security bins for confidential shredding
- Do not leave confidential papers at printers, copiers and fax machines
- Store confidential files in locked cabinets
- Use card keys
- **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, public transit, restaurant, etc.).



PHYSICAL SECURITY

- Remember to;
- Prevent Unauthorized Access
- Properly Secure Confidential Documents
- Use locked cabinets and doors
- Keep Computer Safe
 - At home
 - In Transit

PROPERLY DESTROY PHI ON PAPER

- **RECYCLING IS NOT SHREDDING!**
- PHI on paper **MUST** be protected and properly disposed of when not needed any more
- Even notes require the same safeguards as medical records
- Shredding is the correct way to dispose of papers with PHI (use a shredder or take your papers to the nearest “shred-it” container at least daily!





PROPERLY DESTROY EPHI

- Electronic equipment **MUST** be properly disposed of when not needed any more
- Electronic equipment with any data storage capability (computers, cell phones, tablets, printers, flash drives, etc.,) **MUST** be destroyed, wiped or made unreadable, before disposal or recycling
 - Wiping, degaussing, shredding (approved methods)
 - Certified vendors are available
 - Keep records!
- Guidelines for Media Sanitization
 - [NIST Special Publication 800-88](#)

Did you remember to wipe your old phone before handing it to a relative?


DDS – A PERFECT STORM

- 2018 – DDS blindsided breach –
when you least expect it..... Expect it.....
 - 12 midnight - vendor applies changes to phone system
 - Landlord fails to coordinate changes
 - 3 AM external actor breaches facility (*timing is everything*)
 - 5 AM fires inside building activate fire suppression system
 - 8 AM CHP notices flooding coming from inside of building
 - No direct action of the business was responsible for the breach
 - Results...

DDS – A PERFECT STORM

[Welcome](#) [File a Breach](#) [HHS](#) [Office for Civil Rights](#) [Contact](#)

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information



[Under Investigation](#) [Archive](#) [Help for Consumers](#)

Archive

This page archives all resolved breach reports and/or reports older than 24 months.

[Show Advanced Options](#) [Research Report](#)

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Valperaiso Fire Department	IN	Health Plan		09/03/2013	Theft	Desktop Computer
	Anthem Inc.	IN	Health Plan	78800000	02/13/2015	Hacking/IT Incident	Network Server
	CA Department of Developmental Services	CA	Health Plan	582174	04/06/2018	Theft	Paper/Films

COSTS:

- **ALMOST: \$1 Million Dollars**
- \$950,000 – in administrative costs
 - Staff Time
 - Postage
 - Call center
 - Displaced Staff (needed temporary office space)
 - Neighboring department damage

LESSONS LEARNED: ADMINISTRATIVE



- **RETENTION POLICIES**

- Email
- Documents

Having a policy in place that defines the retention schedule of documents based on their classification allows you to significantly “reduce the risk” to your organization.

**Note: your legal departments can often be instrumental in getting these policies in place.*



LESSONS LEARNED: PHYSICAL SECURITY

Tablet (cable locks)

- (ineffective, the cable locks were cut and removed within minutes).

Locked Rooms vs Locked Cabinets

- Locked Rooms
 - **Note: Everything in the room is considered a “potential breach” if not secured.*
- Locked Cabinets
 - *Everything in the affected cabinets is considered a “potential breach” if not secured.*

TECHNICAL SAFEGUARDS



- Protection of Health Information depends on everyone being conscientious
- At NBRC we:
 - Use 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 electronic devices (USB, laptops, desktops, servers, cell phones, etc.)

