

Welcome to PMI's Webinar Presentation

Brought to you by:
Practice Management Institute[®]
pmiMD.com

Meet the Presenter...



Regina Mixon Bates,
IRO, CPC, CPC-I, CMC,
CMOM, CMIS, TPA

On the topic:

Why Mobile Security Matters



Welcome to Practice Management Institute's Webinar and Audio Conference Training. We hope that the information contained herein will give you valuable tips that you can use to improve your skills and performance on the job. Each year, more than 40,000 physicians and office staff are trained by Practice Management Institute. For 30 years, physicians have relied on PMI to provide up-to-date coding, reimbursement, compliance and office management training. Instructor-led classes are presented in 400 of the nation's leading hospitals, healthcare systems, colleges and medical societies.

PMI provides a number of other training resources for your practice, including national conferences for medical office professionals, self-paced certification preparatory courses, online training, educational audio downloads, and practice reference materials. For more information, visit PMI's web site at www.pmiMD.com

Please be advised that all information in this program is provided for informational purposes only. While PMI makes all reasonable efforts to verify the credentials of instructors and the information provided, it is not intended to serve as legal advice. The opinions expressed are those of the individual presenter and do not necessarily reflect the viewpoint of Practice Management Institute. The information provided is general in nature. Depending on the particular facts at issue, it may or may not apply to your situation. Participants requiring specific guidance should contact their legal counsel.

CPT® is a registered trademark of the American Medical Association.



Why Mobile Security Matters

Presented by:
Regina Mixon Bates
IRO, TPA, CPC, CPC-I, CMC, CMOM, CMIS



Copyright 2019, by The Physicians Practice S.O.S. Group® Atlanta GA, all rights reserved. All materials presented at seminars are copyrighted. Reproduction in whole or in part without the express written permission of The Physicians Practice S.O.S. Group®. is prohibited.

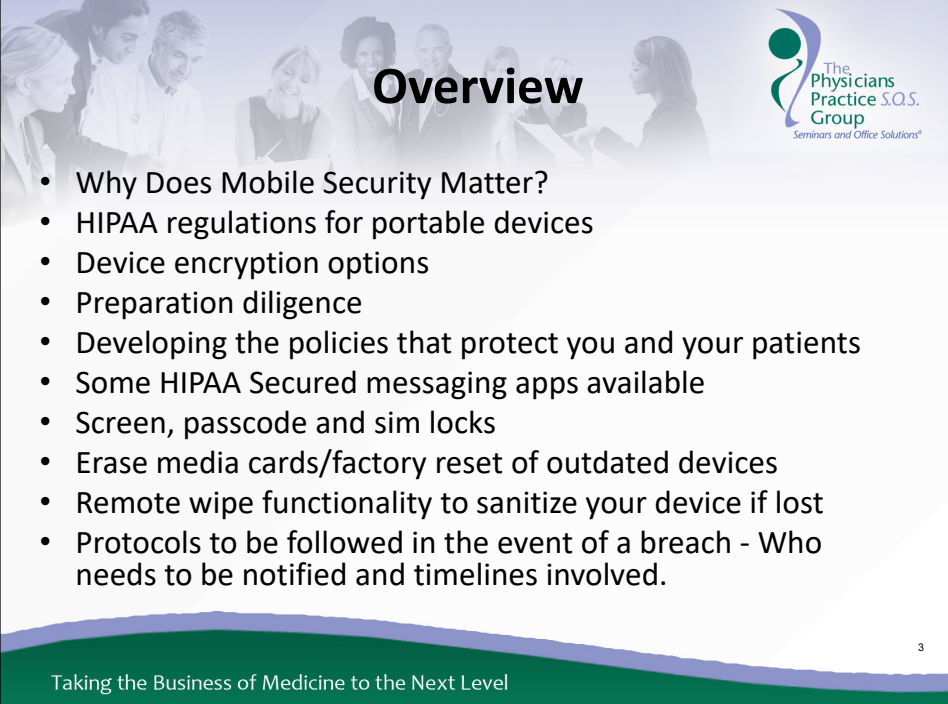
We do not endorse or provide any guarantee on the use of any software programs mentioned in this webinar; it is up to you to investigate any software, apps or programs.

FIND US ON
Facebook, LinkedIn, Twitter, Fix my Practice Blog and U-Tube :



2

Taking the Business of Medicine to the Next Level



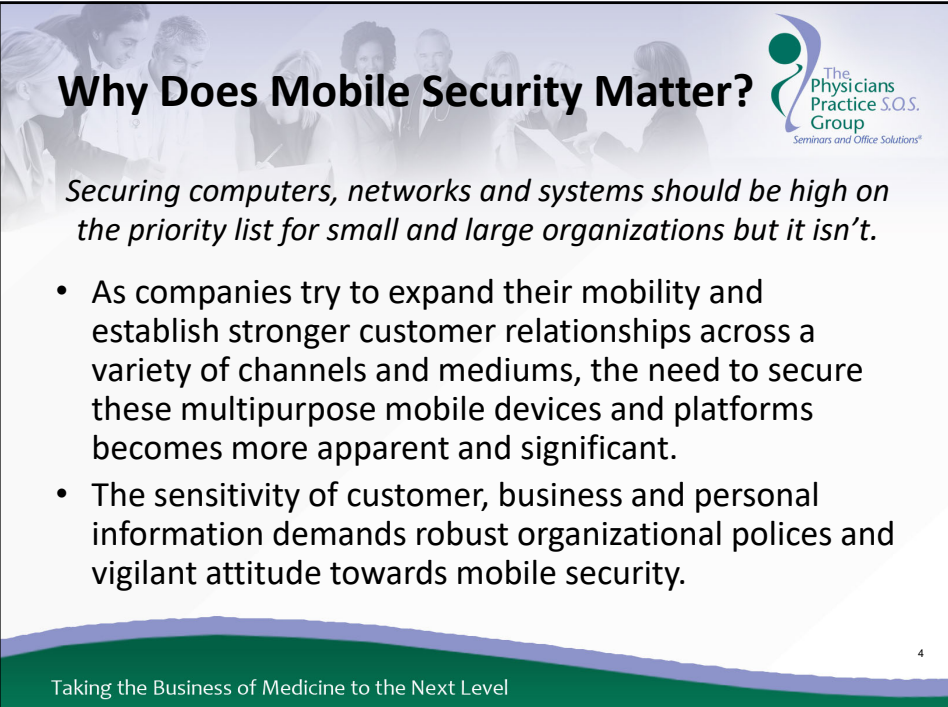
Overview

The Physicians Practice S.O.S. Group
Seminars and Office Solutions®

- Why Does Mobile Security Matter?
- HIPAA regulations for portable devices
- Device encryption options
- Preparation diligence
- Developing the policies that protect you and your patients
- Some HIPAA Secured messaging apps available
- Screen, passcode and sim locks
- Erase media cards/factory reset of outdated devices
- Remote wipe functionality to sanitize your device if lost
- Protocols to be followed in the event of a breach - Who needs to be notified and timelines involved.

3

Taking the Business of Medicine to the Next Level



Why Does Mobile Security Matter?


The Physicians Practice S.O.S. Group
Seminars and Office Solutions®

Securing computers, networks and systems should be high on the priority list for small and large organizations but it isn't.

- As companies try to expand their mobility and establish stronger customer relationships across a variety of channels and mediums, the need to secure these multipurpose mobile devices and platforms becomes more apparent and significant.
- The sensitivity of customer, business and personal information demands robust organizational polices and vigilant attitude towards mobile security.

