

Hackers, HIPAA, and Headaches

Security & HIPAA Compliance



Travis Watson



Travis is from Florida and attended Randolph College. After college, he joined the Marines. He then found his way into the medical and dental industry after completing his service. Travis loves educating practices on compliance and helping them protect their organization and patients.

WHO WE ARE



Technology Company



HIPAA Experts



**Compliance Education &
Solutions for
Independent Practices**

Dennis Krohn Jr.



Dennis has had an entrepreneurial spirit from a young age: he started working on computers with his father when he was 14 years old, and started his first company when he was 18. He's had 25 years in general IT, and 20+ years of Dental specific IT experience. Dennis loves the ever changing landscaping of the technology and creating new ways of providing innovative, safe, and accessible for clients.

SD Reliance



sd reliance

SD Reliance is a Managed Service Provider (MSP) & Outsourced Dental Billing company that has worked in the dental space for over 10 years.

TODAY'S AGENDA



MATCH MADE IN HIPAA HEAVEN

A brief history on Cybersecurity & Compliance



DATA BREACHES

What constitutes a data breach and what the common breaches you need to be aware of



PATH TO COMPLIANCE & SECURITY

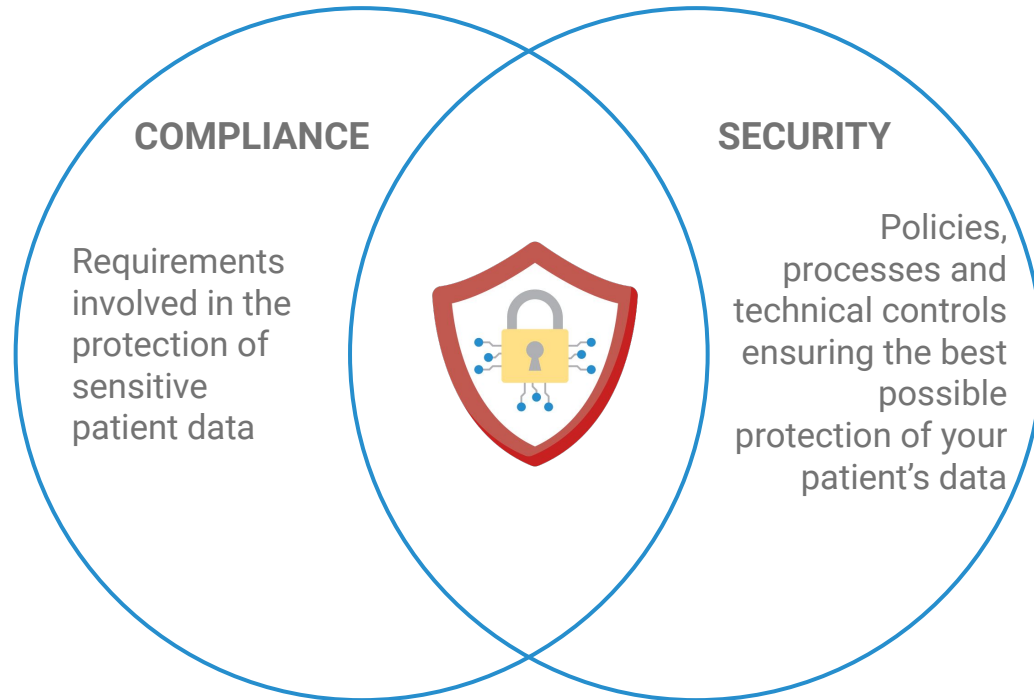
Do it right the first time by documenting and implementing what you need



LEARNING FROM OTHERS MISTAKES

Real-world stories and current events so you can learn what no to do

MATCH MADE **IN HEAVEN**



WHAT IS **HIPAA**?

What does **H-I-P-A-A**
stand for?

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT

AUGUST
1996



HIPAA officially signed into Law

MARCH
2013



OCR commits to HIPAA enforcement

2016



Proactive audit enforcement starts

2018



State Attorneys General start fining for HIPAA violations

JANUARY
2021



Amendment to HITECH Act, Safe Harbor Law

May
2023



Telehealth waivers expired

WHO ENFORCES THIS LAW?



U.S. Department of
Health and Human Services

Enhancing the health and well-being of all Americans



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

CMS.gov

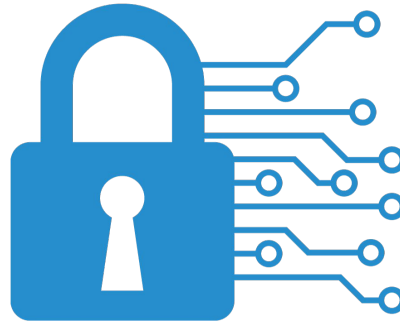


OCR DIVISIONS



WHAT IS
CYBERSECURITY?

CYBERSECURITY



- **Cybersecurity involves the practice of protecting systems, networks, and data from digital threats, ensuring the confidentiality, integrity, and availability of sensitive information.**
- **In the context of dentistry, it plays a crucial role in safeguarding patient records and maintaining the trust and privacy of individuals.**

BRIEF HISTORY OF CYBERSECURITY

2012



Rise of IoT (Internet of Things) devices introduces new vulnerabilities.