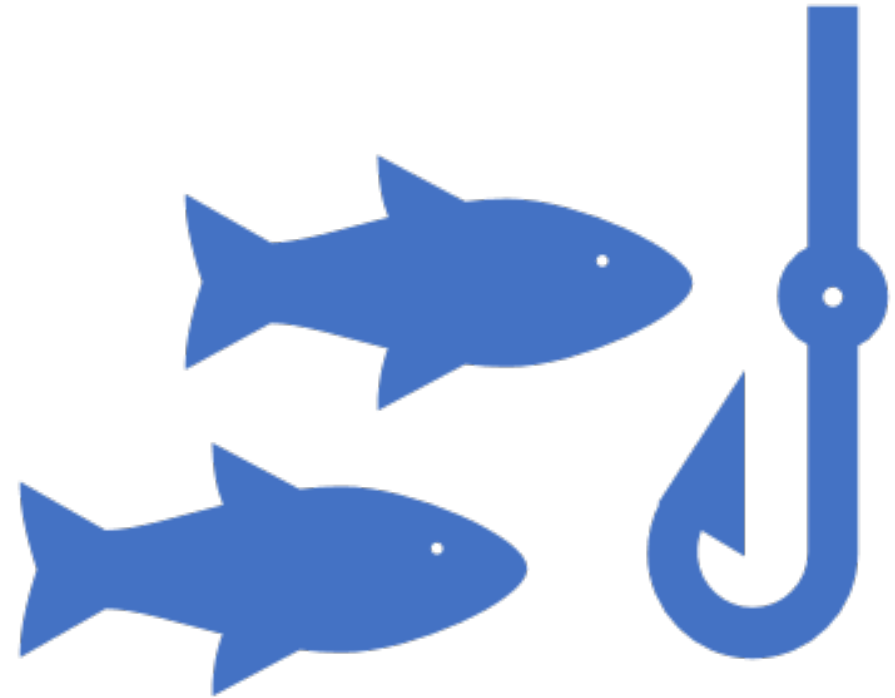
Encryption prevents the breach!

An illustration on the left side of the slide. It features a stylized circuit board with black lines and white circles on a dark grey background. Overlaid on this are several envelopes: a purple one at the top, a green one in the middle, and a brown one at the bottom. The brown envelope is open, showing a white card with a large blue '@' symbol. The entire graphic is set against a light blue background that transitions to a darker blue at the bottom.

EMAIL PRIVACY

- **ONLY** use your work email for work related purposes
- Put only the minimum amount of PHI (necessary to get the job done) in the email
- **ALWAYS ENCRYPT** email messages that include PHI
- Double check the “TO” recipients before clicking “Send”

PHISHING



PHISHING

- **COMMON PHISH**
 - The ancestor of all modern phish, beloved of Nigerian royalty, lonely hearts and helpful “pharmacists.” Its distinctive behaviors of poor spelling and awkward language make it easy to spot and avoid, but if it hooks its prey, the results can be deadly.
- **SPEARPHISH**
 - This monster picks its targets carefully based on the access they have to information it craves. May spend months lurking and researching its prey before it attacks with one targeted email strike.
- **CLONE PHISH**
 - Impersonates legitimate contacts and sends cloned messages with malicious links in place of genuine ones.
- **WHALING SHARK**
 - This greedy specimen will take only the biggest and juiciest catches. Its chosen prey includes the Common American CEO and the Red-Striped Financial Manager.





PHISHING SCAMS!

- Make sure you know and **verify the sender** of an email before you respond
- **Don't click on links** embedded in emails if the sender isn't someone you know
- **NEVER submit your system credentials** without verifying the need to do so through another method – call the Help Desk or the sender

PHISHING – TIS THE SEASON

- Flashy Emails
- Pickup Reminders
- Transaction Alerts
- Twitter & Facebook Posts
- Delivery Alerts
- Payment Reminders





HOW BIG IS THE PHISHING PROBLEM?

- Nearly **900,000 unique phishing attacks** were reported between April 2018 and March 2019
- Nearly **200,000 phishing websites** identified during the first quarter of 2019
- More than **10 million** unsafe or unwanted emails are blocked **every minute**
- Attackers send **6.2x more phishing emails** to corporate inboxes than personal inboxes

COMPROMISED EMAIL ACCOUNTS



- REMEMBER:
- Alert your IT Service Desk
 - **Immediately!**
- Disconnect from network.
- Reset your password.
- Do a risk analysis of 'potential' impact.

