Suze Shaffer, CHSP

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

She has spoken at numerous conferences and functions to educate organizations on what it means to be HIPAA compliant.

It involves more than what you think!

ARIS MEDICAL SOLUTIONS

Who are we?
What do we do?

- Annual HIPAA Risk Analysis (MIPS)
- HIPAA training (customized)
- Breach notification plan
- Security incident / breach forms
- Patient privacy policies
- Patient request forms
- Security policies and procedures
- Security documentation forms
- Contingency plans
- Consulting and implementation

ARIS
MEDICAL SOLUTIONS

Poll

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

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

ARIS
MEDICAL SOLUTIONS
"Simplifying HIPAA"

How to avoid non-compliance penalties when responding to patient requests and other costly data privacy violations.

Educating your Staff

- Information blocking – What is it and how this affects your practice
- Right of Access - Watch the timeline
- Audit logs – What are these logs and why they are so important
- Data security - What every employee needs to know
- Security incidents – What are they and how to avoid them
- Phishing – Scammers are more difficult to spot now

ARIS MEDICAL SOLUTIONS

Poll

To keep this relevant and interesting I would like to ask…

What are you most interested in learning about?

1. Information blocking
2. Right of Access
3. Audit logs
4. Data Security
5. Security Incidents
6. Phishing examples

Privacy vs Security

How are these Rules Defined?

They encompass many aspects of Patient Privacy, Patient Rights, and Security.

- Privacy Rule, 2003
- Security Rule, 2005
- HITECH Act, 2009
- Omnibus Rule, 2013
- Enforcement Rule
- Breach Notification Rule

ARIS MEDICAL SOLUTIONS

What is Information Blocking?

Information blocking is a practice by an "actor" that is likely to interfere with the access, exchange, or use of electronic health information (EHI), except as required by law or specified in an information blocking exception.

The “actors” definition under the Cures Act applies to healthcare providers, health IT developers of certified health IT, and health information exchanges (HIEs)/health information networks (HINs).

ARIS MEDICAL SOLUTIONS

When does the Law Apply?

The law applies whether the actors know, or should know, that a practice is likely to interfere with the access, exchange, or use of EHI.

For healthcare providers, the law applies the standard of whether they know that the practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.

ARIS MEDICAL SOLUTIONS

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.

ARIS MEDICAL SOLUTIONS

Check the Availability

When a patient requests access or to share their information, if the staff member is unsure about the request, they should advise the patient they will check the availability of their request with their compliance officer.

Depending on the method of access or transfer, it may or may not be feasible at that time.

Remember, NEVER just say NO!
This could be considered information blocking!

Exceptions are Divided into Two Categories

Exceptions that involve not fulfilling a patient's request to access, exchange, or use EHI.

- Preventing harm
- Privacy
- Security
- Infeasibility
- Health IT Performance

Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.

- Licensing
- Fees
- Content and manner

When the practices with respect to accessing, exchanging, or using electronic health information (EHI) meet the conditions of one or more exceptions, such practices will not be considered information blocking.

ARIS MEDICAL SOLUTIONS

Right of Access

Patients have the "right of access" to view and receive a copy of their PHI/ePHI. HIPAA prohibits undue restrictions when a patient makes this request. You must make a "reasonable" effort to verify their identity.

HIPAA states you must answer the patient request within 30 days, with one 30-day extension. If you use this extension, you must advise the patient the reason for the delay and a date that their records will be made available.

We recommend acting as soon as possible to avoid a patient complaint.

There have been citations ranging from $3,500K-$200K!

Timing is Important!

Under Information Blocking, you must respond immediately or within a reasonable time frame.

The Office of the National Coordinator (ONC) takes in the complaint, the Office of the Inspector General (OIG) conducts the investigation, and the Office for Civil Rights (OCR) has jurisdiction when HIPAA intersects.

Proposed Rules

The right of access time frame may be reduced to 15 days, with one 15-day extension.

