Compliancy Group
HIPAA Done Right.™

HIPAA Year in Review:

Lessons & Examples from 2019's HIPAA Breaches and Fines

Compliancy Group Free Education Series

Upcoming & past webinars:
http://compliancy-group.com/webinar/

Free Resources *(whitepapers, articles, infographics)*
https://compliancy-group.com/blog/

Please ask questions
If we are unable to address them during the webinar, you will receive a response via email within 24-48 hours.

We simplify compliance so you can confidently focus on your business.

No client has ever Failed an OCR or CMS audit!

The Guard™ Endorsed by:

- Health Care standard - 40+ medical associations
- Used by Industry Leading MSPs, SaaS providers, Hosting providers, Security consultants, etc.
- Top medical & Insurance specialties

Recognized Leader of Compliance & Cyber Security

- 2017 ChannelPro Visionary
- CRN Emerging technology
- CompTIA Channel Advisory Board – Co Chair
- CompTIA Business Applications Advisory Council – Chair

Subject Matter Experts

- National Publications – Becker's Hospital Review, ChannelE2E
- Recognized National speaker - CompTIA , MedRO360
- Software Executive Magazine - editorial Board

The Seven Fundamental Elements of an Effective Compliance Program

Compliance According to HHS:

1. *Implement written policies, procedures and standards of conduct.*
2. *Designate a person to ensure they are followed.*
3. *Conduct effective training and education.*
4. *Develop effective lines of communication.*
5. *Conduct internal monitoring and auditing.*
6. *Enforce standards through well-publicized disciplinary guidelines.*
7. *Responding promptly to detected offenses and undertaking corrective action.*

Reference: https://oig.hhs.gov/compliance/provider-compliance-training/files/compliance101tips508.pdf

HIPAA Compliance

What Causes an Audit?

Not One, But Two Breaches!

- **Who**: Cottage Health
- **What**:
  - 1st breach – ePHI on a Cottage Health server was accessible from the internet (no usernames or passwords were being used to access files)
  - 2nd breach – misconfigured server exposed ePHI over the internet
- **Settlement**: **$3,000,000**
- **Why**: Risk Analysis / Remediation, No BAA

*"The Cottage settlement reminds us that information security is a dynamic process and the **risks to ePHI may arise before, during, and after** implementation covered entity makes system changes." – OCR Director Roger Severino*

https://www.hhs.gov/about/news/2019/02/07/ocr-concludes-all-time-record-year-for-hipaa-enforcement-with-3-million-cottage-health-settlement.html

Reporting a Breach is NOT optional!

- **Who**: Touchstone Medical Imagining
- **What**: Server was breached allowing access to ePHI, and patients were not notified of the breach
- **Settlement**: **$3,000,000**
- **Why:** Risk Analysis, Breach Notification, Failure to Investigate Breach, No BAA with IT Firm.

"Covered entities must respond to suspected and known security incidents with the seriousness they are due, especially after being notified by two law enforcement agencies of a problem," said OCR Director Roger Severino. "Neglecting to have a comprehensive, enterprise-wide risk analysis, as illustrated by this case, ***is a recipe for failure.****"*

https://www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html

Watch Out for Hackers!

- **Who:** Medical Informatics Engineering.
- **What:** Hackers used a compromised user ID and password to access approximately 3.5 million patient records.
- **Settlement:** **$100,000**
- **Why:** No Risk Analysis

*"Entities entrusted with medical records **must be on guard against hackers**," said OCR Director Roger Severino. "The failure to identify potential risks and vulnerabilities to ePHI opens the door to breaches and violates HIPAA."*

https://www.hhs.gov/about/news/2019/05/23/indiana-medical-records-service-pays-100000-to-settle-hipaa-breach.html

Don't Ignore Patients Right to Access!

- **Who**: Bayfront Health St. Petersburg
- **What**: Failed to provide a mother timely access to records about her unborn child
- **Settlement**: **$85,000**
- **Why**: HIPAA Right of Access violation.

*"Providing patients with their health information not only lowers costs and leads to better health outcomes, **it's the law,**" said OCR Director Roger Severino. "We aim to hold the healthcare industry accountable for ignoring peoples' rights to access their medical records and those of their kids."*

https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html

Social Media is NOT for Sharing PHI!

- **Who**: Elite Dental Associates
- **What**: Responded to a social media review by disclosing patient's last name and health condition
- **Settlement**: **$10,000**
- **Why:** Lack of Policy & Procedure, as well as Notice of Privacy Practices.

"Social media is not the place for providers to discuss a patient's care," said OCR Director, Roger Severino. "Doctors and dentists ***must think carefully about patient privacy*** *before responding to online reviews."*

https://www.hhs.gov/about/news/2018/12/04/florida-contractor-physicians-group-shares-protected-health-information-unknown-vendor-without.html

What About Your Staff?

- **Who**: Jackson Health System
- **What**:
  - 2013 - Lost three boxes of paper records containing PHI
  - 2015 - PHI of a patient was disclosed without authorization (NFL player)
  - 2015 - Pictures of an operating room display board was posted on social media
  - 2016 - Employee had been accessing and selling patient PHI
- **Settlement**: **$2,150,000**
- **Why**: Breach Notification, Risk Analysis, Minimum Necessary Standard.