RANSOMWARE

- **Definition:** *it is a type of malware that stops users from accessing their data until payment is arranged.*
- **Average Cost was \$133,000** to a business in 2018.
- Malware **accounts for 56%** of all phishing attacks.
- **Estimated Health Organization costs in 2019 are 25 Billion!**
- If somebody encrypts your data, they have taken control of it and OCR considers it a breach.



TO SHARE OR NOT TO SHARE?

- Do not share passwords, keys, card keys, ID Badges, etc.,
- Do not use same password for business and personal
- Do not save on a sticky note
- Who is listening (Alexa/Google/?)
- IF YOU CARE..... DO NOT SHARE!!!



Password

PASSWORD OR PASSPHRASE?

LONGER IS ALWAYS MORE SECURE

CREATE A PASSPHRASE

- Time to hack:
- 5 Characters = 18 minutes
- 6 Characters = 2 ½ hours
- 7 Characters = 1 ½ days
- 8 Characters = 2 weeks
- 9 Characters = 1 month
- 10 Characters = 7 Weeks
- 11 Characters = 3 ½ months
- **16 Characters = 10 years**



PASSWORD OR PASSPHRASE?

- Password: **DgY4!v@7** ----Too complex to remember
- Passphrase: **i_love_dachshunds**
- Consider using a passphrase formula:
 - UsingXXXX@nbrciseasy
 - The XXXX is the system you are logging into:
 - Examples: Long and strong passphrases:
 - UsingDocushare@nbrciseasy
 - UsingSignNow@nbrciseasy
 - UsingSandis@nbrciseasy
 - UsingWindows@nbrciseasy

THE COST OF NOT ENCRYPTING

"Because theft and loss are constant threats, failing to encrypt mobile devices needlessly puts patient health information at risk... When covered entities are warned of their deficiencies, but fail to fix the problem, they will be held fully responsible for their neglect." - Roger Severino, OCR Director.

- **NEVER** keep ePHI on an unencrypted device!
 - recent fines for just 1 missing laptop with ePHI were **\$1.5Million** and **\$1.7Million!**
 - a lost thumb drive with ePHI on it cost a small dermatology practice **\$150,000** in fines!

November 5, 2019

Failure to Encrypt Mobile Devices Leads to \$3 Million HIPAA Settlement

The University of Rochester Medical Center (URMC) has agreed to pay \$3 million to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. URMC includes healthcare components such as the School of Medicine and Dentistry and Strong Memorial Hospital. URMC is one of the largest health systems in New York State with over 26,000 employees.

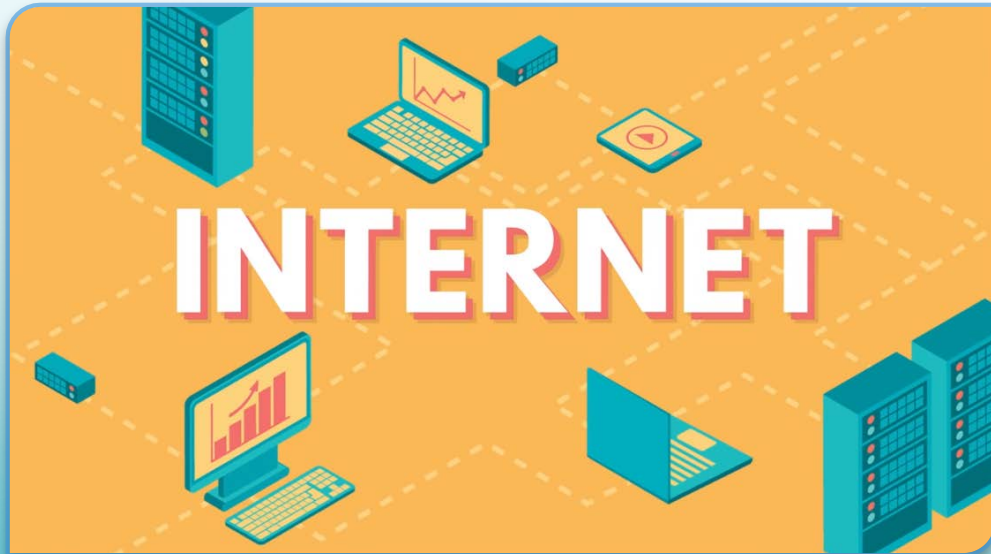
URMC filed breach reports with OCR in 2013 and 2017 following its discovery that protected health information (PHI) had been impermissibly disclosed through the loss of an unencrypted flash drive and theft of an unencrypted laptop, respectively. OCR's investigation revealed that URMC failed to conduct an enterprise-wide risk analysis; implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; utilize device and media controls; and employ a mechanism to encrypt and decrypt electronic protected health information (ePHI) when it was reasonable and appropriate to do so. Of note, in 2010, OCR investigated URMC concerning a similar breach involving a lost unencrypted flash drive and provided technical assistance to URMC. Despite the previous OCR investigation, and URMC's own identification of a lack of encryption as a high risk to ePHI, URMC permitted the continued use of unencrypted mobile devices.