Patients may take pictures of their records and record the visit. Some states require consent from both parties to be recorded. Florida happens to be one of those states.

We recommend taking precautions in the event the patient does not disclose they are recording.

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)

Information System Activity

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)

Who is your new BFF?

Information System Activity is referred to as Audit Logs!

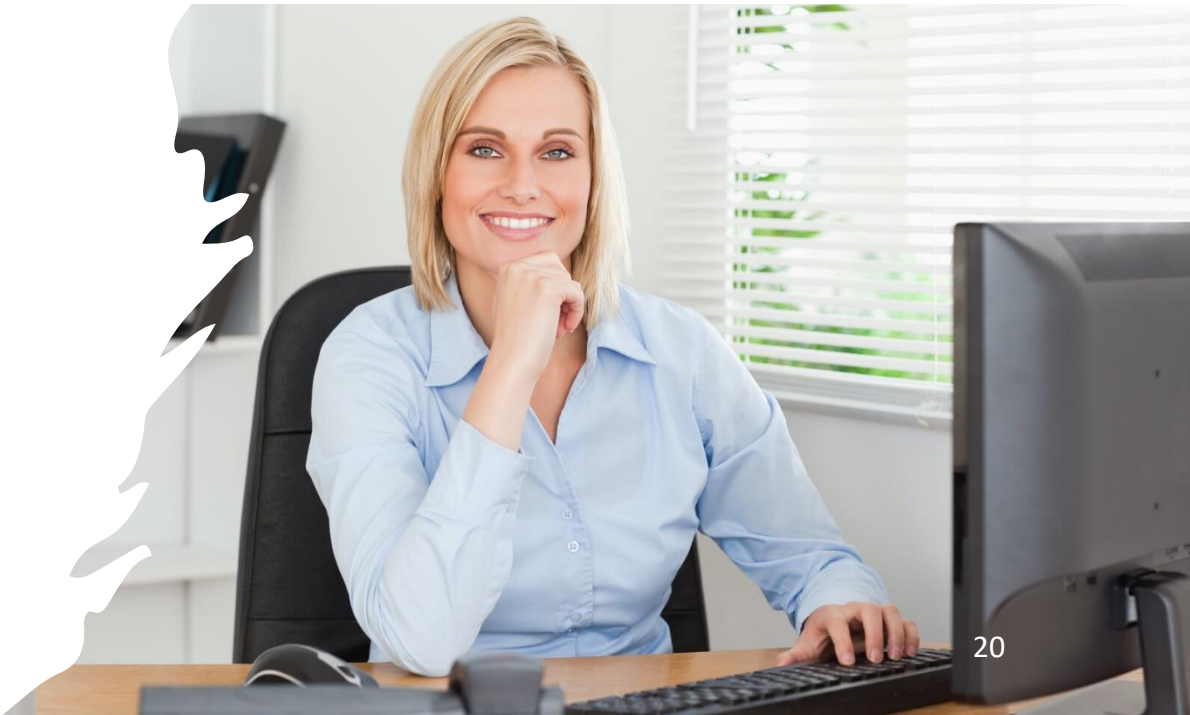
- Where are they located?
- Why do we have to monitor these logs?
- Why are they so important?
- What is the ultimate goal?

ARIS MEDICAL SOLUTIONS

Data Security - Physical

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)

