



PROGRESSIVE
SURGICAL SOLUTIONS
A DIVISION OF BSM CONSULTING

CURRENT TRENDS IN HIPAA AND CYBERSECURITY

KURT BRATTEN
PROGRESSIVE HALFTIME WEBINAR
NOVEMBER 18, 2020

1

Training Topics



How to Work Safely from Home



Computer Security and Phishing



Physical Security and Video Monitoring



Business Associates: Working with Billing Companies



OCR Right of Access Initiative



Incident Response and Other Reporting Obligations

2

How to Work Safely From Home



WHY YOU SHOULD BE CONCERNED

- Remote environment is typically outside of your security and direct control/knowledge
- Remote workers can infect the whole ASC network
- Personal use of work PC or systems can cause a breach or compromise your entire network
 - It's your network - outlaw personal use
 - Administrative and technical options available



3

How to Work Safely From Home

- Follow and enforce your security practices in remote environment
- Have Users Secure Home Networks
 - Reset default password
 - Restrict access to personal computer
 - Anti-virus software, firewalls, etc.



4

How to Work Safely From Home

- Think about Multi-Factor Authentication
- Shred all documentation containing confidential information
- Avoid use of Public Wi-Fi
- Electronic files
 - Avoid flash drives and local storage
 - Do not save files to your desktop



5

How to Work Safely From Home

- Consider using a virtual private network (VPN)
- Consider using Cloud Services and secure storage for remote workers



6

How to Work Safely from Home

STAFF TRAINING
AND REMINDERS
ARE **MORE
IMPORTANT**
THAN EVER



Policies and
Expectations



Recent Incidents



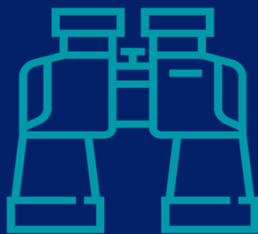
Threats



7

How to Work Safely from Home

**BE
MINDFUL**

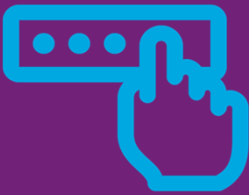


- ✓ Alexa and other such devices
- ✓ Lock your computer or device when you step away
- ✓ How work materials are stored
- ✓ Who is around you



8

Computer Security



PASSWORDS AND LOGINS

- **PASSWORDS MUST BE** secure, complex, unique and not easily guessed by others
- **PASSWORDS MUST BE** at least 8-10 characters, contain at least one uppercase letter, at least one lowercase letter and at least one special character
- **BEST PRACTICE:** Length is more important than complexity



9

Computer Security



PASSWORDS AND LOGINS

- **DO NOT SHARE** any login identification information, passwords or other credentials necessary to access the Entity's systems with any person
- **DO NOT** allow passwords or credentials to be visible to others in open areas (avoid writing them down)



10

Computer Security | Phishing & Vishing

- Your organization can receive fraudulent or phishing emails laced with malicious software or other email or voicemail scams
- Phishing emails contain links or attachments and with one click malicious software is capable of being downloaded
- These scams are becoming more sophisticated and multifaceted, though traditional scams persist



 PROGRESSIVE
SURGICAL SOLUTIONS
A DIVISION OF BSH CONIGIA, INC.

11

Computer Security | Phishing & SPAM

- Phishing emails are usually from suspicious or unknown sources
- Typically contain bad grammar, strange formatting/requests or other “giveaways”
- The links and attachments associated with these emails **MUST NOT** be opened or clicked



 PROGRESSIVE
SURGICAL SOLUTIONS
A DIVISION OF BSH CONIGIA, INC.

12

Phishing Email Examples

From: oalaw.com <a.kozhobekov@sf.kg>
Date: January 24, 2019 at 10:24:15 AM EST
To: <fwander@oalaw.com>
Subject: Re:Parcel Delivery For fwander@oalaw.com

Dear fwander,

Your package arrived at our facility since January 23rd 2019. Our courier agents were unable to deliver the packages due to incorrect delivery address details on the package registry.

DELIVERY DETAILS ARE AS FOLLOWS :

Waybill No.	*****083789
Scheduled Delivery Date	Wednesday January 23rd 2019
Delivery Time	Pending Correction

Please [CLICK HERE](#) to confirm your address, before we submit to our outlet office for dispatch to your destination.