"Because theft and loss are constant threats, failing to encrypt mobile devices needlessly puts patient health information at risk," said Roger Severino, OCR Director. "When covered entities are warned of their deficiencies, but fail to fix the problem, they will be held fully responsible for their neglect."

In addition to the monetary settlement, URMC will undertake a corrective action plan that includes two years of monitoring their compliance with the HIPAA Rules. The resolution agreement and corrective action plan may be found at <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/urmc/index.html>.

IT'S A MOBILE WORLD

KNOW WHO YOU ARE CONNECTED TO



- **DO NOT...**

- Connect to any Wi-Fi that;
 - You don't know.
 - That does not require a password

- **DO**

- Use your cell phone hotspot if you can.
- Be sure to set up a password on your home Wi-Fi that is hard to crack

A decorative graphic on the left side of the slide, consisting of a network of light blue lines and small circles, resembling a circuit board or a neural network, extending from the top to the bottom.

INCIDENT MANAGEMENT & RESPONSE

WHAT IS A BREACH?

- **Breach or Breaches** – “Breach” or “Breaches” have the same meaning of the term “breach” defined under 45 CFR § 164.402, which is the acquisition, access, use or disclosure of PHI in a manner not permitted under Title 45 of the CFR Part 164, Subpart E, that compromises the security or privacy of PHI...
- **Simply:** A breach can be defined as the disclosure of protected information to an unauthorized recipient.

WHO'S WHO?

COVERED ENTITIES (CE)

- **BUSINESS ASSOCIATES (BA)**

DEPT. DEVELOPMENTAL SERVICES (CE)

- **REGIONAL CENTERS (BA)**

REGIONAL CENTERS (BA)

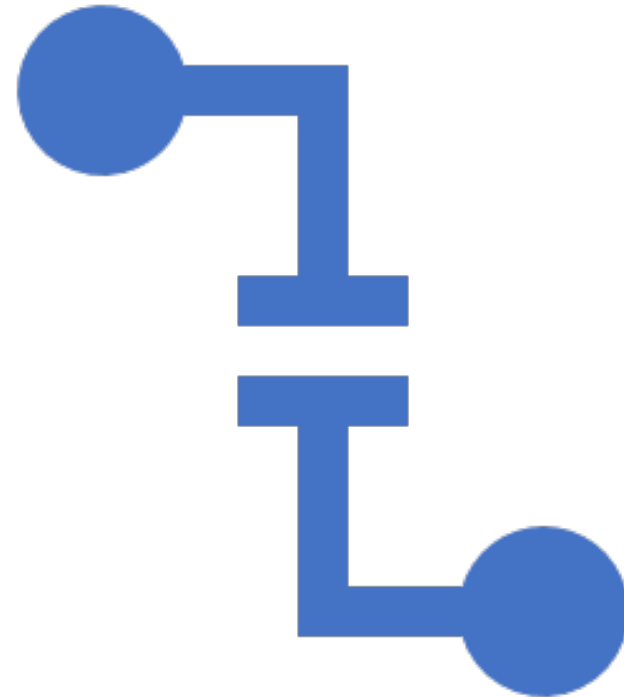
- **VENDORS (BA)**
- **SERVICE PROVIDERS (BA)**
- **CONTRACTOR (BA)**



WHO'S RESPONSIBLE?