Workstation Use and Security



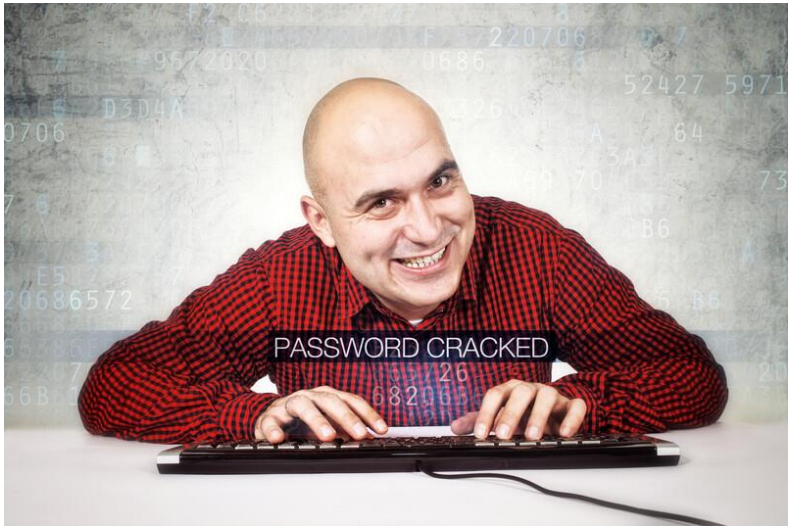
Data Security - Technical

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)

Access Controls

ARIS MEDICAL SOLUTIONS

Person or Entity Authentication



Usernames and passwords are the typical forms of authentication.
However, passwords are the most frequently compromised.

Transmission Security

- Email
- Text
- Website forms

ARIS MEDICAL SOLUTIONS

Online Tracking Technology

The Office for Civil Rights (OCR) has teamed up with the Federal Trade Commission (FTC) to investigate healthcare websites.

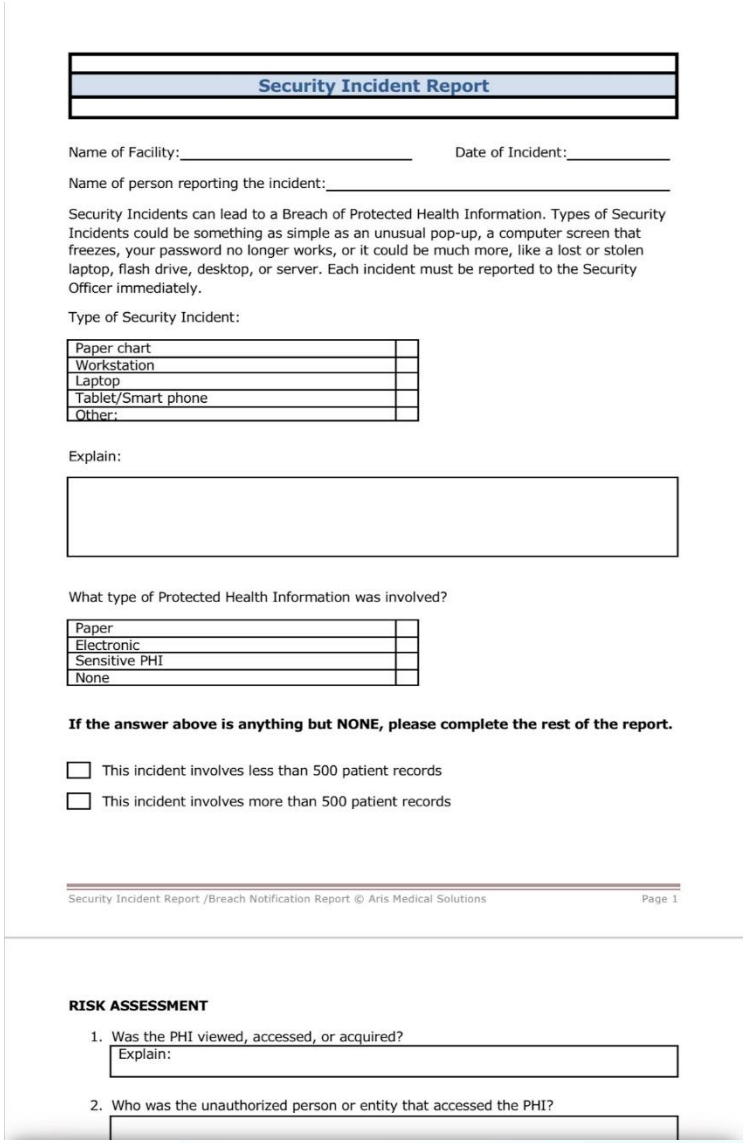
Some medical marketing and website designers are not up to date with the HIPAA requirements.

