Suze Shaffer, CHSP

Suze is a Certified HIPAA Security Professional and the president of Aris Medical Solutions since 2009.

She has been a public speaker at numerous conferences and functions to educate organizations on what it means to be HIPAA compliant.

ARIS
MEDICAL SOLUTIONS

Who are we?
What do we do?

We make HIPAA easy!

We know that Practice Administrators and Office Managers have many responsibilities, and HIPAA is one that is often **DREADED!**

Our online HIPAA *Keeper*™ saves you time and money so you can perform your **MAIN** responsibilities, while we take care of HIPAA!

ARIS MEDICAL SOLUTIONS

Have you heard about…

- Notice of Privacy Practices updates
- Updated privacy policy requirements
- Notice of Non-Discrimination in 15 languages
- Disability and language assistance requirements
- Updated staff training requirements
- Website / App / Kiosk accessibility requirements
- Results from the 2024 Data Breach report

ARIS MEDICAL SOLUTIONS

Poll

Gauging the information on the previous slide, how much would you estimate you know about the New HIPAA requirements?

1. 100%
2. 75%
3. 50%
4. 25%
5. Under 25%

ARIS
MEDICAL SOLUTIONS
"Simplifying HIPAA"

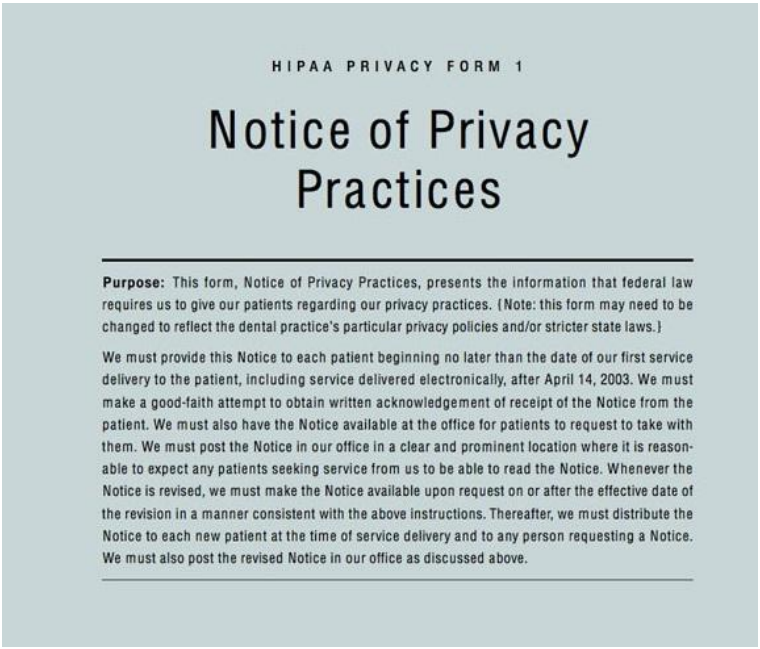
New Rules for ***HIPAA 2025*** *and beyond!*

Poll

To keep this relevant and interesting I would like to ask…
What are you most interested in learning about?

1. Notice of Privacy Practices and Privacy Policy updates
2. Non-Discrimination notices and Disability Assistance Requirements
3. New training requirements
4. What are the website / app / kiosk accessibility requirements
5. Results from the 2024 Data Breach report

Notice of Privacy Practices



HIPAA PRIVACY FORM 1

Notice of Privacy Practices

Purpose: This form, Notice of Privacy Practices, presents the information that federal law requires us to give our patients regarding our privacy practices. {Note: this form may need to be changed to reflect the dental practice's particular privacy policies and/or stricter state laws.}

We must provide this Notice to each patient beginning no later than the date of our first service delivery to the patient, including service delivered electronically, after April 14, 2003. We must make a good-faith attempt to obtain written acknowledgement of receipt of the Notice from the patient. We must also have the Notice available at the office for patients to request to take with them. We must post the Notice in our office in a clear and prominent location where it is reasonable to expect any patients seeking service from us to be able to read the Notice. Whenever the Notice is revised, we must make the Notice available upon request on or after the effective date of the revision in a manner consistent with the above instructions. Thereafter, we must distribute the Notice to each new patient at the time of service delivery and to any person requesting a Notice. We must also post the revised Notice in our office as discussed above.