4

Taking the Business of Medicine to the Next Level



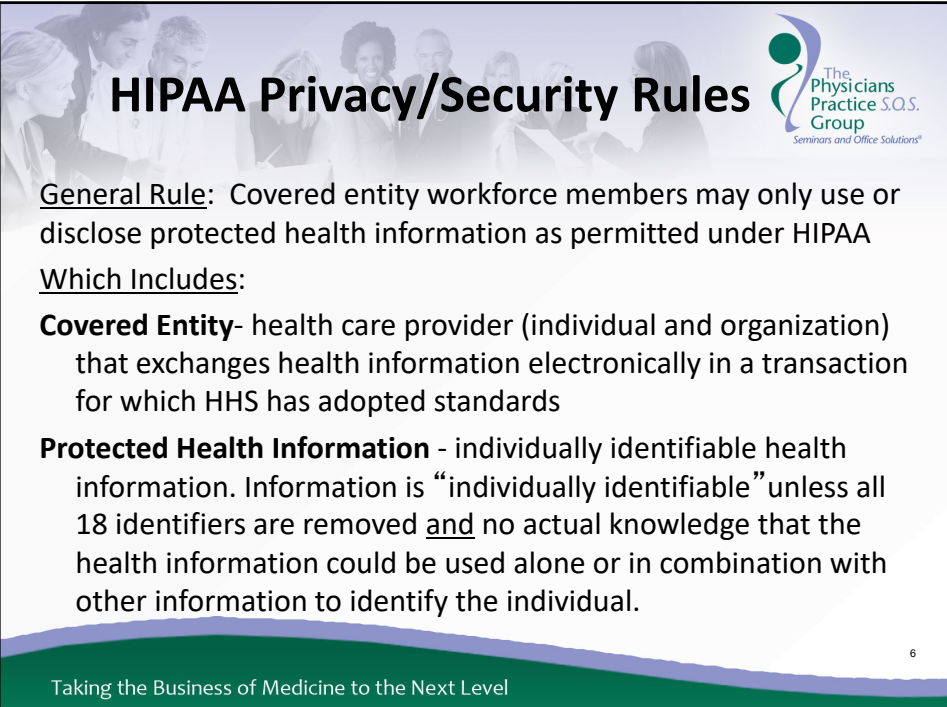
Why Does Mobile Security Matter?

The Physicians Practice S.O.S. Group
Seminars and Office Solutions®

- **Internal Compliance**
 - Safeguards, audits and enforcement more important than ever
- **Mobile Devices**
 - Biggest Risk
- **Patient/Family Interaction**
 - Sending PHI via email
- **Interaction with Colleagues/other health care providers, payors, agencies**
 - Use appropriate safeguards
- **Interaction with Business Partners**
 - BA Agreements; Assess risk; HIPAA liability for actions of agents
- **Social Media**
 - Common and easy; another big risk

5

Taking the Business of Medicine to the Next Level



HIPAA Privacy/Security Rules

The Physicians Practice S.O.S. Group
Seminars and Office Solutions®

General Rule: Covered entity workforce members may only use or disclose protected health information as permitted under HIPAA

Which Includes:

Covered Entity- health care provider (individual and organization) that exchanges health information electronically in a transaction for which HHS has adopted standards

Protected Health Information - individually identifiable health information. Information is “individually identifiable” unless all 18 identifiers are removed and no actual knowledge that the health information could be used alone or in combination with other information to identify the individual.

6

Taking the Business of Medicine to the Next Level




HIPAA Privacy/Security Rules




- HIPAA Security Compliance Requirements:
 - Privacy Officer must be named
 - Privacy Policies and Procedures must be implemented and enforced
 - Workforce members must be trained
 - Unique designations must be identified (hybrid entities, affiliated covered entities)
 - Workforce members' access to PHI must be designated
 - Other administrative/operational matters (e.g., notice of privacy practices, business associate agreements, accounting of disclosures, breach notification processes, risk assessments)

7

Taking the Business of Medicine to the Next Level



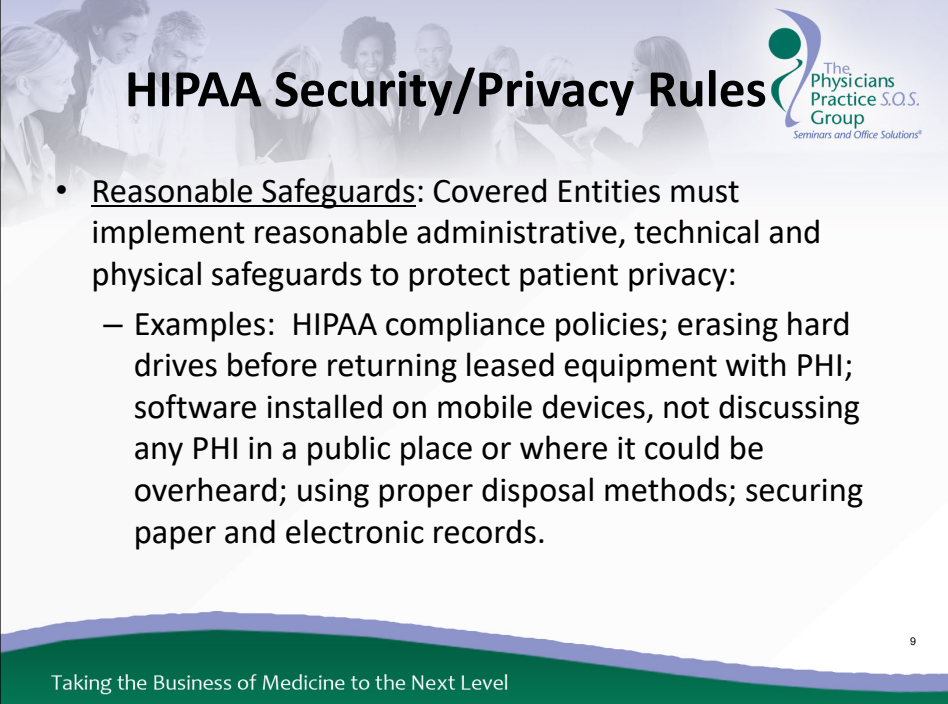
HIPAA Security/Privacy Rules



- Treatment, Payment, Healthcare Operations:
 - In general, Covered Entities may use/disclose PHI without a patient's authorization for **TPO**
 - Treatment purposes
 - Payment purposes
 - Operations purposes
 - e.g., Case management, care coordination, peer review, training, legal, auditing, business management