2014



CryptoLocker ransomware infects computers globally, demanding bitcoin payments

2016



Rise of machine learning and AI for advanced threat detection.

2018



European Union introduces GDPR (General Data Protection Regulation) for data protection and privacy.

2020



The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is established.

2020-2023



Increased emphasis on cybersecurity education and training to empower individuals and organizations against evolving threats.

YEAR IN REVIEW | HIPAA



**Increased Cyber
Attacks**



**Patient Right of
Access Initiative**



**Introduction of
New Legislation**



**HIPAA & Telehealth
Waivers Expired**



**OCR Enforcement
Efforts & New
Director**

WHISTLEBLOWER PROTECTION ACT



Protects employees from retaliation who report violations of various workplace safety and health laws



Offers monetary rewards for info that leads to violation discovery



Provides protection to patients - they will be watching!

HIPAA SAFE HARBOR LAW

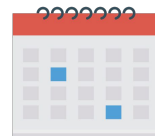
Reduced Penalties for Compliance



Encourages entities to meet basic security measures as cybersecurity threats rise



Requires compliance with HIPAA Security Rule AND appropriate technical safeguards



Must be compliant for 12 months prior to a breach to qualify



Reduces fines, audit intensity and Corrective Action Plan measures

HIPAA INVESTIGATION

TRIGGERS

Complaint | Breach | Proactive Audit

WHAT IS A
DATA BREACH?

DEFINING A BREACH

A breach is, generally, an impermissible use or disclosure of information that compromises the security or confidentiality of the information and jeopardizes the privacy or health of the individual.

A breach occurs when private health information is mishandled, endangering its security and privacy. This is considered a breach unless the organization can demonstrate a very low probability of the information being at risk.

2.

3. Whether

4. The extent to which

MOST COMMON BREACHES

| Year | Issue 1 | Issue 2 | Issue 3 | Issue 4 | Issue 5 |
|-------------|----------------------------------|----------------|---------------------------|---------------------------|-------------------------------|
| 2021 | Impermissible Uses & Disclosures | Access | Safeguards | Administrative Safeguards | Breach - Notice to Individual |
| 2020 | Impermissible Uses & Disclosures | Safeguards | Access | Administrative Safeguards | Technical Safeguards |
| 2019 | Impermissible Uses & Disclosures | Safeguards | Access | Administrative Safeguards | Minimum Necessary |
| 2018 | Impermissible Uses & Disclosures | Safeguards | Administrative Safeguards | Access | Technical Safeguards |

TIMEFRAME TO **REPORT**

Federal Time Frame for Individual Notice
and Submitting to OCR for
breach over 500 Patients

60 Days

California Time Frame for Individual Notice
and Submitting to Attorney General

10 Days

TYPES OF BREACHES



Hacking/IT
Incident



Improper
Disposal



Loss



Theft



Unauthorized
Access/
Disclosure

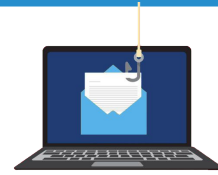


Other

COMMON TYPES OF CYBER THREATS



Malware



Phishing



Social Engineering



Ransomware

RANSOMWARE



- Ransomware is like a **digital hostage situation** for your computer.
- Imagine someone sneaking into your computer and putting **all your files into a locked, secret box**.
- They won't give you the key **unless you pay them money**, usually in a form of digital currency like Bitcoin.
- Until you pay up, **you can't access your important documents**, photos, or anything else on your computer.

SIMPLE STRATEGIES FOR PHISHING EMAILS

- **S**ender: Check the sender's email address
- **L**inks: Hover and check any links before clicking
- **A**ttachments: Don't open attachments from someone you don't know or attachments that you weren't expecting
- **M**essage: Check the content of the message and keep an eye out for bad grammar or misspellings



HIPAA PENALTIES & COST OF CYBER EVENT

“OCR is sending a clear message to regulated entities that they must appropriately *safeguard patients’ protected health information*. We take complaints about potential HIPAA violations seriously, **no matter how large or small the organization.**”

OCR Director, Melanie Fontes Rainer

HIPAA PENALTIES

Monetary

Tier 1 - Compliant

Violation could not have been reasonably avoided.

Max:
\$59,500
per violation

Tier 2 - Compliant

Violation should have been corrected.

Max:
\$59,500
per violation

Tier 3 - Not Compliant

Made attempt to correct violation.

Max:
\$59,500
per violation

Tier 4 - Not Compliant

No attempt made to correct violation.

Max:
\$1,785,000
per violation

HIPAA PENALTIES

Criminal

Tier 1 - 1 Year Max Jail Time

Reasonable cause or no
knowledge of violation

Tier 2 - 5 Years Max Jail Time

Obtaining PHI under
false pretenses

Tier 3 - 10 Years Max Jail Time

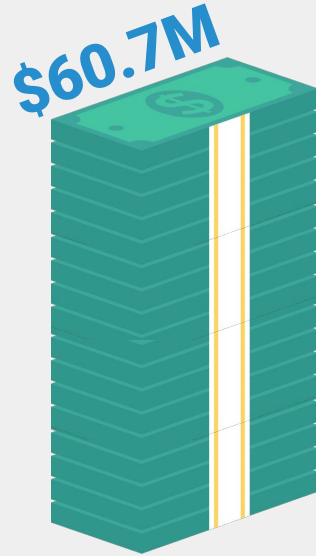
Obtaining PHI for
personal gain or with
malicious intent