Patients have the right to receive a copy of how you collect, share, and protect their information. This is called the Notice of Privacy Practices (NPP).

There have been updates over the years, and the latest is the requirement of specific language and examples.

ARIS MEDICAL SOLUTIONS

What must be included?

The explanation of HIEs (Health Information Exchanges), adding reproductive health care to sensitive information, and an example of how this information will be protected.

The changes instruct providers to update their NPPs to support both the Reproductive Health Care Privacy final rule and the Substance Abuse and Mental Health Services Administration (SAMHSA) updates.

Privacy Policy Updates

- **Patient right of access** you should make every attempt to obtain this request in writing, but you cannot create a hardship for them.
- **Patient Authorizations** your staff will need to be educated on the new requirements when PHI is requested from third parties.
- **Attestation forms,** healthcare providers and BA's must obtain a signed attestation form.

Patient Requests

Patients may request their information in the format of their choice.

This includes third party electronic vendors and even mobile apps.

In previous years, a practice could deny this request if they did not have the requested method.

Proposed Changes

- Reducing a patients' right of access to 15 days.
- Post estimated fee schedules on their websites for PHI access and disclosures.
- Patient recording visits.
- Permitting the patient to take photos of their records.
- More specific risk analyses, policies, procedures, vulnerability scanning, network segmentation, annual reviews, and a lot more!

ARIS MEDICAL SOLUTIONS

Cyber Security Updates

- **Stronger Cybersecurity Requirements** - enhanced administrative, physical, and technical safeguards.
- **Risk Assessments** – more frequent and thorough.
- **Updated Technology** – replace legacy systems, stronger encryption, and implementing multi-factor authentication.

ARIS MEDICAL SOLUTIONS

The HIPAA Security Rule

Security Standards Matrix (Appendix A of the Security Rule)

ADMINISTRATIVE SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Security Management Process	§ 164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	§ 164.308(a)(2)		
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	§ 164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	§ 164.308(a)(8)		
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)

PHYSICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§ 164.310(b)		
Workstation Security	§ 164.310(c)		
Device and Media Controls	§ 164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§ 164.312(b)		
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

ORGANIZATIONAL REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	(R)

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	(R)
		Availability	(R)
		Updates	(R)

Notice of Non-Discrimination

The notice must include certain terminology. Such as "Our practice complies with applicable Federal civil rights laws and does not discriminate on the basis of race, color, national origin, age, disability, religion, or sex (including pregnancy, sexual orientation, and gender identity)".

"We will not exclude people or treat them differently because of race, color, national origin, age, disability, religion, or sex (including pregnancy, sexual orientation, and gender identity)".

Section 1557 rule also includes protection for LGBTQI+ patients from discrimination.

Disability and Language Assistance

We provide free aids and services to people with disabilities to communicate effectively with us, such as:

- Qualified sign language interpreters.
- Written information in other formats (large print, audio, accessible electronic formats, other formats).

We provide free language services to people whose primary language is not English, such as:

- Qualified interpreters.
- Information written in other languages.

ARIS MEDICAL SOLUTIONS

Languages

The notice must be provided in English and in at least the **15 most common languages spoken** by people with Limited English Proficiency (LEP) in the State(s) served.

To ensure effective communication, these notices must be communicated to individuals with disabilities as effectively as they are to individuals without disabilities.

Some practices have decided to combine the two notices into one – Non-Discrimination/ Disability & Language Assistance.

Conscience Rights

Conscience rights apply to health care providers who refuse on religious or moral grounds to perform or assist in the performance of certain health care services.

Certain conscience statutes apply to more than just providers by referring to them as the "Federal health care conscience protection statutes".

Entities that are investigated by the OCR and documentation is requested should respond within a reasonable amount of time to avoid a negative evaluation from the OCR.