8

Taking the Business of Medicine to the Next Level



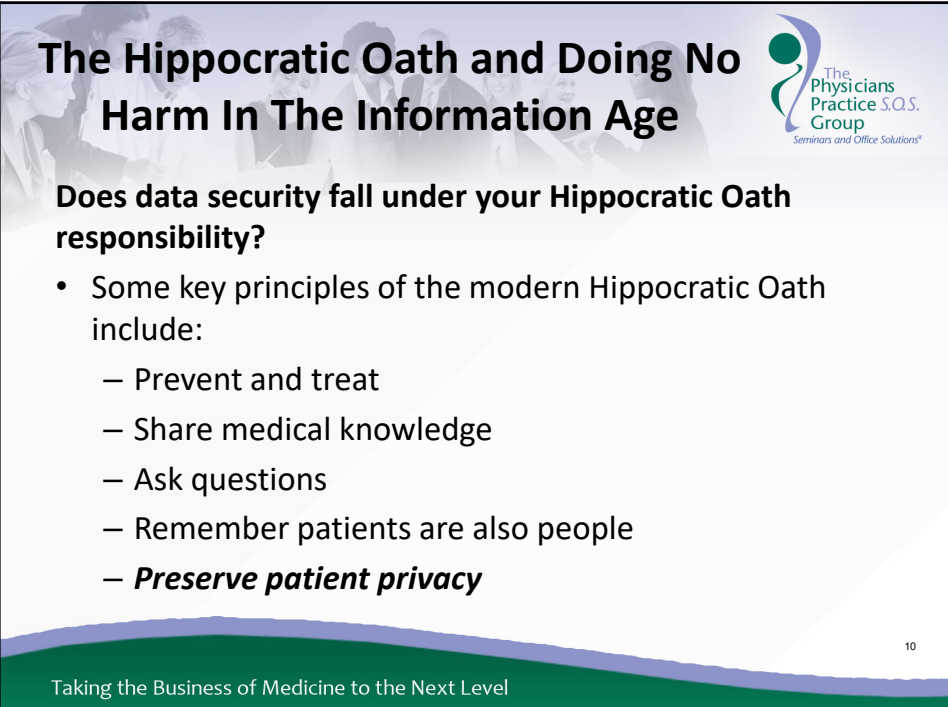
HIPAA Security/Privacy Rules

The Physicians Practice S.O.S. Group
Seminars and Office Solutions®

- **Reasonable Safeguards:** Covered Entities must implement reasonable administrative, technical and physical safeguards to protect patient privacy:
 - Examples: HIPAA compliance policies; erasing hard drives before returning leased equipment with PHI; software installed on mobile devices, not discussing any PHI in a public place or where it could be overheard; using proper disposal methods; securing paper and electronic records.

9

Taking the Business of Medicine to the Next Level



The Hippocratic Oath and Doing No Harm In The Information Age


The Physicians Practice S.O.S. Group
Seminars and Office Solutions®

Does data security fall under your Hippocratic Oath responsibility?


- Some key principles of the modern Hippocratic Oath include:
 - Prevent and treat
 - Share medical knowledge
 - Ask questions
 - Remember patients are also people
 - ***Preserve patient privacy***

10

Taking the Business of Medicine to the Next Level




Statistics on Mobile Device Data Breaches




- Breaches of more than 10,000 records have remained fairly constant year over year.
 - In 2015, there were 52 breaches of 10,000 or more records.
 - That figure jumped to 82 in 2016.
 - There were 78 healthcare data breaches in 2017 involving more than 10,000 records.
- The bad news is there was a significant rise in the number of healthcare data breaches in 2018.
- Ransomware attacks doubled in 2018 and were the primary driver for an overall doubling in total incidents. Ransom-based attacks came in various forms:
 - via malware-laced phishing attacks, malvertising,
 - and drive-by malware that encrypt data and block access to systems, if ransom is not paid.

11

Taking the Business of Medicine to the Next Level



Statistics on Mobile Device Data Breaches




- Privacy Rights Clearinghouse and the Open Security Foundation: Analysis of data concluded that mislaid, stolen or discarded portable devices caused records with personally identifiable information of 80.7 million individuals to be breached.
- Approximately 40% of the breaches involving 500 or more individuals that were reported to HHS involved mobile devices.


12

Taking the Business of Medicine to the Next Level

Most Recent Breaches Reported




The Physicians Practice S.O.S. Group
Seminars and Office Solutions®




NEWS

3 phishing hacks breach 20,000 Catawba Valley patient records



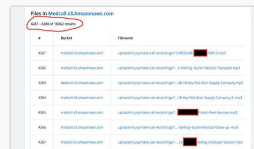
NEWS

CMS responds to data breach affecting 75,000 in federal ACA portal




NEWS

Two phishing attacks on Minnesota DHS breach 21,000 patient records




NEWS

Update: Misconfigured database breaches MedCall Advisors



NEWS

3 Massachusetts hospitals fined nearly \$1 million by OCR for HIPAA violations




NEWS

Employee error exposed Blue Cross patient data for 3 months

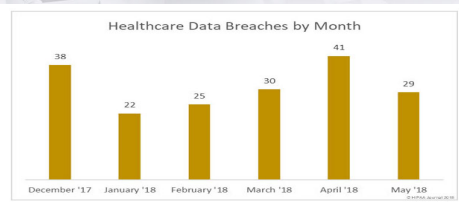
13

Taking the Business of Medicine to the Next Level

2018 Breaches Reported

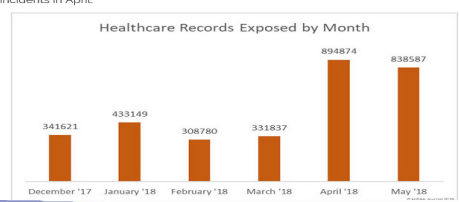


The Physicians Practice S.O.S. Group
Seminars and Office Solutions®



Month	Number of Breaches
December '17	38
January '18	22
February '18	25
March '18	30
April '18	41
May '18	29

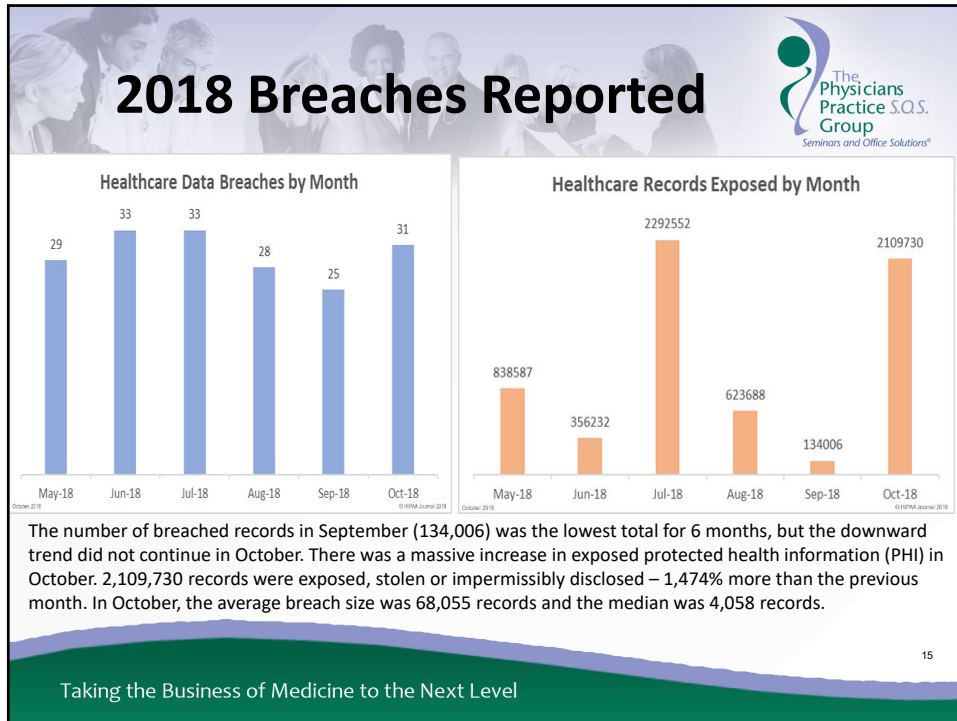
There were 29 healthcare data breaches reported by healthcare providers, health plans, and business associates of covered entities in May – a 29.27% month-over month reduction in reported breaches. However, 838,587 healthcare records were exposed or stolen in those incidents – only 56,287 records fewer than the 41 incidents in April.