OMNIBUS 2013...

HE WHO HOLDS THE DATA
OWNS THE BREACH!





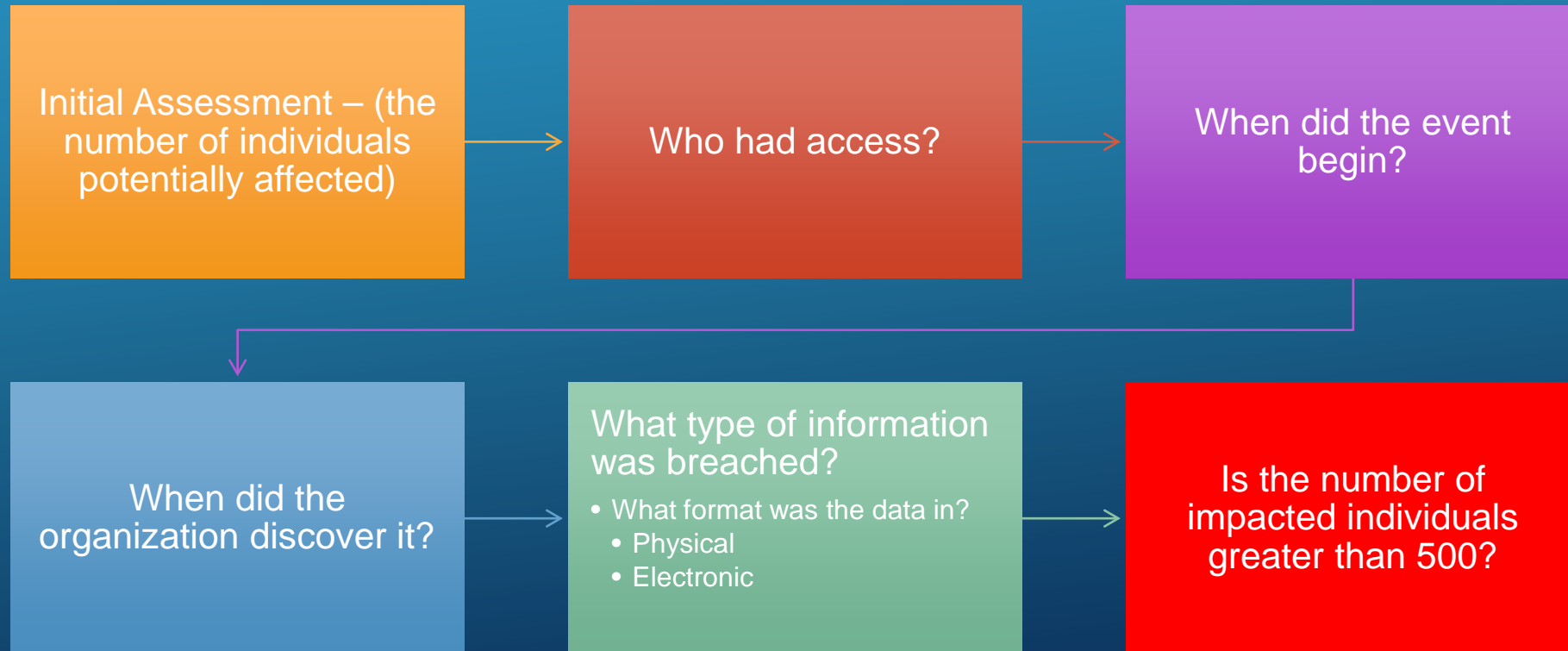
ACTIONS? WHAT'S NEXT?