ARIS MEDICAL SOLUTIONS

Where to post notices

Covered entities are required to provide these notices in prominent locations both physically and on their websites.

For example, your NPP could be listed with patient forms or patient information.

Also make them available upon request.

Disability Access

Section 504 ensures equal access to the health care system and its social service programs for people with disabilities and their families. Ensuring they are not discriminated against under any program or activity receiving funding from HHS because they have a disability.

Medical practitioners shall ensure that medical treatment decisions are not based on negative biases or stereotypes about individuals with disabilities, judgments that an individual with a disability will be a burden on others, or dehumanizing beliefs that the life of an individual with a disability has less value than the life of a person without a disability.

Access is Important!

Health care facilities must ensure that their facilities are accessible to people with disabilities. When possible, medical equipment should also be accessible.

Examples: accessible examination tables, imaging machines, scales, and patient lifts.

Website / App / Kiosk Accessibility

The **ADA** requires that people with disabilities have equal access to information. An inaccessible website, mobile app, or kiosk can exclude people just as much as steps at an entrance to a physical location.

People with disabilities navigate the web in a variety of ways. People who are blind may use screen readers, which are devices that speak the text that appears on a screen. People who are deaf or hard of hearing may use captioning. People whose disabilities affect their ability to grasp and use a mouse may use voice recognition software to control their computers and other devices with verbal commands.

Accessibility Matters

- Increase color contrast.
- Add screen readers.
- Add text alternatives (“alt text”) on images.
- Add captions on videos.
- Add keyboard navigation.
- Add text size and zoom capability.
- Update online forms.

ARIS MEDICAL SOLUTIONS

Staff Training

The updated HIPAA training requirements for 2025 bring several significant changes. The most notable is the emphasis on cybersecurity.

Cybersecurity awareness is a critical component, and employees must be trained in recognizing and responding to potential cyber threats. This includes:

- understanding how to identify phishing attempts,
- using strong passwords, and
- implementing multi-factor authentication.

Regular cybersecurity drills and simulations can also help employees stay prepared for real-world threats.

Additional Requirements for Remote Work and Telemedicine
With remote work and telemedicine, it is critical to have clear guidelines in place.

Patient Privacy and Data Protection
Employees must be trained in the proper handling of patient information, including how to store, share, and dispose of data securely.

Training in non-discrimination
and educating the staff on how to use language assistant tools.

Did you know…

Malware can be imbedded in a download?

Key logger malware can be picked up on the internet without your knowledge and track your keystrokes!

Apps and games on your devices can steal information?

Smart phones and tablets can **transfer malware and viruses** to your network by charging them through a USB port or connecting to the Wi-Fi?

Ways to protect patient data

Don’t click on links in an email or on your phone - Remember **one click** can infect your system.

If an email, or text that asks you to do something **immediately**, requests private information, or asks you to verify by clicking on a link…DON’T.

Phone calls warning you of a new virus and offering a “free” scan - **NEVER** allow anyone access that is not authorized to do so.

ARIS MEDICAL SOLUTIONS

Fwd: Your Costco membership will be Terminated on Monday 27 January 2025

From: Your membership <CovertLocker@cdjtime.co.uk>
Date: January 27, 2025 at 1:53:39 PM EST
To: paedson@aol.com
Subject: Your Costco membership will be Terminated on Monday 27 January 2025
Reply-To: CovertLocker@cdjtime.co.uk

COSTCO WHOLESALE

Subscription Renewal Issue

We Couldn't Renew Your Costco Subscription

Dear Customer, unfortunately, we were unable to process your payment to renew your Costco Membership.

Subscription ID: AAA**82-US**

Product: *Coscto*

Expiration Date: **Monday 27 January 2025**

We attempted to renew your subscription at the end of the billing cycle, but the payment did not go through. As a result, your subscription has been canceled. We would be delighted to have you back.