Month	Number of Records Exposed
December '17	341,621
January '18	433,149
February '18	308,780
March '18	331,837
April '18	894,874
May '18	838,587

14

Taking the Business of Medicine to the Next Level

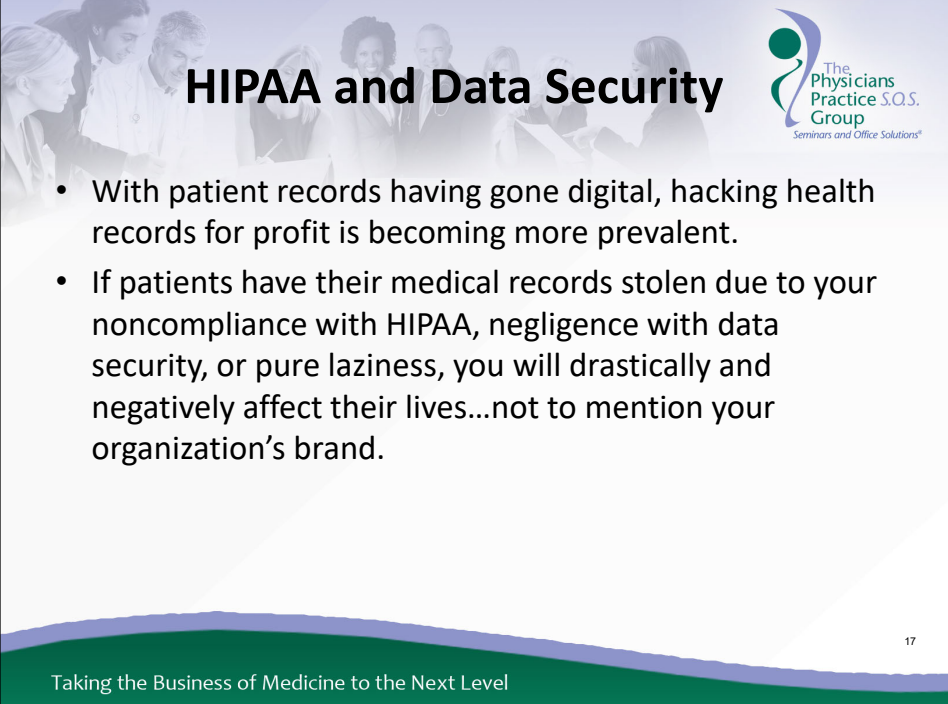


HIPAA and Data Security


- From my day to day experience, HIPAA isn't a major concern to many healthcare organizations and/or providers.
- It's important to remember HIPAA does apply to all covered healthcare providers and organizations.
- The HIPAA Security Rule in particular contains some of the most important considerations for data security that can help you ensure your patient healthcare data stays private.

16

Taking the Business of Medicine to the Next Level



HIPAA and Data Security



- With patient records having gone digital, hacking health records for profit is becoming more prevalent.
- If patients have their medical records stolen due to your noncompliance with HIPAA, negligence with data security, or pure laziness, you will drastically and negatively affect their lives...not to mention your organization's brand.

17

Taking the Business of Medicine to the Next Level



Biggest Risk Areas: Mobile Devices and Laptops



- In today's work force, mobile devices are an essential productivity tool, not simply a communication tool.
- In recent years the medical profession has become aware of the opportunities and challenges associated with mobile devices and Laptops.
- As technology has advanced, many hospitals and health care organizations have found it necessary to create their own policies in order to protect physicians and patients alike.
- Hacking health records for profit has become prevalent.

18

Taking the Business of Medicine to the Next Level



Biggest Risk Areas: Mobile Devices and Laptops



- Mobile Devices
 - It has become common for health care providers to communicate with patients using mobile devices or to access/relay PHI to other providers using mobile devices.
 - The unauthorized disclosure of ePHI (electronic protected health information) is a big risk when using mobile devices because they are small, portable, highly visible, unlikely password protected, unlikely to have encrypted PHI, and likely to connect with Wi-Fi (further risking interception).

19

Taking the Business of Medicine to the Next Level



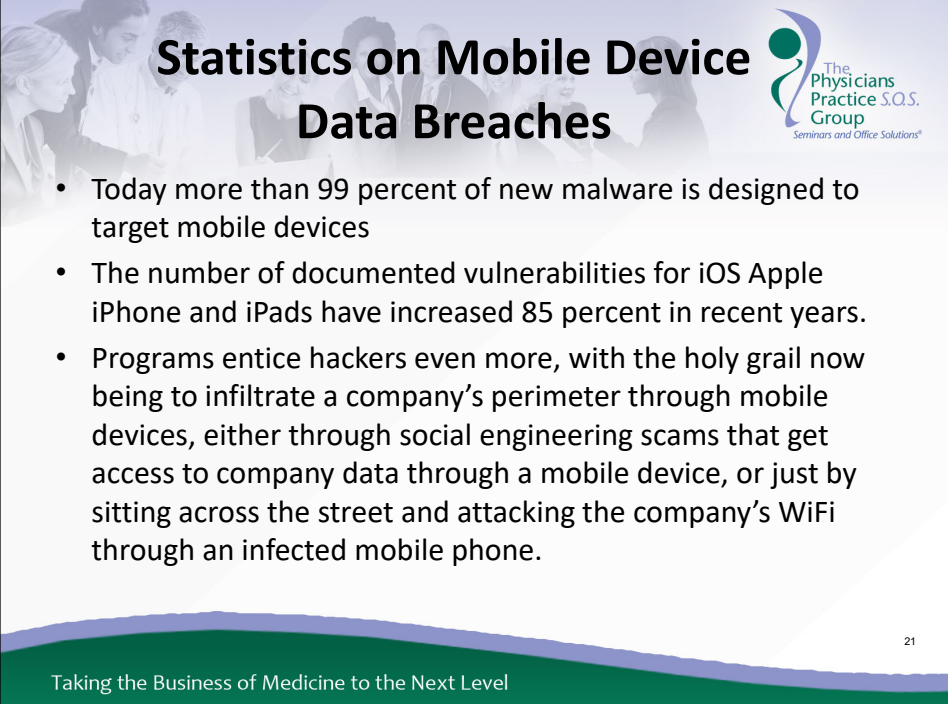
Biggest Risk Areas: Mobile Devices and Laptops




- One laptop is stolen every 53 seconds.
- 70 million smartphones are lost each year, with only 7 percent recovered.
- 4.3 percent of company-issued smartphones are lost or stolen every year.
- 80 percent of the cost of a lost laptop is from data breach.
- 52 percent of devices are stolen from the office/workplace, and 24 percent from conferences.