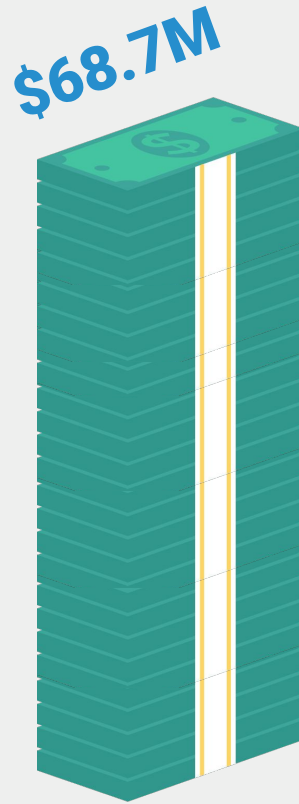
HIPAA FINES SO FAR



2008-2012



2013-2017



2018-2023

\$143,887,440
TO DATE

**From most up to date HHS data*

RANSOMWARE ATTACKS

Key Trend

- Downtime-related losses of **77 billion**.
- Since 2016, there has been **539** ransomware attacks targeting **9,780** healthcare facilities.
- Potentially, more than **52 million** patient records have been compromised due to ransomware attacks.

Healthcare ransomware attacks cost US economy **\$77B**

Naomi Diaz - Thursday, October 26th, 2023



Ransomware attacks on healthcare have resulted in downtime-related losses of more than \$77 billion for the U.S. economy, according to an Oct. 23 report from cybersecurity firm Comparitech. According to the report, since 2016, there have been 539 ransomware incidents targeting healthcare institutions in the U.S., affecting 9,780 healthcare facilities and potentially compromising more than 52 million patient records.

On average, ransomware attacks resulted in 14 days of downtime, but in certain instances, the damage took several months to fully restore. Hackers sought more than \$39 million in 34 attacks, with 31 out of 160 medical organizations confirming payment of the ransom. According to the report, medical organizations are more inclined to reveal when they have not paid the ransom compared to when they have.

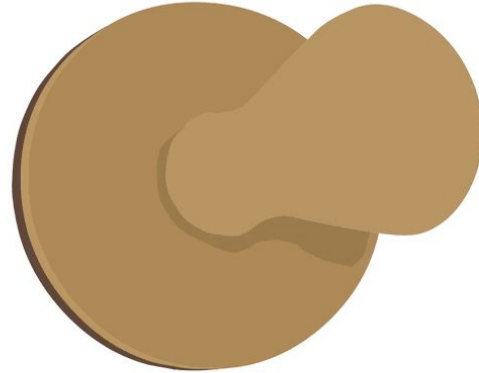
Strengthening your

Cyber Posture

- *Security Awareness Training*
- *Changing Passwords on a regular basis*
- *Working with a MSP (Dental Specific)*
- *Hardware Firewall*
- *Disaster Recovery Plan (Backups)*

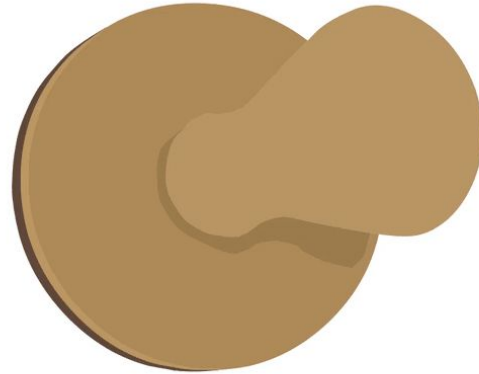
MYTHBUSTERS

Antivirus is enough to protect my practice from being compromised.



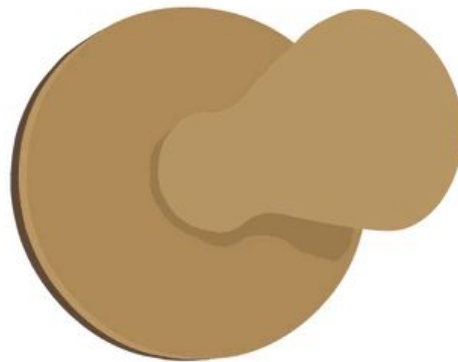
MYTHBUSTERS

We've never had a breach so
we must be secure!



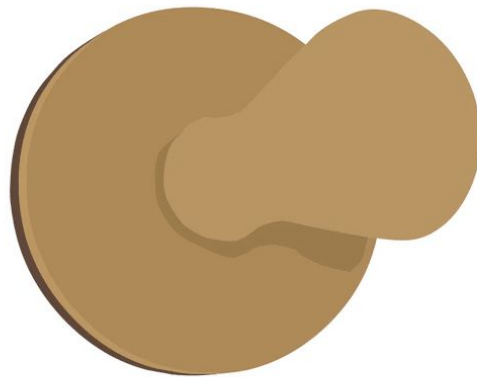
MYTH **BUSTERS**

Human error accounts for most data breaches.



MYTHBUSTERS

"I'm too small to be a target; hackers only go after big companies."