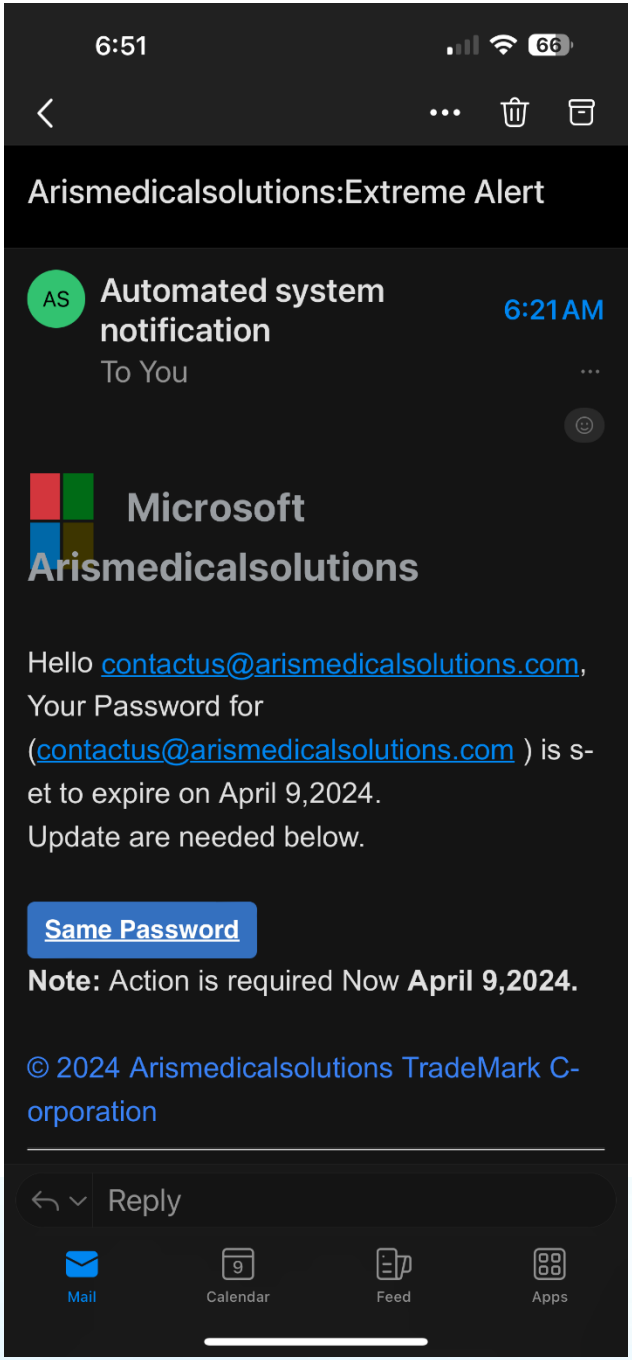
If you would like to renew your membership, please update your payment information by clicking the button below.