20

Taking the Business of Medicine to the Next Level



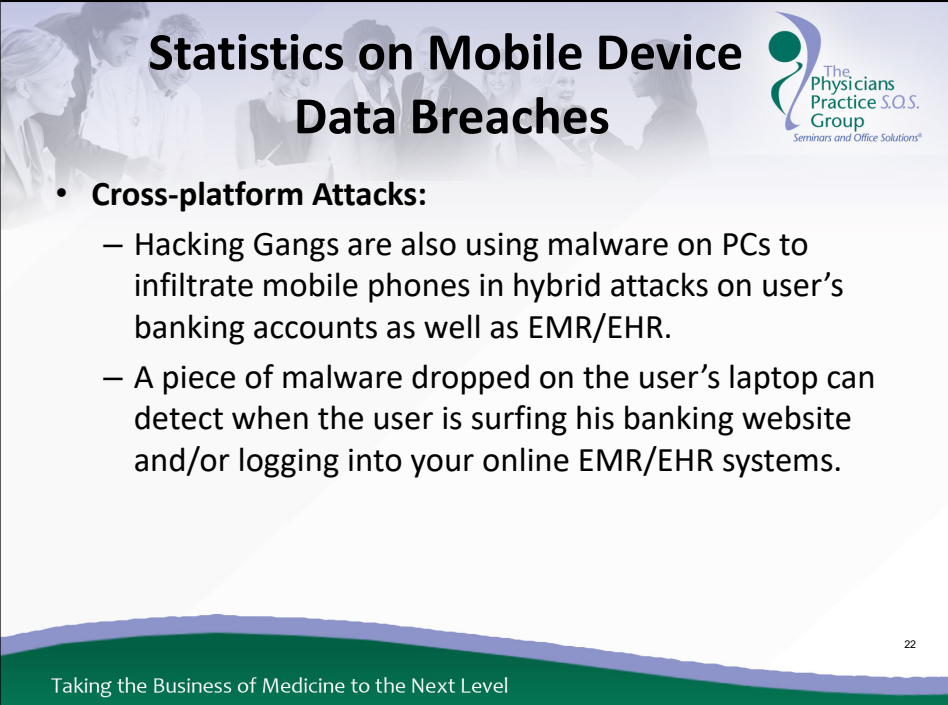
Statistics on Mobile Device Data Breaches




- Today more than 99 percent of new malware is designed to target mobile devices
- The number of documented vulnerabilities for iOS Apple iPhone and iPads have increased 85 percent in recent years.
- Programs entice hackers even more, with the holy grail now being to infiltrate a company's perimeter through mobile devices, either through social engineering scams that get access to company data through a mobile device, or just by sitting across the street and attacking the company's WiFi through an infected mobile phone.

21

Taking the Business of Medicine to the Next Level




Statistics on Mobile Device Data Breaches




- **Cross-platform Attacks:**
 - Hacking Gangs are also using malware on PCs to infiltrate mobile phones in hybrid attacks on user's banking accounts as well as EMR/EHR.
 - A piece of malware dropped on the user's laptop can detect when the user is surfing his banking website and/or logging into your online EMR/EHR systems.

22

Taking the Business of Medicine to the Next Level




The Three Most Common Mobile Security Breaches



- **Malware** -Even more malicious malware might take over a phone's data connection, send spam emails, infect other devices on the network or even harvest passwords.
- This is an increasing problem as hackers begin to target mobile devices instead of desktop computers.
- Your staff must be as careful with downloading software as they are with laptops and desktop.

23

Taking the Business of Medicine to the Next Level



The Three Most Common Mobile Security Breaches



- **Unsecured networks** -Another danger is the rogue Wi-Fi network, set up by hackers to trap people logging on at airports, stations or coffee shops. This has been common in Asia but is less often used, so far, in North America or Europe.
- Either teach your staff to treat Wi-Fi access with caution – or give them unlimited data contracts so they don't need to use such open access points.

24

Taking the Business of Medicine to the Next Level



The Three Most Common Mobile Security Breaches



- **Device loss and theft** -The most common mobile “breach” is a staff member leaving a phone on the bus or in a taxi. This could allow access to company data but is more likely to lead to a flurry of expensive foreign calls and the loss of the device.
- Password protection helps limit the costs and dangers of losing a phone.
- If your business relies on sensitive data then think about software that allows remote control of phones so you can delete files or even disable the phone permanently. Failing that, make sure staff use passwords to protect their devices and consider further passwords for access to important applications.

25

Taking the Business of Medicine to the Next Level




Preparation and Diligence are Key




- Regardless of an organization’s security posture, there is no perfect security. On the other hand, there is no excuse not to implement fundamental security best practices.
- All organizations, regardless of size, must plan for inevitable attacks and loss of (or loss of access to) critical data.
- By recognizing risks, planning ahead and instilling a culture of security and privacy in the entire organization, losses and their impact can be minimized.

26

Taking the Business of Medicine to the Next Level




Key Avoidable Causes For Incidents




- Lack of a complete risk assessment, including internal, third-party and cloud-based systems and services
- Not promptly patching known / public vulnerabilities, and not having a way to process vulnerability reports
- Misconfigured devices / servers
- Unencrypted data and/or poor encryption key management and safeguarding
- Use of end of life (and thereby unsupported) devices, operating systems and applications
- Employee errors and accidental disclosures - lost data, files, drives, devices, computers, improper disposal
- Failure to block malicious email
- Social online exploits

27

Taking the Business of Medicine to the Next Level




Device Encryption Options




- Data and device encryption are critical pieces of an overall mobile security initiative. Implementing encryption is vital to ensuring that sensitive data is kept safe.
- The major mobile operating systems all have different data and device encryption options. Enable the right features to keep devices and data safe.

28

Taking the Business of Medicine to the Next Level



Device Encryption Options




- **Android** runs applications in a kernel-level application sandbox, and at the foundation of Android is a Linux kernel.
- **Windows Phone** uses the Unified Extensible Firmware Interface facilities for Secure Boot, which ensures that devices do not load rooted or unauthorized system images.
- **Apple iOS** applications are sandboxed from each other, using what's called "Completed" meaning they do not share data with each other on the device but only protects email and attachments
- **BlackBerry*** uses BlackBerry Balance, which allows organizations to create isolation between personal and work environments on a device.


**BlackBerry is the currently the only mobile OS with a Federal Information Processing Standard 140-2 security rating.*

29

Taking the Business of Medicine to the Next Level



Mobile Encryption Options Built-in vs. Manual Encryption



- "Built-in" encryption methods mean properly configuring automatic encryption that comes included with the mobile device itself, it will tend to minimize human error in most cases.
- "Manual" encryption relies on the user to encrypt data manually, then we are introducing a dependency on user behavior.

30

Taking the Business of Medicine to the Next Level



Security Essentials




- The Department of Health and Human Services released its own voluntary cybersecurity guidance in the fall, security leaders pointed to the absence of a section dedicated to mobile security.
- It also recommends 10 Cybersecurity Practices to help mitigate these threats


<https://www.hhs.gov/about/news/2018/12/28/hhs-in-partnership-with-industry-releases-voluntary-cybersecurity-practices-for-the-health-industry.html>

31

Taking the Business of Medicine to the Next Level



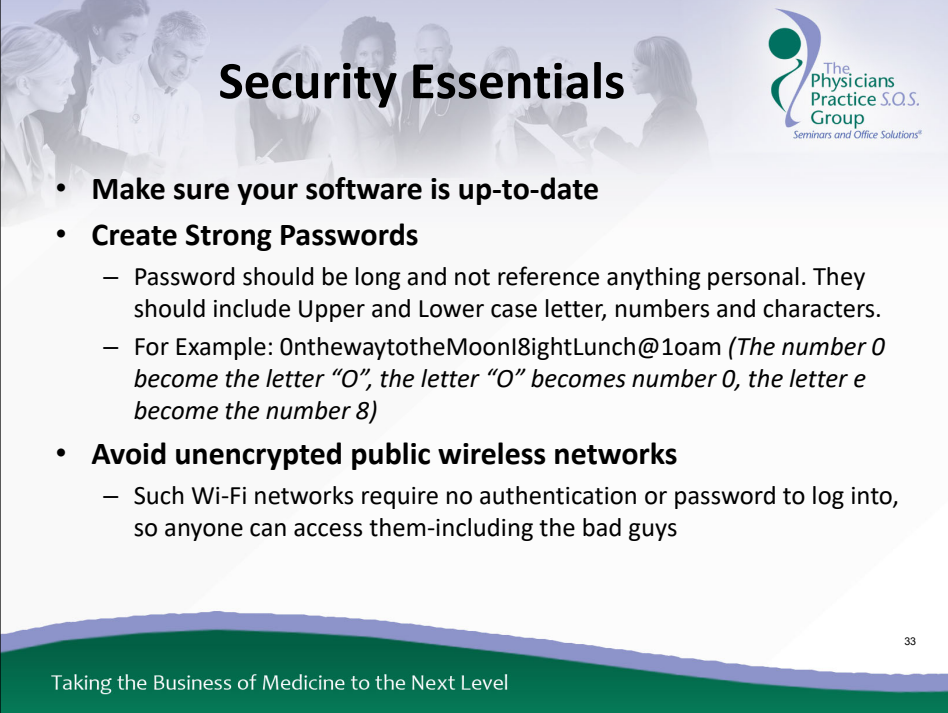
Security Essentials



- **Key Elements In Security:**
 - Screen, passcode and sim locks
 - Erase media cards/factory reset of outdated devices
 - Remote wipe functionality to sanitize your device if lost