THE PATH TO
COMPLIANCE



DEFINITION OF **COMPLIANCE**

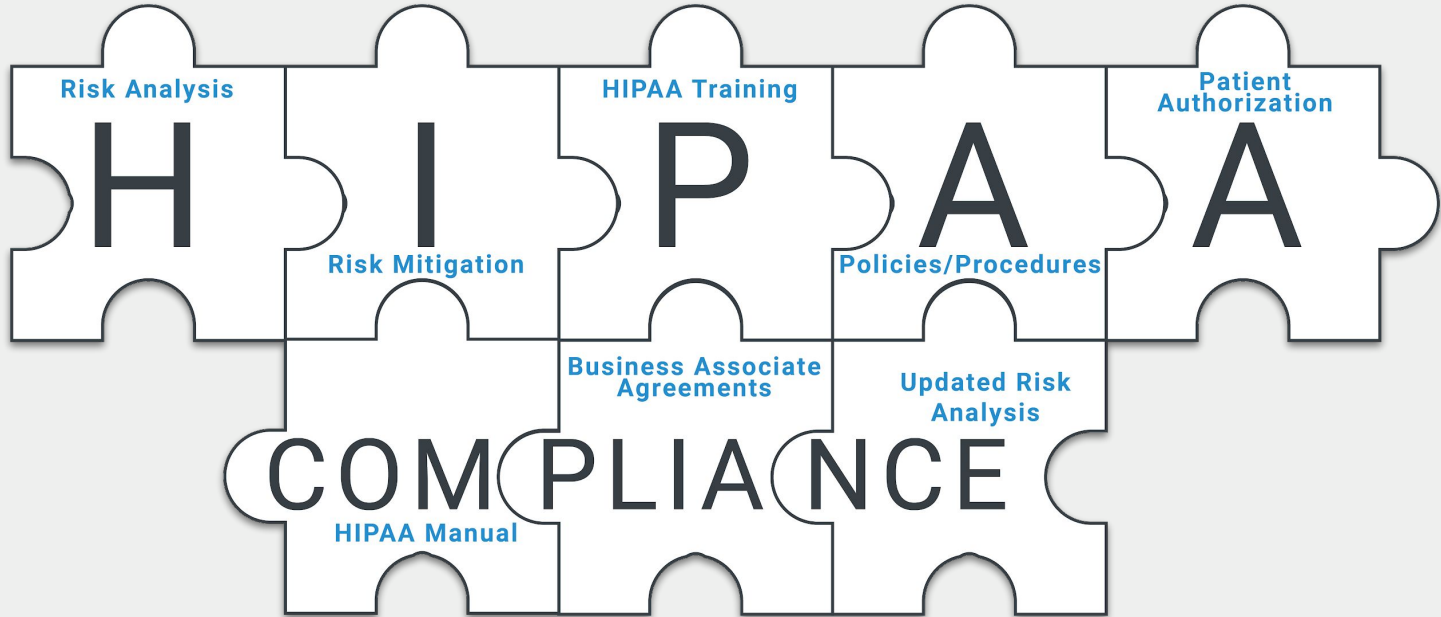
DOCUMENTED proof that there is a
culture of compliance
within your organization.

HOW **MOST PROVIDERS VIEW HIPAA**

H I P A A

C O M P L I A N C E

HOW THE OCR VIEWS HIPAA



SECURITY RISK ANALYSIS



Physical | Technical | Administrative

- Responsibility of the practice
- First step in HIPAA Compliance
- Auditors will ask for Risk Analysis **FIRST**
- Compliance has not been achieved without a **documented** Risk Analysis

The Risk Analysis is a prerequisite for Quality Payment Program (MIPS) incentives.

SECURITY RISK ANALYSIS

(FROM AN IT PERSPECTIVE)

Limited IT Understanding

- Difficulty in conveying IT security importance due to staff's limited understanding IT concepts.

Budget Constraints

- Smaller practices face financial challenges in investing in comprehensive cybersecurity.

Resistance to Change

- Staff reluctance in adapting to new technologies and workflow adjustments.

Compliance Complexity

- Navigating HIPAA and other regulations adds to the intricacy of implementing security measures.



SECURITY RISK ANALYSIS

(FROM AN IT PERSPECTIVE)

Staff Training Challenges

- Time-intensive training and routine disruption lead to resistance in adopting security protocols.

Legacy Systems Limitations

- Difficulty integrating modern cybersecurity solutions with outdated systems and software.

Sensitive Data Handling

- Ensuring adherence to protocols for managing patient information poses continuous challenges.

Emergency Preparedness

- Resistance to establishing and practicing incident response plans due to perceived low risk.



SRA MISCONCEPTIONS

The SRA is a one-time thing that you only need to complete once.

My EHR takes care of privacy and security, so I don't need to do an SRA.

My IT company handles a full SRA.



I'm a small practice so I don't need to conduct an SRA.