ARIS MEDICAL SOLUTIONS

Security Incidents

A security incident under 45 CFR § 164.304 is defined as the **attempted** or **successful** unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Additionally, 45 CFR § 164.308(a)(6)(ii) requires business associates to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the business associate; and document security incidents and their outcomes; and must report security incidents to its covered entity.



Security Incident Report

Name of Facility:_____ Date of Incident:_____

Name of person reporting the incident:_____

Security Incidents can lead to a Breach of Protected Health Information. Types of Security Incidents could be something as simple as an unusual pop-up, a computer screen that freezes, your password no longer works, or it could be much more, like a lost or stolen laptop, flash drive, desktop, or server. Each incident must be reported to the Security Officer immediately.

Type of Security Incident:

Paper chart	
Workstation	
Laptop	
Tablet/Smart phone	
Other:	

Explain:

What type of Protected Health Information was involved?

Paper	
Electronic	
Sensitive PHI	
None	

If the answer above is anything but NONE, please complete the rest of the report.

☐ This incident involves less than 500 patient records

☐ This incident involves more than 500 patient records

Security Incident Report /Breach Notification Report © Aris Medical Solutions Page 1

RISK ASSESSMENT

1. Was the PHI viewed, accessed, or acquired?
   Explain:
2. Who was the unauthorized person or entity that accessed the PHI?

Security Incident form should include:

- What type of incident?
- What type of PHI was involved?
- Did this involve less than 500 records or Over 500 records?
- Conduct a risk assessment of the incident.
- Breach determination.
- Then you sign and date the report once finalized.

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 avoid a security incident

Let IT install updates - Remember one click can infect your system.

If an email, text, or a phone call asks you to do something immediately or asks for private information, DON'T. Trust but verify!

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

More ways to avoid a security incident

Do not plug in any USB drive without knowing where it came from.

Facebook Links and Ads - Open your browser and search for the topic or product instead.

Do not click on any links in an email or text messages, open your web browser and go to the website directly or look up the phone number and call them.

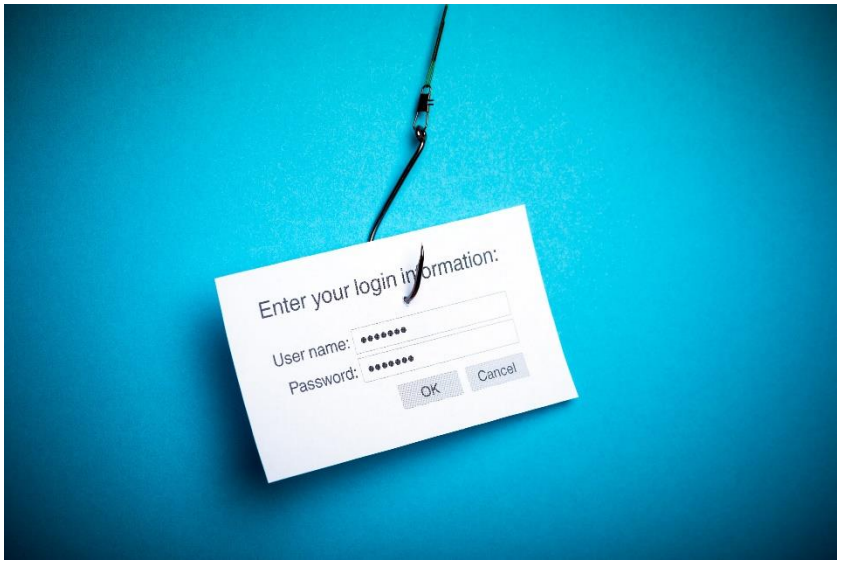
Reasonable & Appropriate

This is a HUGE gray area, and you must be careful you don't fall into the BIG black hole!