32

Taking the Business of Medicine to the Next Level



Security Essentials

- **Make sure your software is up-to-date**
- **Create Strong Passwords**
 - Password should be long and not reference anything personal. They should include Upper and Lower case letter, numbers and characters.
 - For Example: OnthewaytotheMoon!8ightLunch@1oam (*The number 0 become the letter "O", the letter "O" becomes number 0, the letter e become the number 8*)
- **Avoid unencrypted public wireless networks**
 - Such Wi-Fi networks require no authentication or password to log into, so anyone can access them-including the bad guys

33

Taking the Business of Medicine to the Next Level



Security Essentials

- **Don't mess with the security settings**
 - Most of the default browser settings in Android, iPhone, and Blackberry phones are fairly secure out of the box.
- **Paying to access a Wi-Fi network doesn't mean it's secure**
- **URLs beginning with 'https:' are safer (but not foolproof)**
- **Use VPN**
 - If you have access to a VPN (virtual private network), use it. A VPN provides secure access to an organization's network and allows you to get online behind a secure layer that protects your information.

34

Taking the Business of Medicine to the Next Level



Security Essentials



- **Turn off cookies and autofill**
 - If your mobile device automatically enters passwords and login information into Websites you visit frequently, turn that feature off.
- **Watch your apps!**
 - You should be selective about the apps you download, particularly in the Android market, because "the Android app market is a little bit more open," without the strict developer guidelines found in Apple's App Store. Do some due diligence before downloading apps. Make sure that you trust the developer and have taken the time to review some of comments.

35

Taking the Business of Medicine to the Next Level



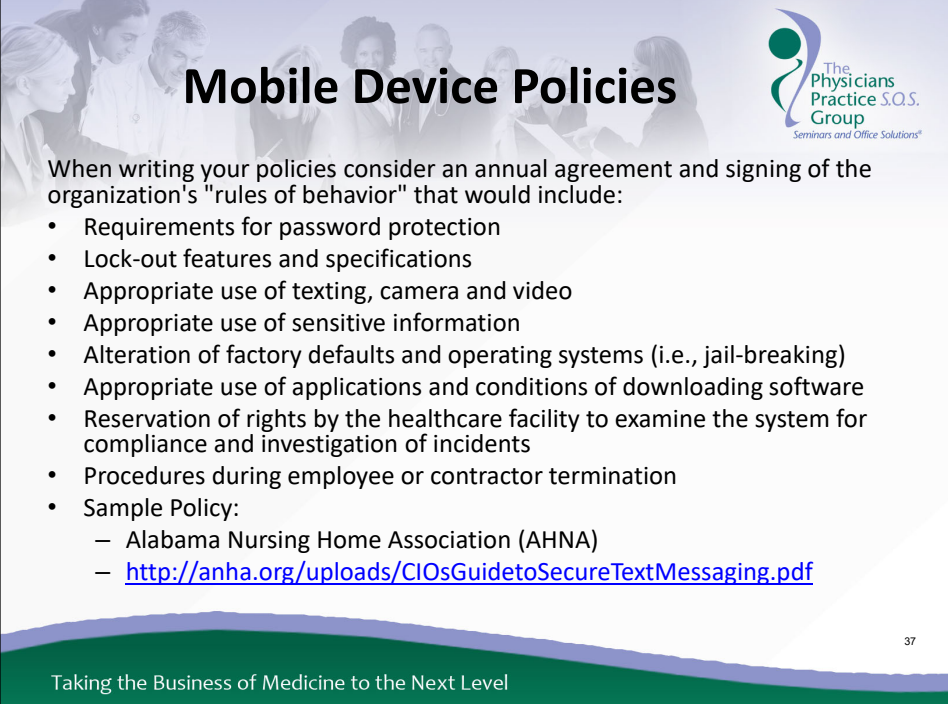
Mobile Device Policies




- Mobile Devices come in a variety of forms, processing capabilities, and wireless accessibility
 - Policies should include but are not limited to, laptop computers, smart phones, USB thumb drives, external hard drives, tablet computers (e.g., iPad, Motorola Xoom), and even e-readers like the Kindle or the Nook.

36

Taking the Business of Medicine to the Next Level



Mobile Device Policies

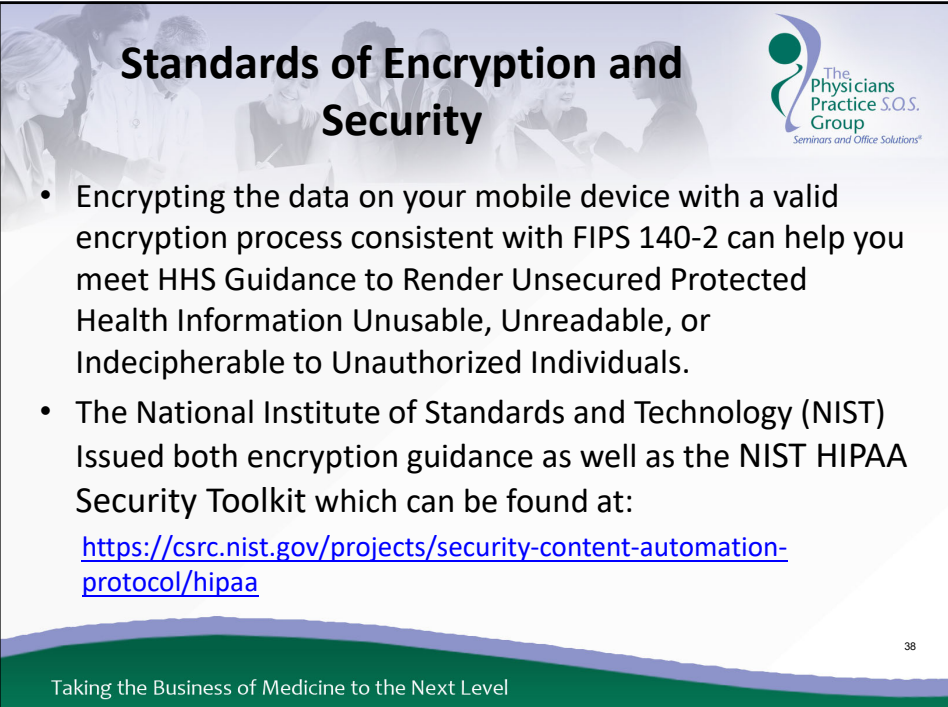


When writing your policies consider an annual agreement and signing of the organization's "rules of behavior" that would include:


- Requirements for password protection
- Lock-out features and specifications
- Appropriate use of texting, camera and video
- Appropriate use of sensitive information
- Alteration of factory defaults and operating systems (i.e., jail-breaking)
- Appropriate use of applications and conditions of downloading software
- Reservation of rights by the healthcare facility to examine the system for compliance and investigation of incidents
- Procedures during employee or contractor termination
- Sample Policy:
 - Alabama Nursing Home Association (AHNA)
 - <http://anha.org/uploads/CIOsGuidetoSecureTextMessaging.pdf>

37

Taking the Business of Medicine to the Next Level




Standards of Encryption and Security




- Encrypting the data on your mobile device with a valid encryption process consistent with FIPS 140-2 can help you meet HHS Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.
- The National Institute of Standards and Technology (NIST) Issued both encryption guidance as well as the NIST HIPAA Security Toolkit which can be found at:
<https://csrc.nist.gov/projects/security-content-automation-protocol/hipaa>

38

Taking the Business of Medicine to the Next Level



HIPAA Secured Messaging App's




- Backline via DrFirst
- Inpriva
- QliqSOFT
- pMD
- Spectrum Secure Delivery (used by some answering services)


We do not endorse provide any guarantee on the use of any software programs mentioned in this webinar; it is up to you to investigate any software, app or program.