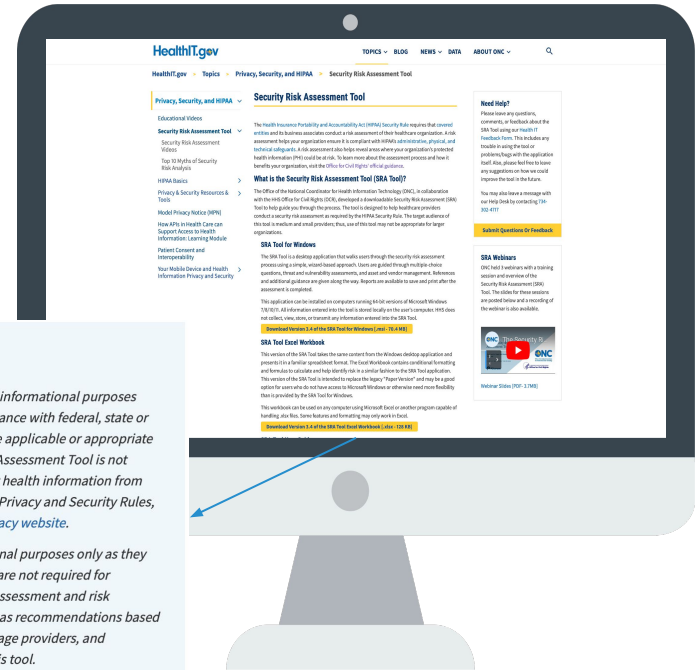
I can use a simple templated checklist to complete my SRA.

“Neglecting to have a comprehensive, enterprise-wide risk analysis, is a recipe for failure.”

- OCR Director

OUTSOURCING

- An outside resource such as your IT provider can be valuable for HIPAA compliance.
- It's essential for dentists to choose reputable and experienced professionals in healthcare compliance to ensure the security and privacy of patient information.
- An outside source can ensure you are staying compliant instead of trying to reinvent the wheel.

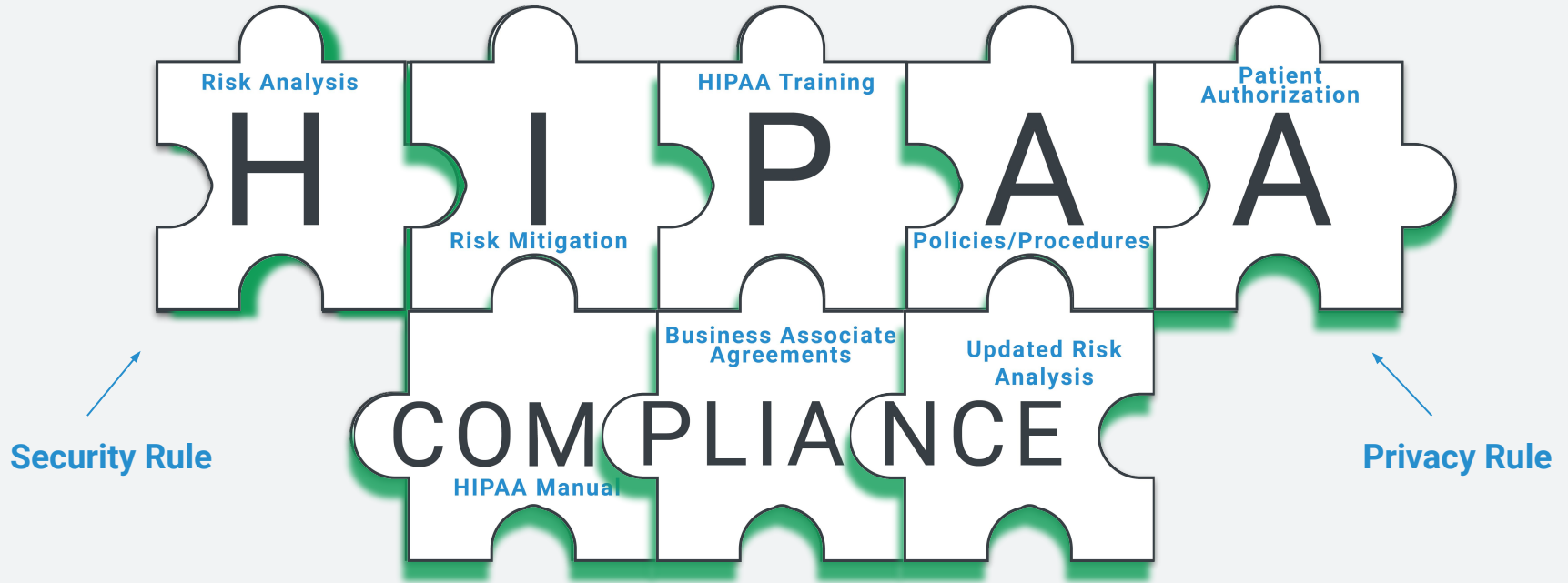


Disclaimer

The Security Risk Assessment Tool at HealthIT.gov is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights Health Information Privacy website.

NOTE: The NIST Standards provided in this tool are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers, and professionals to seek expert advice when evaluating the use of this tool.