Regards,
Leandro Bravo
Customer Care

2019 © FEDEX International GmbH. All rights reserved.
FEDEX Global Mail

FEDEX Global Mail is your specialist for international Business Mail, B2C Parcel, Direct Marketing, and Hybrid or fully Digital Services. With our international postal solutions, we are dedicated to making our customers' lives easier.

13

Phishing Email Examples



You have a parcel coming.

Scheduled Delivery Date: Tuesday, 25/04/2017

To verify the actual transit status of your shipment, click on the tracking link below.

Shipment Details

From:
Tracking Number: [9FW98042870231419](#)
Number of Packages: 7
Scheduled Delivery: 25/04/2017
Weight: 16.3 KGS

14

Phishing Email Examples

From: Gina Sullivan [<mailto:emerald.credit@princessegypthotels.com>]
Sent: Tuesday, January 22, 2019 10:46 AM
To: Nancy Sciocchetti <nsciocchetti@Oalaw.com>
Subject: Invoice 023905

Thank you for your help. Please see the attached.

[DOC-023905.doc](#)

Gina Sullivan
GSullivan@sefcu.com

15

Computer Security and Phishing



AVOID BEING A VICTIM OF PHISHING

- You must tell your workforce what is expected and prohibited
- Policies, training and reminders are essential
 - Use real examples
- Must be persistent



16

Computer Security and Phishing



USE POSITIVE REINFORCEMENT

- Tell staff how it works and that a single click could compromise the network
- Create a clear password policy and assign someone to enforce it
- Explain to your staff how to avoid phishing and other scams
- Use interpersonal (non-email) verification of important data and instructions
 - Wiring instructions
 - Any email or request that is suspicious or unexpected
- Every email does not need to be reconciled



17

Computer Security and Phishing



PROHIBITED ACTIVITY | POLICIES AND TRAINING

- ***“Do not click on anything suspicious or from an unknown source and to scrutinize every incoming email”***
 - Notify staff that the failure to immediately report will be grounds for disciplinary action



18

Computer Security and Phishing



PROHIBITED ACTIVITY | POLICIES AND TRAINING

- ***“The Entity’s systems are for Entity purposes. All data collected or generated by in or by the Entity’s assets, systems and IT network or created thereon, remain the property of the Entity. You must be careful of the websites you visit and the files and applications you open. Do not visit or open questionable or unknown content on our system.”***
 - File sharing Apps should be forbidden
 - Personal Financial Data and Wiring Instructions should never be sent over email



19

Physical Security and Video Monitoring

Physical security is the people, locks, doors, surveillance and other physical features used to secure your spaces and Confidential Information

Physical access restrictions are critical and encourage compliance



20

Physical Security and Video Monitoring



MANY ASCs USE VIDEO CAMERA SURVEILLANCE

- No federal law; most states allow video cameras, except for areas where an individual has a reasonable expectation of complete privacy (bathroom, changing rooms, etc.). Some states require employee notice and/or consent.
- I encourage notice because it fosters compliant behavior
- Audio recordings are a separate issue – be sure to follow state law



21

Business Associates

Covered Entities (CEs) and Business Associates (BAs) are independently required to have BA Agreements in place

- The failure to do so is an independent violation of the HIPAA regulations
- The **HITECH Act** significantly expanded liability and obligations for BAs
 - BAs must comply with the Security Rule



22

Business Associates



WHO IS A BUSINESS ASSOCIATE

- Business Associates are entities that create, receive, maintain, or transmit PHI on behalf of the Covered Entity
 - Typically assist CE with HIPAA functions (i.e. healthcare operations, payment, etc.); or
 - Perform traditional function requiring access to PHI (i.e. legal, accounting, billing or claims management)
- Data storage or hosting companies (i.e. cloud or off-site storage providers) are BAs even if they do not access PHI
- Includes subcontractors of BAs with access to PHI



23

BA | Working with Billing Companies

- In my experience, many billing companies have weak security and internal controls, tenuous relationships with employees and warrant added scrutiny
- Focus on contract terms
 - Demand strong indemnification and liability protections
 - Make sure your bills and data will be protected/returned post-termination
 - Confirm legality of fee arrangement
- Trust by verify