SCOPE...

CONTACTS...

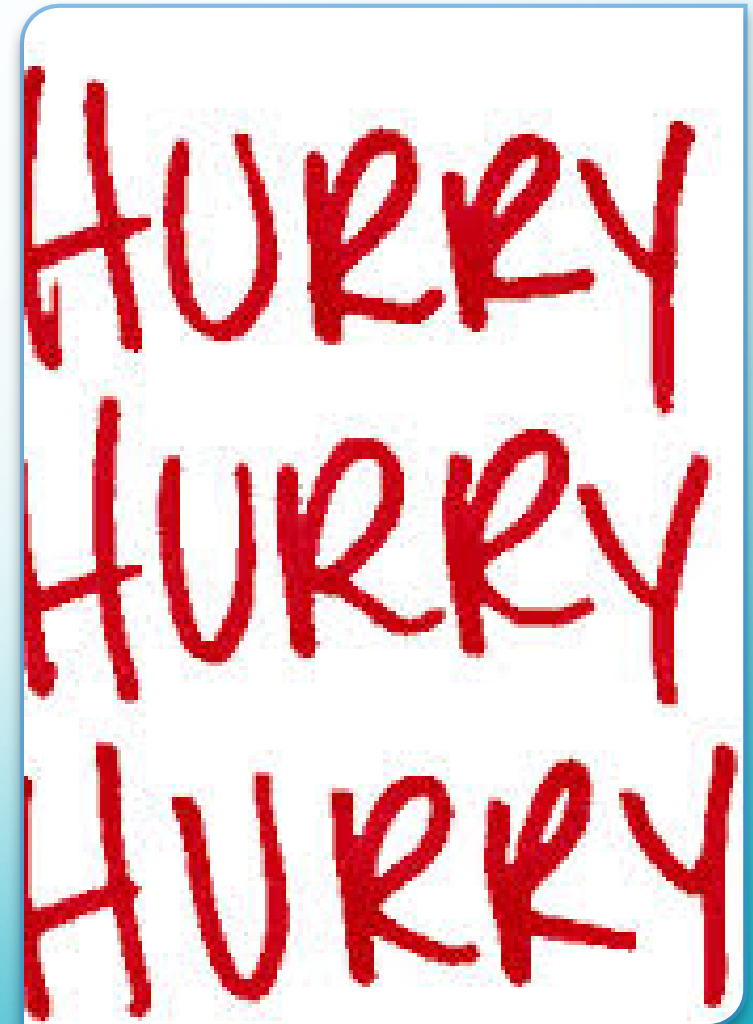
REPORTING...

DEFINING THE SCOPE



NEXT STEPS...

- Alert your Covered Entity within 72 hours (form: DS 5340B)
 - Vendors/Service Providers - contact your Regional Center
 - Regional Centers - contact DDS Information Security Office (iso@dds.ca.gov)
- **COMMUNICATE...COMMUNICATE...**





INCIDENT REPORTING

Remember to..

- Play it safe
- Immediately report Cyber Security Incidents
- Seconds can count
- Privacy Breach:

*Notification letter to be mailed to impacted individuals in less than **60 days** from the date of discovery.*

NOTIFICATIONS AND REPORTING

INDIVIDUALS IMPACTED

LESS THAN 500

- Notify Covered Entity (CE) within 72 hours of discovery
- Breach notification letter to all individuals **within 60 days** of breach discovery ([CA Civil Code §1798.29](#))

** Alternate notification required if accurate contact information missing for 10 or more individuals*

- Notify Office for Civil Rights (OCR) no later than February 28th of calendar year following breach discovery year