TWO PHASES TO COMPLIANCE



ONGOING COMPLIANCE | PRIVACY RULE



Risk Mitigation

Reduce vulnerabilities found in the Risk Analysis

HIPAA Training

Staff must be trained at minimum once per year
(Quiz recommended)



Policies & Procedures

ALL must be documented for the practice

Patient Authorization & Consent Forms

All patients must sign *before* being treated



ONGOING COMPLIANCE | PRIVACY RULE



HIPAA Manual

Documentation related to HIPAA must be easily accessible

Business Associate Agreements

All Business Associates must sign BAAs to offset liability in case of breach



Updated Risk Analysis

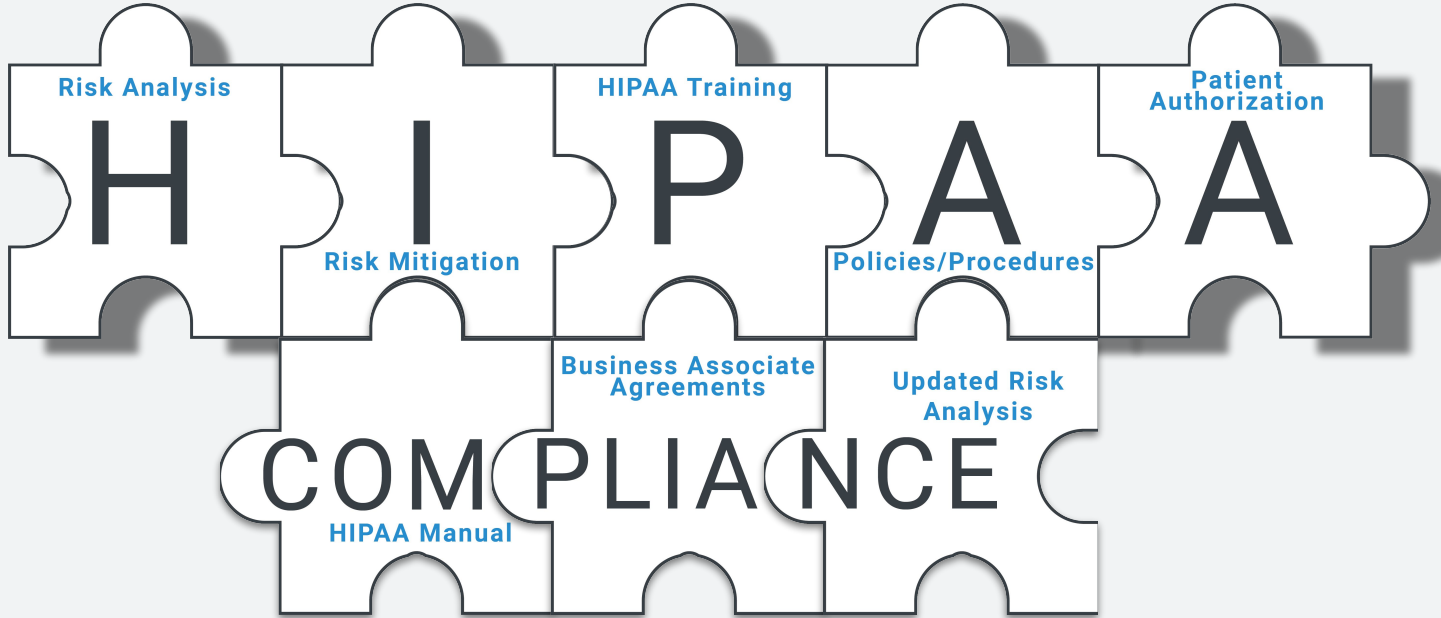
The RA must be updated and contain an accurate portrayal of past, present and future compliance programs

BUSINESS ASSOCIATE AGREEMENTS



- HIPAA requires you to have a BAA with everyone you are sharing your patients PHI with.
- Helps to ensure the companies you are working with will protect your patients data.






CULTURE OF COMPLIANCE



COMMON MISCONCEPTIONS



“We’re HIPAA Compliant Because...”

-  Our PM/EHR Product is HIPAA Compliant
-  We don’t discuss patients in front of others
-  We get patients to sign authorization forms
-  Our IT company makes us compliant
-  We’re too small or it’s never happened to me

STORY TIME

Learning from other's mistakes

HENRY SCHEIN DATA BREACH

Key Trend

- Ransomware attacked twice in **two months**
- The BlackCat Ransomware gang stole **35 terabytes** of sensitive data
- Failed negotiations led to a second attack
- FBI links BlackCat to **60+ global breaches** (Nov 2021 - Mar 2022)

BlackCat Ransomware Group Re-encrypts Henry Schein Data

Posted By Steve Alder on Nov 27, 2023

The BlackCat ransomware group conducted a ransomware attack on the Fortune 500 firm Henry Schein and claimed to have stolen 35 TB of sensitive data. The healthcare giant was engaged in ongoing discussions with the group but negotiations had stalled. According to a spokesperson for the BlackCat group, "We have not received any indication of their willingness to prioritize the security of their clients, partners, and employees, let alone protect their own network." Just as Henry Schein was about to finish restoring its systems, the BlackCat hackers struck again and re-encrypted its data.

Henry Schein confirmed in an October 15, 2023, announcement that it had been forced to take some of its systems offline to contain a cyberattack that had affected its manufacturing and distribution businesses. According to the announcement, the attack occurred the previous day. The company had been working around the clock to resolve the situation and bring its systems online, and as its investigation progressed it became clear that the ransomware group had gained access to sensitive customer and supplier information. That information included personal information, bank account information, and payment card numbers. Around two weeks after Henry Schein announced the attack, the BlackCat ransomware group claimed responsibility and added Henry Schein to its data leak site.