24

OCR Right of Access Initiative

**PATIENTS HAVE
THE RIGHT TO
ACCESS THEIR
RECORDS**



- HIPAA requires disclosure to patient or qualified person upon verbal or written authorization
- Providers may require written authorization for the release of confidential data/records but this cannot serve as a barrier



25

OCR Right of Access Initiative



OCR is Aggressively Enforcing Patient Access Rights

- OCR has settled 12 enforcement actions that include fines ranging from \$10,000 - \$160,000 and formal corrective action plans since 2019.
- These are triggered by single patient complaints.






26

Reporting Obligation



You **MUST** report
to your Supervisor or Security Officer

-  Suspicious Activity
-  Data Loss
-  Security Concerns



27

Incident Response and Other Reporting Obligations



EXAMPLES OF REPORTABLE ISSUES

- Lost devices, phones and data
- Corrupt systems and information (missing or incorrect data or unauthorized changes)
- Theft of/damage to physical IT assets like computers, storage devices, printers
- Misuse of access rights, services, information, or assets
- Infection of systems by unauthorized or hostile software
- Attempted unauthorized access
- Unusual system behavior
- Warnings from malware/virus detection software and intrusion detection alarms



28

Available on
eSupport

HIPAA Overview

eSupport/Compliance/HIPAA



HOME ESUPPORT BLOG FORUM ACCOUNT

HIPAA: OVERVIEW

2018 WAS A RECORD YEAR FOR DATA BREACHES

It can happen to you

REFERENCE

Across all industries, the number of U.S. data breaches tracked in 2016 hit an all-time record high of 1,093, and in healthcare, troubling data security trends continue to plague the sector, according to new research from the Identity Theft Resource Center (ITRC) and CyberScout.

The number of breaches in 2016 represents a substantial hike of 40 percent over the near record high of 780 reported in 2015. Since 2005, the ITRC has been identifying data breaches in five industry sectors. In 2016, the business sector again topped the list in the number of data breach incidents, with 494 reported, representing 45.2 percent of the overall number of breaches. This was followed by the healthcare/medical industry (377 incidents), representing 34.5 percent of the overall total.

WHAT THIS MEANS:

The healthcare sector had the most records exposed by employee error or negligence. The healthcare industry was also the hardest hit by hacking, skimming and phishing attacks. So if you have not had a professional risk assessment done yet, get one done now! A formal risk assessment is required for all covered entities.

NEED HELP? WE RECOMMEND HIPAA SECURE NOW FOR ALL OF YOUR HIPAA COMPLIANCE NEEDS.

HIPAA  Secure Now!

SEARCH

HIPAA

HIPAA Overview

- Privacy vs. Security Officer
- Risk Assessment
- Disaster Recovery Plan
- Insurance Coverage
- Cell Phone Use



29



Questions?

Kurt Bratten

(518) 462-5601

kbratten@oalaw.com



30

Continued Education



1 CE CONTACT
HOUR PER
ATTENDEE.
(LICENSED NURSES)



COMPLETE COURSE
EVALUATION SENT
VIA EMAIL
BY FRIDAY 12/4.



ALLOW 2 WEEKS
FOR PROCESSING
OF YOUR
CERTIFICATE.



ANY QUESTIONS
REGARDING CE
CREDIT, CONTACT
LYN@PSS4ASC.COM

1 CE contact hour credit is offered to registered nurses who attend and complete course evaluation. *Progressive Surgical Solutions, LLC is approved by the California Board of Registered Nurses, Provider Number 17435.*



31

Join the eSupport Community!



Request your free web demo today
www.progressivesurgicalsolutions.com/esupport



Email us at info@pss4asc.com



Or call us! (855) 777-4272



32

Join our Private Facebook Group

A place to connect, support, and network with other ASC managers all over the country



www.facebook.com/groups/ascmangers/



33

Mark your Calendar

DATE	🕒	CE	WEBINAR TOPIC	SPEAKER
December 18	20 min		Annual Survey Watch Report	Vanessa Sindell

www.ProgressiveSurgicalSolutions.com/webinars



34