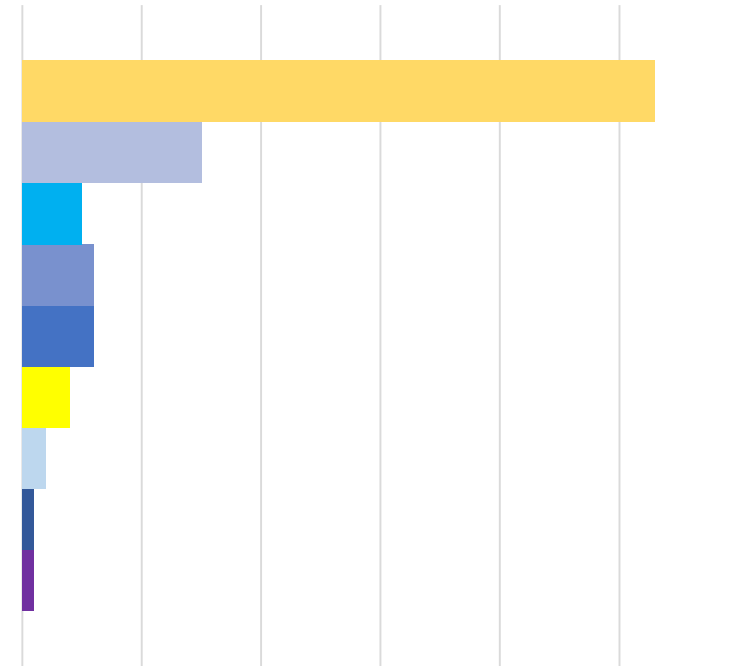
500 OR MORE

- Notify Covered Entity (CE) within 72 hours of discovery
- Breach notification letter to all individuals **within 60 days** of breach discovery ([CA Civil Code §1798.29](#))
- Alternate notification required if accurate contact information missing for 10 or more individuals
 - Either website home page for 90 days, or
 - Major local print/broadcast media
- Provide notice to prominent media outlets serving the State or jurisdiction no later than 60 days of discovery (press release, e.g.)
- Toll-free phone number active at least 90 days
- Notify Office for Civil Rights (OCR) **within 60 days of the breach discovery date** at the **LATEST!**

DDS INCIDENTS REPORTED 2019

Incidents Reported to DDS in 2019

- Mail incorrect individual
- Email incorrect individual
- Theft from vehicle; break-in
- Email PHI and forget to encrypt data
- Disclosure
- Lost paper documents
- Fax incorrect individual
- Vandalism
- Email account compromised (phishing response)



BEST PRACTICES

INCIDENT RESPONSE:



Have an Incident Response Plan (*for common cyber events*)!

- Complete a risk assessment, know your vulnerabilities

Ensure, your organization has a “Incident Response Team”

- Ensure staff know where to find the plan
- Test the plan
- Ensure your executive management team as endorsed it.
- (Sometimes, seconds count!)

PENALTIES ARE INCREASING

- Up to \$50,000 per impacted individual



October 23, 2019

OCR Imposes a \$2.15 Million Civil Money Penalty against Jackson Health System for HIPAA Violations

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services has imposed a civil money penalty of \$2,154,000 against Jackson Health System (JHS) for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Breach Notification Rules between 2013 and 2016. JHS is a nonprofit academic medical system based in Miami, Florida, which operates six major hospitals, a network of urgent care centers, multiple primary care and specialty care centers, long-term care nursing facilities, and corrections health services clinics. JHS provides health services to approximately 650,000 patients annually, and employs about 12,000 individuals.

On August 22, 2013, JHS submitted a breach report to OCR stating that its Health Information Management Department had lost paper records containing the protected health information (PHI) of 756 patients in January 2013. JHS's internal investigation determined that an additional three boxes of patient records were also lost in December 2012; however, JHS did not report the additional loss or the increased number of individuals affected to 1,436, until June 7, 2016.

In July 2015, OCR initiated an investigation following a media report that disclosed the PHI of a JHS patient. A reporter had shared a photograph of a JHS operating room screen containing the patient's medical information on social media. JHS subsequently determined that two employees had accessed this patient's electronic medical record without a job-related purpose.