39

Taking the Business of Medicine to the Next Level



Most Recent Breaches Reported




- **February 1, 2018:** Five breaches add up to millions in settlement costs for entities that failed to heed HIPAA's risk analysis and risk management rules
 - Fresenius Medical Care North America (FMCNA) has agreed to pay \$3.5 million to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and to adopt a comprehensive corrective action plan, in order to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. FMCNA is a provider of products and services for people with chronic kidney failure with over 60,000 employees that serves over 170,000 patients. FMCNA's network is comprised of dialysis facilities, outpatient cardiac and vascular labs, and urgent care centers, as well as hospitalist and post-acute providers.

40

Taking the Business of Medicine to the Next Level

Other Large Healthcare Data Breaches Reported in 2018




- Other largest healthcare data breach by some distance – was the 538,127-record breach at the Baltimore, MD-based healthcare provider LifeBridge Health Inc. The breach was reported in May 2018, although it occurred more than a year and a half earlier in September 2016, when malware was installed on its server that hosts electronic health records.
- In addition to names and contact information, clinical and treatment information, insurance information, and, in some instances, Social Security numbers, were compromised. The scale of the breach and the types of information exposed makes it one of the most serious healthcare data breaches discovered in 2018.

41

Taking the Business of Medicine to the Next Level

Largest Healthcare Data Breaches Reported in May 2018



As the table below shows, hacks and IT incidents were behind the most serious breaches in May.

Breached Entity	Entity Type	Records Breached	Breach Type
LifeBridge Health, Inc	Healthcare Provider	538127	Hacking/IT Incident
The Oregon Clinic, P.C.	Healthcare Provider	64487	Hacking/IT Incident
Dignity Health	Healthcare Provider	55947	Unauthorized Access/Disclosure
Aultman Hospital	Healthcare Provider	42625	Hacking/IT Incident
Holland Eye Surgery and Laser Center	Healthcare Provider	42200	Hacking/IT Incident
USACS Management Group, Ltd.	Business Associate	15552	Hacking/IT Incident
Florida Hospital	Healthcare Provider	12724	Hacking/IT Incident
Aflac	Health Plan	10396	Hacking/IT Incident
Cerebral Palsy Research Foundation of Kansas, Inc.	Healthcare Provider	8300	Unauthorized Access/Disclosure
Associates in Psychiatry and Psychology	Healthcare Provider	6546	Hacking/IT Incident

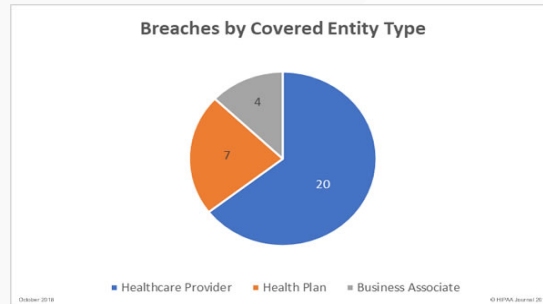
42

Taking the Business of Medicine to the Next Level

Breaches By Covered Entity Type



- In terms of the number of incidents, healthcare providers were the worst hit by data breaches in October 2018 with 20 reported breaches, followed by health plans/health insurers with 7. Four HIPAA business associate breaches were reported, three of which were by the same business associate



43

Taking the Business of Medicine to the Next Level


Covered Entities Data Breaches: Real World Cases




- \$387,200 St. Luke's operates the Institute for Advanced Medicine, for careless handling of HIV information. St. Luke's provides comprehensive health services to persons living with HIV or AIDS and other chronic diseases. St. Luke's is 1 of 7 hospitals that comprise the Mount Sinai Health System (MSHS).
- \$1.7M settlement with WellPoint for lack of administrative and technical safeguards surrounding an online application database. HHS also found a lack of sufficient policies and procedures. Breach affected over 600,000 individuals.
- \$1.2M settlement with health plan for failing to erase ePHI stored on photocopiers before returning the machines to leasing agent. HHS also cited failure to implement policies and procedures, and failure to perform adequate risk assessment. Breach affected 344,579 individuals.
- \$1.5M settlement with Mass. Provider who had unencrypted personal laptop stolen, contained PHI of more than 500 patients and research subjects, including patient prescription and clinical information.

44

Taking the Business of Medicine to the Next Level



What Happen After a Data Breaches:




- What happens when someone's health information is illegally sold or fraudulently used?


Bad credit: Say an attacker sells your patient's information to someone who racks up a bunch of unpaid medical bills, and opens up credit cards or other credit purchases under your patient's name and social security number. This can seriously ruin the real patient's credit. Bill collectors could come knocking. The victim could be denied a job due to bad credit and his insurability could be affected.

45

Taking the Business of Medicine to the Next Level




Protocols - In The Event Of A Breach




- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.
- An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors.

46

Taking the Business of Medicine to the Next Level




Protocols - In The Event Of A Breach




- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

47

Taking the Business of Medicine to the Next Level




Protocols - In The Event Of A Breach




- Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media.
 - Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.

48

Taking the Business of Medicine to the Next Level



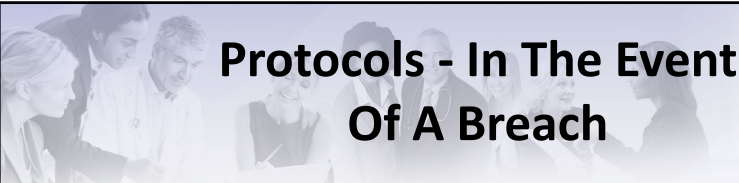
Protocols - In The Event Of A Breach




- Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.

49

Taking the Business of Medicine to the Next Level




Protocols - In The Event Of A Breach




- These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include:
 - A brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

50

Taking the Business of Medicine to the Next Level



Protocols - In The Event Of A Breach




The Physicians Practice S.O.S. Group
Seminars and Office Solutions®


- Covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out the breach form.
 - Breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

51

Taking the Business of Medicine to the Next Level



Fines



The Physicians Practice S.O.S. Group
Seminars and Office Solutions®

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	\$100 per violation, with an annual maximum of \$25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	\$50,000 per violation, with an annual maximum of \$1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	\$1,000 per violation, with an annual maximum of \$100,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	\$10,000 per violation, with an annual maximum of \$250,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
HIPAA violation is due to willful neglect and is not corrected	\$50,000 per violation, with an annual maximum of \$1.5 million	\$50,000 per violation, with an annual maximum of \$1.5 million

52

Taking the Business of Medicine to the Next Level

3 major HIPAA fines so far in 2018



1. MD Anderson slapped with \$4.3M penalty for HIPAA violations

An HHS administrative law judge upheld an HHS Office for Civil Rights finding requiring the University of Texas MD Anderson Cancer Center in Houston to pay \$4,348,000 in civil penalties for HIPAA violations related to the organization's encryption policies, HHS confirmed June 18. The violations include three data breaches in 2012 and 2013, which exposed health information of more than 33,500 people.