Henry Schein has now confirmed that the second attack resulted in applications such as its e-commerce platform being made unavailable; however, Henry Schein anticipated a quick recovery from the attack and only expected it to cause short-term disruption. Following the attack, the BlackCat group threatened to publish internal payroll data on its data leak site within a few hours if Henry Schein refused to negotiate, and claimed additional data would be released on a daily basis thereafter. Instead of posting data, BlackCat removed the listing. That could mean Henry Schein has started negotiating again or that ransom payment has been made. Entries on the data leak sites of ransomware groups are removed if a ransom has been paid.

KEY TAKEAWAYS

1

If a company as big as Henry Schein, who could dedicate a large amount of resources to cyber security could be compromised, then any small/medium size businesses is at risk too!

2

This highlights the significant impact of cyber attacks on organizations, particularly in the healthcare sector, where the compromise of sensitive data poses serious privacy and security concerns.

NO ORGANIZATION TOO BIG

ASPEN DENTAL

- Scheduling and phone systems down
- Cannot accept new patients
- No comment on ransomware attack
- No comment on patient information being compromised

The screenshot shows a press release from Aspen Dental. The header includes the AspenDental logo and navigation links for 'CONTACT / SUBSCRIBE / SEARCH', 'DENTAL PROFESSIONALS', 'PATIENTS', and 'MED'. A 'Press Release' tag is visible. The main title is 'Updated Cybersecurity Incident Statement'. Below the title are social media sharing icons and a 'SHARE ON:' label with icons for Facebook, Twitter, LinkedIn, and Pinterest. The body of the text is as follows:

TAG - The Aspen Group experienced a cybersecurity incident that temporarily impacted our ability to access scheduling systems, phone systems and other business applications for Aspen Dental.

Thanks to our IT team, the issue was discovered early, and we have been working diligently to bring systems back online as quickly and as safely as possible. Our offices are open and we are seeing patients. We are still working to resolve all the issues related to the incident, but we are open and seeing patients largely as normal.

Our investigation into the incident is in its early stages and is still ongoing. We remain focused on remediating this incident, and will provide our employees, patients, and partners with updates directly as we have further information to share.

When will your systems be restored?

While we are not able to share a specific timetable as to when everything will be 100 percent back to normal, our offices are open, and we are continuing to care for our patients as we did pre-cyber incident.

Was this a ransomware attack or some other type of hack?

The investigation is ongoing and confidential in nature, and we do not have additional details to share at this time.

Was patient information compromised?

Our investigation into the scope of the incident is in its early stages and remains ongoing. If it is determined that any sensitive, personal information may have been involved in the incident, we will notify those individuals in accordance with applicable law and as quickly as possible.

NO PRACTICE TOO SMALL

FBI and Secret Service Involvement

- Server being held at ransom
- All patient information compromised
- Not able to access any patient information



CYBERSECURITY

Key trend

- **Record breaches** from both covered entities and business associates
- Ongoing enforcement related to **lack of HIPAA documentation** when a breach occurs
- **\$200,000 fine** for **not terminating a former employee's access** and she maliciously stole data as a result



KEY TAKEAWAYS

1

Have basic technical safeguards in place

2

Understand which employees have remote access to PHI

3

Have policies in place to properly offboard employees

BUSINESS ASSOCIATE AGREEMENTS

Key trend

- State Attorney's across the country levied a \$1.4 million fine toward business associate, software company Inmediata
- Protected Health Information of 1.5 million exposed. 10,000 Coloradans
- Vendors must have the same safeguards in place to protect PHI as a Cover Entity and now must undergo 5 years of 3rd party assessments



KEY TAKEAWAYS

1 *Get BAA's signed BEFORE an incident & before working with BA*

2 *Ensure vendors are using the proper safeguards for PHI*

“It won’t happen to me.”

- Small businesses are at higher risk than large businesses
- 82% of ransomware attacks were targeted at companies with less than 1000 employees
- 47% of businesses that have less than 50 employees don’t allocate any funds towards cybersecurity

FEDERAL & STATE

AUDIT LETTERS

STATE AUDIT LETTER



OFFICE OF THE ATTORNEY GENERAL

ATTORNEY GENERAL

TELEPHONE: [REDACTED]
FAX: [REDACTED]

April 30, 2020

RE: [REDACTED] | Request for Additional Information

This communication is to ensure that your company is and has been in compliance with the applicable HIPAA regulations and [REDACTED] statutes. To ensure compliance with HIPAA, please provide:

1. A description of the Protected Health Information disclosed.
2. Whether [REDACTED] is a Covered Entity or Business Associate, as defined by 45 C.F.R. § 160.103.
3. The identification of any other Covered Entities or Business Associates that are related to the disclosure, and the Business Associate Contract(s) with those parties.
4. If [REDACTED] is a Covered Entity, provide the privacy policies and procedures, as required by 45 C.F.R. § 164.530(i). Also, provide the privacy practice notice, as required by 45 C.F.R. §§ 164.520(a) and (b).
5. The security policies and procedures, as required by 45 C.F.R. § 164.316(a).
6. The administrative safeguard policies and procedures, as required by 45 C.F.R. § 164.308(a)(1)(i).
7. The technical safeguard policies and procedures, as required by 45 C.F.R. § 164.312(a)(1).
8. The physical safeguard policies and procedures, as required by 45 C.F.R. § 164.310(a)(1).
9. The sanction policies and procedures, as required by 45 C.F.R. § 164.308(a)(1)(ii)(C).
10. The risk analysis conducted immediately before the disclosure, as required by 45 C.F.R. § 164.308(a)(1)(ii)(A).