- Cost is a partial factor
- Size doesn't matter
- How you store your data
- Policies and Procedures
- Documentation is the KEY!

ARIS MEDICAL SOLUTIONS

Phishing



There two main types of phishing, regular phishing and spear phishing.

But the goal is the same!

They want you to click and share information!

9:52

safetytransactionswellsfarg087935...

Text Message
Yesterday 7:37 PM

(Get in touch: 8669661263) #Vvfx-9712 Your CARD is temporarily unavailable for usage. 7:36:08 PM

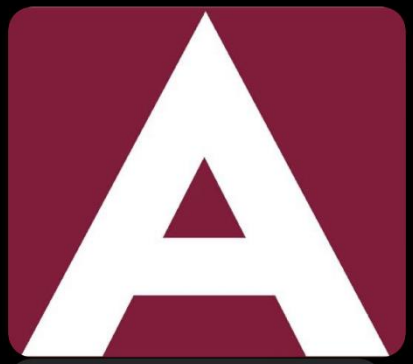
The sender is not in your contact list.
Report Junk

Text Message

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

10:01

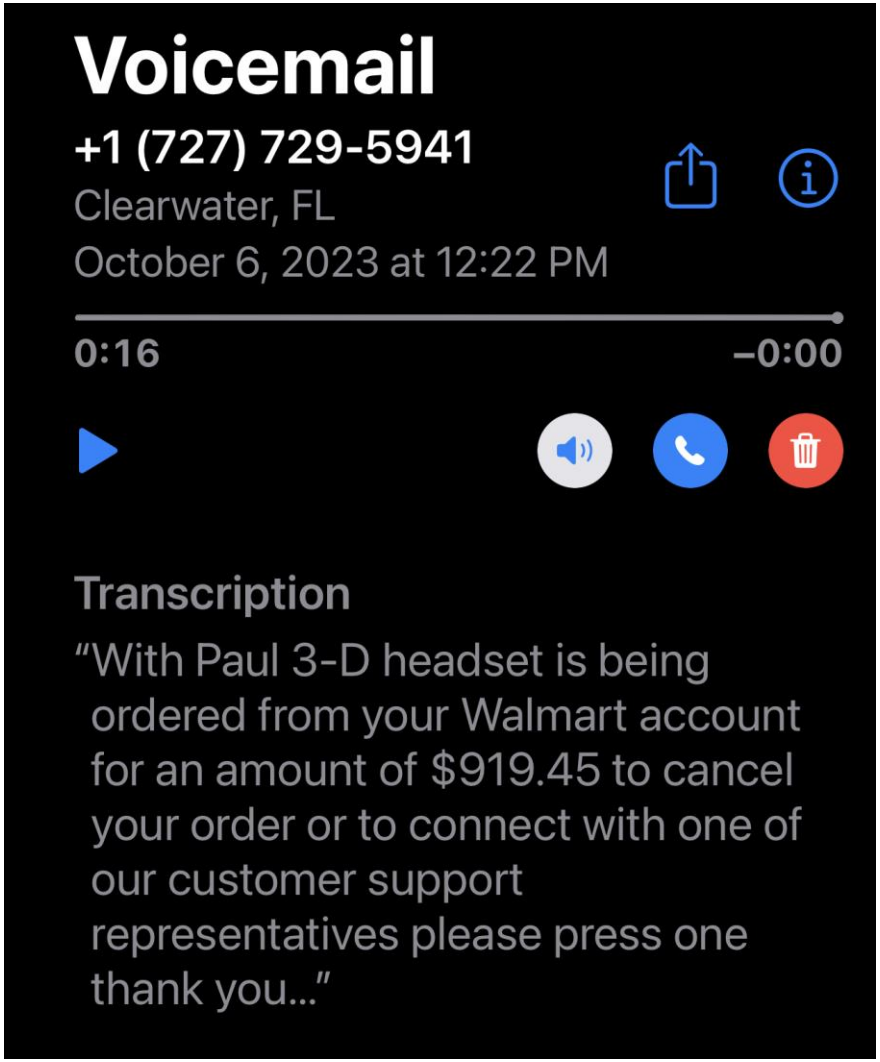
+1 (313) 980-3515

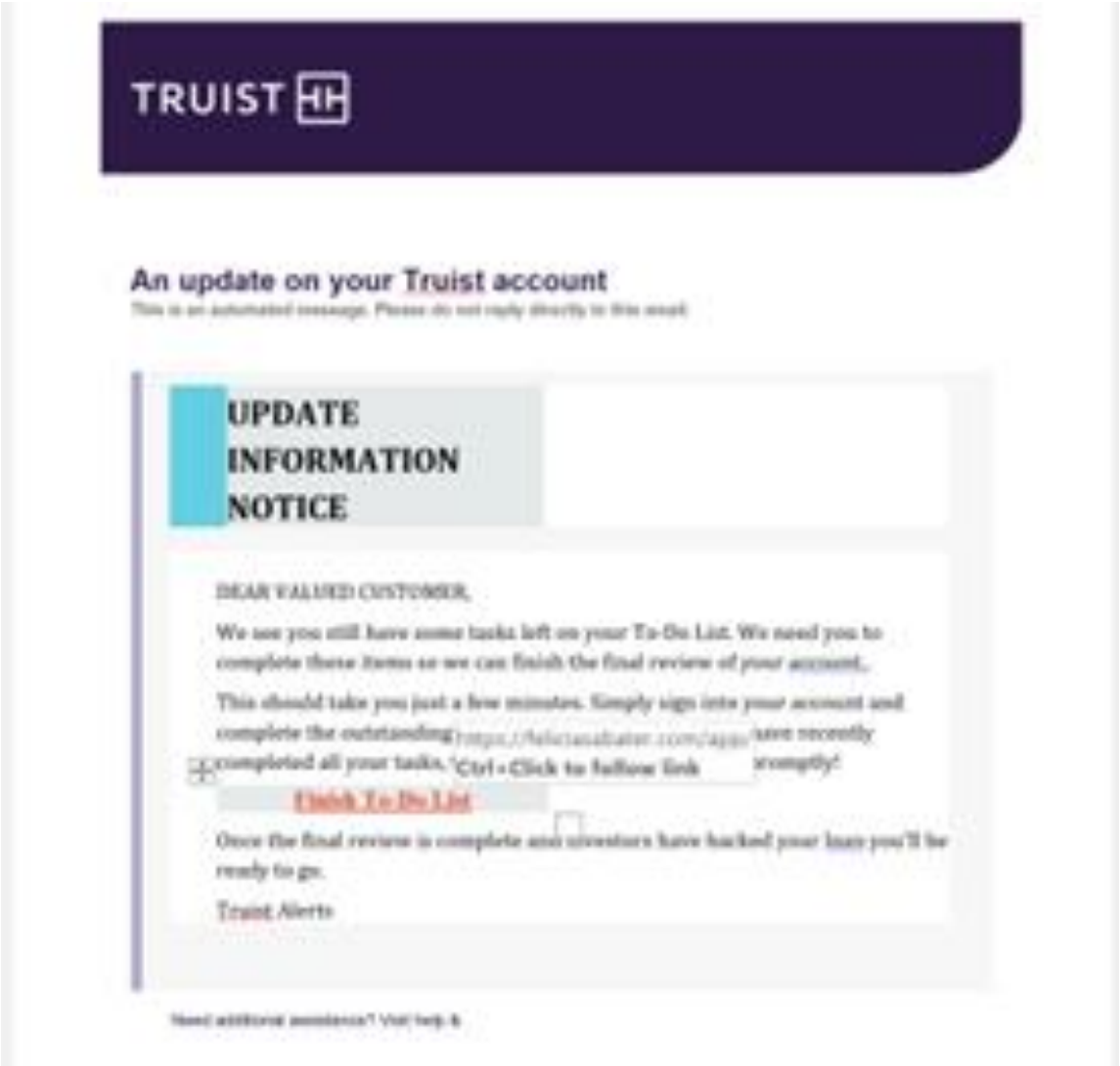
Text Message
Mon, Aug 28 at 1:15 PM

•{ ACHIEVA CU } ~A New transaction was added to your Bill pay; if this was done in an error,Visit Here https://disputeachievafcu.online/ to Cancel

The sender is not in your contact list.
Report Junk

Text Message


Voicemail
+1 (727) 729-5941
Clearwater, FL
October 6, 2023 at 12:22 PM
0:16
-0:00
Transcription
"With Paul 3-D headset is being ordered from your Walmart account for an amount of $919.45 to cancel your order or to connect with one of our customer support representatives please press one thank you..."



If you hover over the “Finish to-do List” you will see it takes you to a different website: Feliciasabater.com