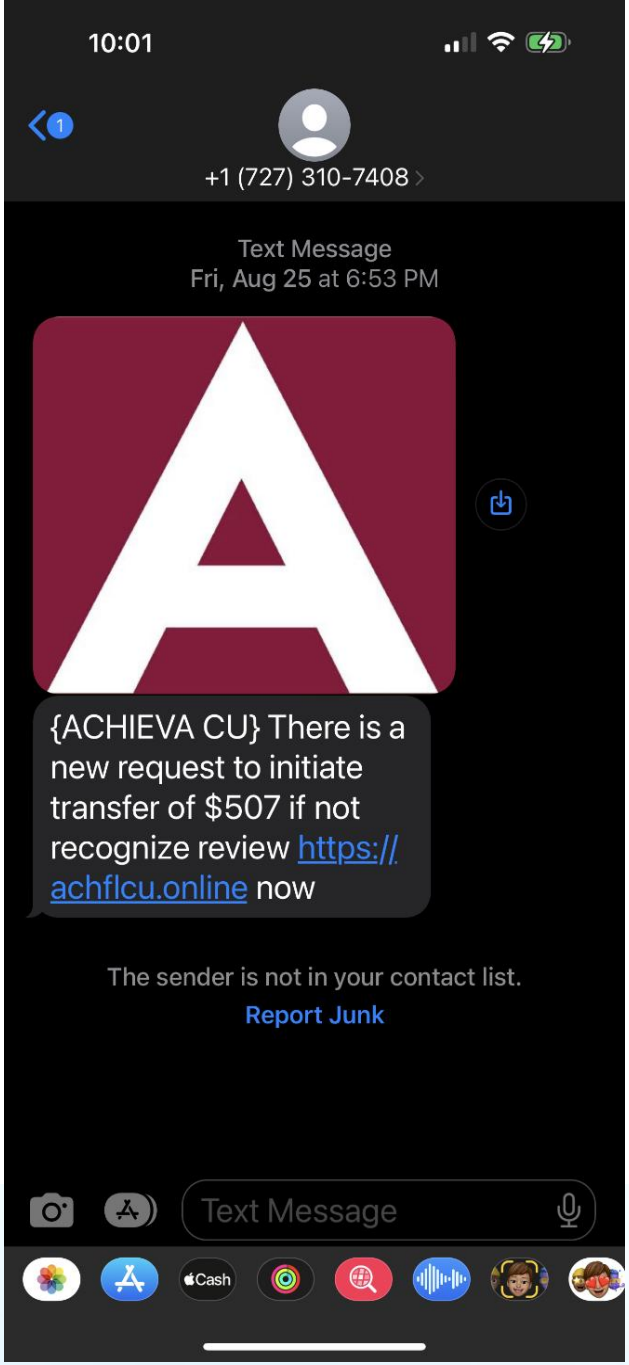
Update Payment Details

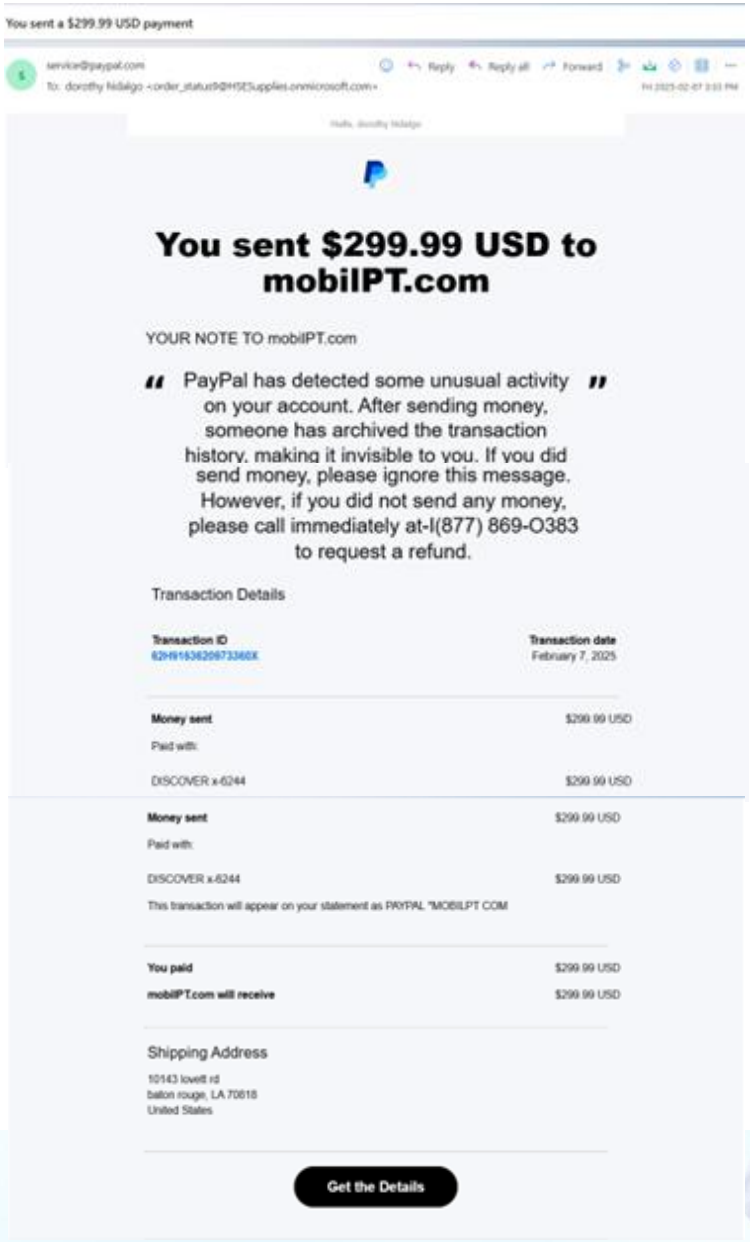
Note: If no action is taken, your services will be fully suspended within 24 hours, as outlined in our agreement.