*"OCR's investigation revealed a HIPAA compliance program that had been in **disarray for a number of years**," said OCR Director Roger Severino.*

https://www.hhs.gov/about/news/2019/10/23/ocr-imposes-a-2.15-million-civil-money-penalty-against-jhs-for-hipaa-violations.html

Encrypt, Encrypt, & Encrypt!

- **Who**: University of Rochester Medical Center
- **What**: Two breaches:
  - 2013 – Lost unencrypted flash drive
  - 2017 – Theft of unencrypted laptop
- **Settlement**: **$3,000,000**
- **Why**: Risk Analysis, Remediation, Device Controls.

"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****."*

https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html

Keep Your Head in the Game!

- **Who**: Texas Health and Human Services Commission
- **What**: An internal application was moved from a private server to a public one.
- **Settlement**: **$1,600,000**
- **Why**: Missing Risk Analysis, Access Controls

*"Covered entities need to know who can access protected health information in their custody **at all times**," said OCR Director Roger Severino. "No one should have to worry about their private health information being discoverable through a Google search."*

https://www.hhs.gov/about/news/2019/11/07/ocr-imposes-a-1.6-million-dollar-civil-money-penalty-against-tx-hhsc-for-hipaa-violations.html

Oops, Don't Do That Again!

- **Who**: Sentara Hospital
- **What**: Sent billing statements with PHI to the wrong individuals and failed to properly notify HHS, because they said it was not PHI.
- **Settlement**: **$2,175,000 – Thanksgiving Day!**
- **Why**: Refusal to Report Breach Properly, Missing BAA with Parent Company

*"HIPAA compliance depends on **accurate and timely self-reporting** of breaches because patients and the public have a right to know when sensitive information has been exposed." said Roger Severino, OCR Director.*

https://www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html?language=es

18 HIPAA Identifiers

The Department of Health and Human Services (HHS) lists the 18 HIPAA identifiers as follows:

1. Patient names
2. Geographical elements (such as a street address, city, county, or zip code)
3. Dates related to the health or identity of individuals (including birthdates, date of admission, date of discharge, date of death, or exact age of a patient older than 89)
4. Telephone 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
13. Device attributes or serial numbers
14. Digital identifiers, such as website URLs
15. IP addresses
16. Biometric elements, including finger, retinal, and voiceprints
17. Full face photographic images
18. Other identifying numbers or codes

HIPAA is the Law!

- **Who**: Korunda Medical
- **What**: Failed to forward a patient's medical records in electronic format and charged more than the reasonably cost-based fees under HIPAA
- **Settlement**: **$85,000**
- **Why:** Previously Investigated, Continued to Violate HIPAA Right of Access Rule.

"For too long, healthcare providers have slow-walked their duty to provide patients their medical records out of a sleepy bureaucratic inertia." said Roger Severino, OCR Director.

https://www.hhs.gov/about/news/2019/12/12/ocr-settles-second-case-in-hipaa-right-of-access-initiative.html

Noncompliance is More Expensive than Compliance!

- **Who**: West Georgia Ambulance, Inc.
- **What**: Loss of unencrypted laptop containing PHI uncovered long-standing noncompliance (failing to conduct a SRA, training, policies and procedures, etc.)
- **Settlement**: **$65,000**
- **Why:** No Risk Analysis, Staff Training, or Policies & Procedures.

*"**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**," said OCR Director Roger Severino. "All providers, large and small, need to take their HIPAA obligations seriously."*

https://www.hhs.gov/about/news/2019/12/30/ambulance-company-pays-65000-settle-allegations-longstanding-hipaa-noncompliance.html

Prior Fines

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
	Native American Rehabilitation Association of the Northwest, Inc.	OR	Healthcare Provider	25187	01/03/2020	Hacking/IT Incident	Email
	Douglas County Hospital dba Alomere Health	MN	Healthcare Provider	49351	01/03/2020	Hacking/IT Incident	Email
	The Center for Facial Restoration, Inc.	FL	Healthcare Provider	3600	12/26/2019	Hacking/IT Incident	Network Server
	Ann & Robert H. Lurie Children's Hospital of Chicago	IL	Healthcare Provider	4196	12/26/2019	Unauthorized Access/Disclosure	Electronic Medical Record
	btyDENTAL	AK	Healthcare Provider	2008	12/26/2019	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Email, Network Server

- **Missing BAA - $31,000**
  - Small pediatric practice caused by BA, failure to have policy and procedures
- **Late breach notification - $475,000**
  - Did not notify OCR/patients within (60) days, – failure to have policy and procedures
- **Ineffective Compliance Program - $150,000**
  - Alaska Nonprofit org – failure to have updated policy and procedures
- **Malware - $750,000**
  - Incomplete Risk Assessments, failure to have policies/procedures
- **Unencrypted devices- $2,700,000**
  - SIX risk analysis – failure to have updated policy and procedures
- **Patient testimonials – $25,000**
  - Physical Therapy – posted testimonials on website w/out permission, failure to have updated policy and procedures
- **Press Release - $2,400,000**
  - Publish Press release including PHI w/out authorization, failure to have policy and procedures

Reference: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Questions?

Compliancy Group

Liam Degnan
855-854-4722 ext. 530
liam@compliancygroup.com
www.CompliancyGroup.com

FREE Compliance Checklist

https://compliancy-group.com/simple-hipaa-compliance-checklist/