2. HHS to collect millions in settlement costs resolving 5 breaches at a single entity

Waltham, Mass.-based Fresenius Medical Care North America agreed to pay the HHS Office for Civil Rights \$3.5 million to settle allegations it violated HIPAA rules after data breaches at five sites in 2012, HHS confirmed Feb. 1. The healthcare company's network comprises dialysis facilities, outpatient cardiac and vascular labs, urgent care centers, and hospitalist and post-acute providers.

3. HHS imposes \$100K fine on shuttered facility for 2015 HIPAA violation

A receiver appointed to liquidate the assets of Filefax, a now-closed medical records management company, will pay \$100,000 out of the receivership estate to the HHS Office for Civil Rights to settle potential HIPAA violations related to a 2015 breach, HHS confirmed Feb. 13. The civil rights office determined Filefax had disclosed information of 2,150 patients by leaving medical records at a shredding and recycling facility.

53

Taking the Business of Medicine to the Next Level

Other Large HIPAA fines



1. Advocate Health System (Downers Grove, Ill.): \$5.55 million

The latest HIPAA settlement is also the biggest. In the first week of August, Advocate Health System agreed to settle HIPAA violation claims related to three data breaches that occurred in 2013. In total, the three incidents compromised the protected health information of 4 million individuals. [Read more](#)

2. NewYork-Presbyterian Hospital and Columbia University (New York City): \$4.8 million

In May 2014, these organizations agreed to pay a combined \$4.8 million to settle charges from a 2010 breach when a Columbia-based physician attempted to deactivate a personal computer connected to the NewYork-Presbyterian network that contained patient information. The attempt left protected health information accessible on internet search engines. While separate entities, the organizations have an affiliation where Columbia professors work as attending physicians at NewYork-Presbyterian, and the two share a data network and firewall. NewYork-Presbyterian paid \$3.3 million and Columbia paid \$1.5 million. [Read more](#)

3. Cignet Health (Prince George's County, Md.): \$4.3 million

HHS determined Cignet Health violated HIPAA by denying 41 patients' access to their medical records. The HIPAA Privacy Rule requires covered entities provide patients copies of records within 30 dates of a patient's request. The agency investigated Cignet Health, and the system allegedly refused to respond to OCR's demands to give patients the records. [Read more](#)

4. Triple-S (San Juan, Puerto Rico): \$3.5 million

This insurance holding company settled alleged widespread noncompliance with HIPAA throughout its subsidiaries. The OCR investigated Triple-S after receiving multiple breach notifications. [Read more](#)

5. University of Mississippi Medical Center (Jackson): \$2.75 million

The OCR launched an investigation into UMMC in March 2013 after the health system reported a missing password-protected laptop that contained protected health information. The breach affected approximately 10,000 individuals. The investigation found UMMC did not notify each individual whose information was compromised, nor did it initiate any risk management activity until after the breach. [Read more](#)

54

Taking the Business of Medicine to the Next Level

Why Create (and follow) Mobile Device Policies



- HIPAA allows providers to communicate with patients and with other providers and to share ePHI using mobile devices as long as “reasonable safeguards” are applied when doing so.
- However, there is no specific requirement to have or not to have a social media/networking and mobile device policy.
- Given today’s environment of near-constant use of social media/networking, common access to PHI via mobile and highly portable devices, and where the vast majority of reported breaches stem from inappropriate safeguarding of ePHI, there is not any clear direction from the government which has resulted in a covered entity’s failure to implement the reasonable safeguards required under HIPAA.

55

Taking the Business of Medicine to the Next Level

Best Practices Moving Forward



- **Data security is fundamental**
 - Conduct data security review often
- **Plan ahead**
 - Create a plan to review your data security status and policies and create routine processes to access, handle and store the data safely as well as archive unneeded data.
- **Know what data you have**
 - Know what data you have and what levels of protection are required to keep the data both confidential and safe from loss
- **Scale down the data**
 - Keep only the data you need for routine current business, safely archive or destroy older data
- **Lock up!**
 - Physical security is the key to safe and confidential computing. All the passwords in the world won't get your laptop back if the computer itself is stolen. Back up the data to a safe place in the event of loss.

56

Taking the Business of Medicine to the Next Level



Best Practices Moving Forward

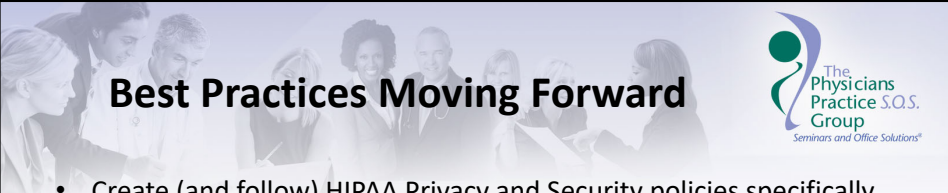


Seminars and Office Solutions®


- Require providers to register their mobile devices if Bring Your Own Device (“BYOD”) is allowed
- Require use of passwords or other use authentication
- Install and enable encryption for ePHI including text or SMS messages
- Install and activate remote wiping and/or remote disabling ability
- Disable and do not install or use file sharing applications
- Install and enable a firewall
- Install and enable security software (and update it)
- Do not share ePHI over public Wi-Fi
- Delete all stored ePHI before discarding or reusing the mobile device.

57

Taking the Business of Medicine to the Next Level



Best Practices Moving Forward




Seminars and Office Solutions®

- Create (and follow) HIPAA Privacy and Security policies specifically addressing the exchange of PHI using mobile devices and social media
- Ensure all staff and personnel receive copies of your HIPAA Privacy and Security Manuals, including policies relating to mobile devices and social media
- Impose appropriate safeguards on use of both mobile devices and social media
- Consider annual testing for employees
- Audit to ensure staff and personnel with access to ePHI on mobile devices have implemented the appropriate safeguards

58

Taking the Business of Medicine to the Next Level



Questions?

59

Taking the Business of Medicine to the Next Level



The Physicians Practice S.O.S. Group
Seminars and Office Solutions®

- **We offer services in the following areas of Practice Management and Operation:**
 - Practice Assessment, Education and Management Oversight
 - New Practice Set-up
 - Baseline Chart Audits
 - One-on-one Physician Training/Education
 - MACRA: MIPS and APM's Consulting Services
 - IRO (Government Approved Independent Review Organization) Services
 - HIPAA, OSHA, and OIG Compliance Documentation, Planning, and Implementation
- **We also offer a series of seminars for Physicians and Staff**

60

Taking the Business of Medicine to the Next Level



Thank you for attending!!

Visit us online: www.ppsosgroup.com
You can contact us at: info@ppsosgroup.com
770.333.9405

FIND US ON
Facebook, LinkedIn, Twitter, Fix my Practice Blog and YouTube :



<https://www.facebook.com/pages/The-Physicians-Practice-SOS-Group/280246238670673>
LinkedIn: The Physicians Practice S.O.S. Group
<https://twitter.com/PPSOSGRP>
Blog: <http://www.ppsosgroup.com/fixmypracticeblog/>
<http://www.youtube.com/user/ppsosgroup>

61

Taking the Business of Medicine to the Next Level