Thank you for being a valued customer.
Best regards,

If you wish to unsubscribe, click here
115 E 23rd St New York, NY, US 10010


6:51
Arismedicalsolutions:Extreme Alert
AS
Automated system notification
6:21 AM
To You
Microsoft
Arismedicalsolutions
Hello contactus@arismedicalsolutions.com,
Your Password for
(contactus@arismedicalsolutions.com) is s-
et to expire on April 9,2024.
Update are needed below.
Same Password
Note: Action is required Now April 9,2024.
© 2024 Arismedicalsolutions TradeMark C-
orporation
Reply
Mail
Calendar
Feed
Apps


10:01
+1 (727) 310-7408
Text Message
Fri, Aug 25 at 6:53 PM
{ACHIEVA CU} There is a new request to initiate transfer of $507 if not recognize review https://achflcu.online now
The sender is not in your contact list.
Report Junk
Text Message
Cash



You sent a $299.99 USD payment

service@paypal.com
to: dorothy hidalgo <order_status9@HSESupplies.onmicrosoft.com>

Reply Reply all Forward

Fri 2025-02-07 3:03 PM

Hello, dorothy hidalgo

You sent $299.99 USD to mobilPT.com

YOUR NOTE TO mobilPT.com

" PayPal has detected some unusual activity on your account. After sending money, someone has archived the transaction history, making it invisible to you. If you did send money, please ignore this message. However, if you did not send any money, please call immediately at-I(877) 869-O383 to request a refund. "

Transaction Details

Transaction ID	Transaction date
62H91636209733660X	February 7, 2025

Money sent	$299.99 USD
Paid with:	
DISCOVER x-6244	$299.99 USD

Money sent	$299.99 USD
Paid with:	
DISCOVER x-6244	$299.99 USD

This transaction will appear on your statement as PAYPAL *MOBILPT COM

You paid	$299.99 USD
mobilPT.com will receive	$299.99 USD

Shipping Address

10143 lovett rd
baton rouge, LA 70818
United States

Get the Details

The 2024 Data Breach Report

The recurring HIPAA compliance issues that were documented from the OCR conference are:

- Patient Right of Access
- Risk Analysis
- Business Associate Agreements
- Access Controls
- Audit Controls
- Information System Activity reviews

What Triggers an Investigation

Data Breach - Either from the Covered Entity **OR** from a business associate.

Disgruntled Employee – this has become more prevalent than in the past.

Patient Complaint - If a patient is upset, do your best to listen to their complaint.

Social Media Posts – Be careful how you respond to negative reviews or comments.

Responding to an OCR Inquiry

After you receive a letter requesting documentation, **do not delay**! This elephant in the room is not going to disappear!

Depending on the type of incident, gather your security team or your privacy team to discuss what happened. Review your documentation. Never give the OCR more than what they request and always be clear and concise in your explanation.

How to prepare?

- Conduct a system wide risk analysis.
- Review your policies and procedures.
- Update your forms and notices.
- Train your staff.
- Repeat.

How can we help?

ARIS MEDICAL SOLUTIONS

"Simplifying HIPAA"

We know that the HIPAA compliance officer has many responsibilities because they are usually the practice administrator or an office manager.

You don't have time to research the changes, then write the policies, and create the forms.

That is what we do!

Suze Shaffer, CHSP
877.659.2467
info@arismedicalsolutions.com

Simplifying HIPAA through Automation, Education, and Support!