On February 19, 2016, JHS submitted a breach report to OCR reporting that an employee had been selling patient PHI. The employee had inappropriately accessed over 24,000 patients' records since 2011.

OCR's investigation revealed that JHS failed to provide timely and accurate breach notification to the Secretary of HHS, conduct enterprise-wide risk analyses, manage identified risks to a reasonable and appropriate level, regularly review information system activity records, and restrict authorization of its workforce members' access to patient ePHI to the minimum necessary to accomplish their job duties.

JHS waived its right to a hearing and did not contest the findings in OCR's Notice of Proposed Determination. Accordingly, OCR issued a Notice of Final Determination and JHS has paid the full civil money penalty.

"OCR's investigation revealed a HIPAA compliance program that had been in disarray for a number of years," said OCR Director Roger Severino. "This hospital system's compliance program failed to detect and stop an employee who stole and sold thousands of patient records; lost patient files without notifying OCR as required by law; and failed to properly secure PHI that was leaked to the media."

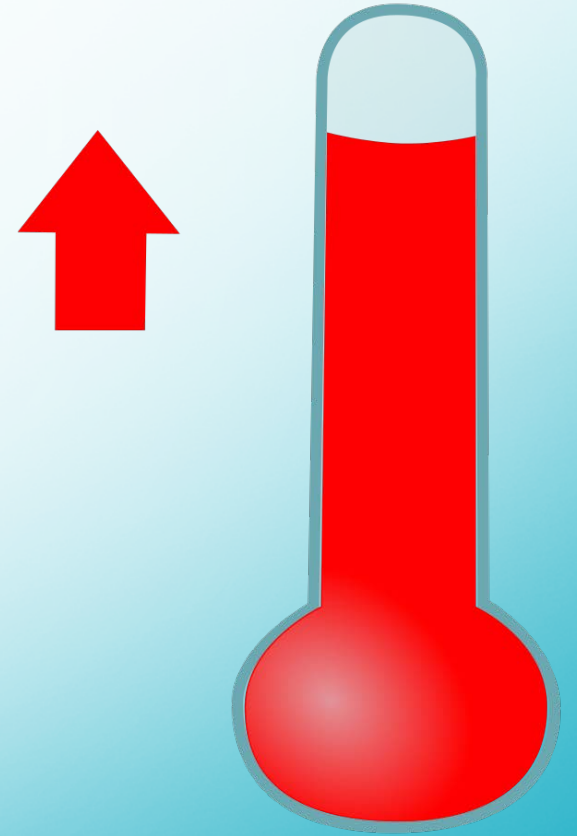
The Notice of Proposed Determination and Notice of Final Determination may be found at: <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/jackson/index.html>.

OFFICE FOR CIVIL RIGHTS (OCR)

THE TEMPERATURE IS INCREASING!

Roger Severino, OCR Director:

- November 5, 2019: "Because theft and loss are constant threats, failing to encrypt mobile devices needlessly puts patient health information at risk. When covered entities are warned of their deficiencies, but fail to fix the problem, they will be held fully responsible for their neglect."
- November 27, 2019: "When health care providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by OCR."
- December 30, 2019: "The last thing patients being wheeled into the back of an ambulance should have to worry about is the privacy and security of their medical information. All providers, large and small, need to take their HIPAA obligations seriously."





REFERENCES

ADDITIONAL
RESOURCES
FOR YOUR
REFERENCE

RECOMMENDED EMAIL SUBSCRIPTIONS

- OCR HIPAA Privacy Rule Information Distribution:
 - <https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-PRIVACY-LIST&A=1>
- OCR HIPAA Security Rule Information Distribution:
 - <https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-SECURITY-LIST&a=1>

GOVERNMENT - 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 Administrative Manual ([SAM](#))
- State Information Management Manual ([SIMM](#))

PARTING THOUGHTS

YOU HOLD THE KEY

Security & Privacy



Contact information:

Department Developmental Services

1600 9th Street

Sacramento, CA 95814

DDS Security Office:

ISO@dds.ca.gov

Thank you!