[REDACTED] for notifying the Office of Attorney General concerning the HIPAA related disclosure your company, [REDACTED]. Separate from any potential HIPAA requirements, [REDACTED] law requires database owners to disclose a security breach toidents whose personal information was acquired by an unauthorized person if the could result in identity theft or fraud against the [REDACTED] resident. The required must occur "without unreasonable delay" ([REDACTED] Code § 24-4-9-1-1 *et seq.*).

ication is to ensure that your company is and has been in compliance with the HIPAA regulations and [REDACTED] statutes. To ensure compliance with HIPAA, please

scription of the Protected Health Information disclosed. [REDACTED] other [REDACTED] is a Covered Entity or Business Associate, as defined 5 C.F.R. § 160.103. identification of any other Covered Entities or Business Associates that are related to disclosure, and the Business Associate Contract(s) with those parties.

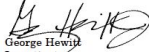
[REDACTED] is a Covered Entity, provide the privacy policies and edures, as required by 45 C.F.R. § 164.530(i). Also, provide the privacy practice ce, as required by 45 C.F.R. §§ 164.520(a) and (b). security policies and procedures, as required by 45 C.F.R. § 164.316(a). administrative safeguard policies and procedures, as required by 45 C.F.R. § 308(a)(1)(i). technical safeguard policies and procedures, as required by 45 C.F.R. § 164.312(a)(1). physical safeguard policies and procedures, as required by 45 C.F.R. § 164.310(a)(1). sanction policies and procedures, as required by 45 C.F.R. § 164.308(a)(1)(ii)(C). risk analysis conducted immediately before the disclosure, as required by 45 C.F.R. § 308(a)(1)(ii)(A).

above that seek protected health information are allowed under 45 C.F.R. § (ii)(C), because they are contained within this administrative request or within a gative demand which will be issued to [REDACTED] upon request. In e requests above 1) seek information that is relevant and material to the Office of eneral's legitimate enforcement inquiry of this matter; 2) are specific and limited in extent reasonably practicable in light of the purpose for which the information is

3) de-identified health information could not reasonably be used for the purposes ation is being requested.

ide the above information above no later than May 20, 2020. Please respond by the policies attached as PDFs. No hard copy is necessary and will only delay the you have any questions, please contact me by email at [REDACTED]@dcg. With ication, please reference File No. [REDACTED]

Sincerely,


George Hewitt
Investigator
Data Privacy and Identity Theft Unit



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

Southwest Region • 1301 Young Street
Suite 106 • Dallas, TX 75202
Voice - (800) 368-1019 • TDD - (214) 767-8940
Fax - (214) 767-0432 • <http://www.hhs.gov/ocr>

ATTN: Mr. [REDACTED]

JAN 31 2020

Re: [REDACTED]

OCR Transaction Number: [REDACTED]

Dear Mr. [REDACTED]

On [REDACTED] 2018, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) received a breach notification report (the report), as required by 45 C.F.R. § 164.406 (the Covered Entity). Per the report, the Covered Entity reported that it might not be in compliance with the Federal Standards for Privacy and Security of Protected Health Information and/or the Security Standards for the Protection of Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, D, and E) (the Security and Breach Notification Rules).

Specifically, the report indicated that on [REDACTED] 2018, the Covered Entity's unencrypted laptop containing the electronic protected health information of [REDACTED] individuals, was stolen from the facility. The ePHI included patients' names and medical diagnoses.

OCR enforces federal civil rights laws which prohibit discrimination in the delivery of human services based on race, color, national origin, disability, age, sex, religion, or ancestry of conscience, and also enforces the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules.

On [REDACTED] 2018, the Covered Entity reported and provided evidence of corrective actions. Specifically, the Covered Entity provided evidence it reported the breach to local law enforcement, installed a multi-camera security system, and encrypted workstations.

Regarding the Breach Notification Rule, the Covered Entity reported that it sent notice to the affected individuals on [REDACTED] 2018. The Covered Entity provided evidence that for individuals whom Covered Entity could not reach, it placed notice on the facility's website which remained for 90 days. The Breach Notification Rule also requires a covered entity to notify prominent media outlets of a breach involving more than 500 individuals in a community. See 45 C.F.R. § 164.406. The Covered Entity reported that, on [REDACTED] 2018, [REDACTED]. Additionally, on [REDACTED] 2018, an article was published online by [REDACTED].

OCR AUDIT LETTER

Based upon the information and evidence described above, we have determined that no further OCR action is required; we are closing our investigation as of the date of this letter. OCR's determination as stated in this letter applies only to the issues that were identified in this breach and which were investigated by OCR.

If you have any questions, please do not hesitate to contact Leon Loggins, OCR Investigator, at [REDACTED]. Thank you for your cooperation in this matter.

Sincerely,

Marisa M. Smith, Ph.D.
Regional Manager

QUESTIONS TO **CONSIDER**

1 What methods do you use to protect our Data and environment?

2 How are data backups and disaster recovery handled?

3 Do you offer Security Awareness Training?

4 What is your response time for critical issues?