When you receive an email, text, or phone call, you should call your bank or the company to advise them of what happened. If they are doing this to you, they are doing this to MANY others. Also, you can report this to the FTC. Federal Trade Commission.

NOTE: The FTC does not resolve individual reports, but your report will be entered in the FTC's Consumer Sentinel database and will be available to federal, state, and local law enforcement across the country

WHAT TO DO?

If you think you clicked a link or opened an attachment that downloaded harmful software:

- Update your computer's security software.
- Then run a scan and delete anything it identifies as a problem.
- Learn more about how to get fewer spam emails at ftc.gov/spam

If you think a scammer has your information, like your Social Security, credit card, or bank account number:

- Go to identitytheft.gov for steps you can to take based on what kind of information was lost or exposed.

If you gave your username and password to a scammer:

- Change your password right away. If you use the same password for other accounts or sites, change it there, too. Create a new password that is strong.

If someone calls and offers to "help" you recover money you have already lost:

- Don't give them money or personal information. You are probably dealing with a fake refund scam.

Scam Advice:

- Learn more about different scams and how to recovery from them at ftc.gov/scams.

General Advice:

- You can find tips and learn more about bad business practices and scams at consumer.ftc.gov.
- If you're concerned that someone might misuse your information, like your Social Security, credit card, or bank account number, go to identitytheft.gov for specific steps you can take.

You can get answers to common questions the FTC gets about filing a report at ReportFraud.ftc.gov/FAQs.

You can also update your report with more details at ReportFraud.ftc.gov/Update.

Find out what is going on in your state or metro area at ftc.gov/exploredata.

Check out ftc.gov/refunds to see recent FTC cases that resulted in refunds.

HELP!

Do you need a vendor?

- Have you conducted a system wide Risk Analysis?
- Have you created a Risk Management Plan from your Risk Analysis?
- Do you have the time to write your Policies & Procedures?
- Do you fully understand network security?

How to select a vendor?

- How many healthcare clients do they have?
- Has their product or service passed audits?
- Is support included with their product or service?
- Cost is not the only consideration!

ARIS MEDICAL SOLUTIONS

Simplifying HIPAA through Automation, Education, and Support!

Thank you!

ARIS MEDICAL SOLUTIONS

"Simplifying HIPAA"

If you would like to schedule a customized HIPAA training or if you would like to learn about our online HIPAA *Keeper*™ and let Aris help you safeguard your patient data…

Contact:
Suze Shaffer, CHSP
HIPAA Security Analyst
info@arismedicalsolutions.com
877.659.2467

Simplifying HIPAA through Automation, Education, and Support!