

Privacy / Security Breach Response

2023 Healthcare Enforcement Compliance Conference

Washington, D.C.

November 5, 2023

Joan Podleski, CCEP, CHRC, CHC, CHPC
VP & Chief Privacy Officer
Children's Health
Dallas, Texas
Office: 214.456.6068
joan.podleski@childrens.com

Gina G. Greenwood, JD, CIPP/US, Partner
Chair Data Privacy & Security Group
Chair Data Breach Response Team
gina.greenwood@nelsonmullins.com
Mobile: 404.909.0665 | Office: 404.322.6790
Data Breach 24/7/365 Hotline: 404.322.6767
NMDataResponseTeam@nelsonmullins.com



1

Introductions




Joan Podleski, CCEP, CHRC, CHC, CHPC
VP & Chief Privacy Officer
Children's Health
Dallas, Texas
Office: 214.456.6068
joan.podleski@childrens.com




- Joan has been in the academic health care and research administration field for over 30 years.
- Joan is currently the Chief Privacy Officer for Children's Health System of Texas - which is the pediatric partner to UTSW.
- Prior to that, she served as Director of the Institutional Ethics & Compliance Program at Duke University, where she was responsible for the oversight program related to all compliance issues for the University and also served as the HIPAA Privacy Officer for the academic units of Duke.
- Prior to that, Joan spent more than 20 years at Washington University at St. Louis where she held multiple positions – including HIPAA Privacy Officer and Assistant Chancellor for Clinical Affairs.

2


2



Badger



Eспен




















Atticus

2022 key metrics

children'shealth[®]

Data reflects totals from 2022, ending Dec. 31, 2022, unless otherwise noted.

 288,085 <small>total patients seen</small>	 5.6 million <small>square feet</small>	 9,051 <small>employees</small>
<small>patient visits</small> 919,535 553,505 182,735 <small>total patient visits dallas plano</small>	 562 <small>licensed beds</small>	50+ <small>pediatric specialty and subspecialty programs</small>
 23,802 <small>surgeries</small>	 237 <small>school-based telehealth sites</small>	 280,212 <small>outpatient visits</small>
 33 <small>solid organ transplants</small>	 330 <small>school-based telebehavioral health sites*</small>	 1,202 <small>medical and dental staff</small>
 524 <small>cardiac surgical procedures</small>	 9 <small>facility therapy dogs</small>	110 years <small>of dedication to making life better for the children of North Texas and beyond</small>
 14,810 <small>NICU patient days</small>	 52 <small>locations offering specialty care</small>	146,206 <small>ancillary visits</small>
 \$4.6 billion <small>gross revenue</small>	 \$28.2 million <small>charity care**</small>	 156,178 <small>total emergency room visits</small>
97,443 <small>dallas</small>		58,735 <small>plano</small>

*2022 sites are funded and administered by the Texas Children's Hospital system. **Total value of charity care.

3

Introductions



GINA GREENWOOD,
JD, CIPP/US



(404) 322-6790 o
(404) 909-0665 c

- Chair of Data Privacy, Security, & Breach Practice Group
- 20 years of experience in healthcare defense and compliance: EMTALA, HIPAA, Immediate Jeopardy, Survey Response, Government Investigation, etc.
- Handled 1000's of security incidents & breaches
 - 100% success rate
 - Cyber Legal Panel: Beazley, ... AIG, Resilience, Coalition, Corvus
- Gina has been recognized by Chambers USA and by *Georgia Trend Magazine* as a Legal Elite.
- She is listed in Best Lawyers in America (2017 - 2023).

4

**Nelson Mullins
24/7/365
Breach
Response
Intake
Team**

Nelson Mullins 24/7/365 Breach Response Intake Team

In the event of an incident, call our 24/7 Breach Hotline at 404.322.6767 or email NMDDataResponseTeam@nelsonmullins.com. You may also call and text the cell phones of the individual Team Members below. The Breach Intake Team is supported by over 50 breach response, privacy, and security industry specialists across Nelson Mullins U.S. footprint and globally through strategic legal partnerships around the world.

 Gina Greenwood, JD, CIPP/US Partner, Chair of Cyber Security, Privacy and Breach Practice Group Georgia gina.greenwood@nelsonmullins.com M: 404.505.0665	 Brad Moody, JD, CIPP/US, CPP/IC Partner, Co-Chair of the Breach Response Team Mississippi, Alabama brad.moody@nelsonmullins.com M: 601.278.2918	 Will Horkan, J.D., CIPP/US Of Counsel, Breach Team Georgia will.horkan@nelsonmullins.com T: 478.387.0826
 Ashleigh Smith, JD, CIPP/US Senior Associate, Breach Team Marketing Liaison Georgia ashleigh.smith@nelsonmullins.com M: 478.600.8823	 Anil Cavazos, JD Associate, Breach Team Florida anil.cavazos@nelsonmullins.com M: 921.228.2899	 Helen Fernandez Administrative Assistant Georgia helen.fernandez@nelsonmullins.com T: 478.387.0793

NMDDataResponseTeam@nelsonmullins.com is distributed to all Intake Team Members.



1000+
attorneys and professionals

33
offices in 17 states and Washington, D.C.

100+
diversified practice areas

Specialty Areas and Practice Groups:
Healthcare, Automotive, Public Sector, Banking, Retail & Manufacturing



15+ Professionals
with Specialty IT/Privacy Certifications
(CIPP/US, CIPP/C, CIPP/E, C/PM)



ISO/IEC 27001:2013 certified
SOC 2 TYPE 2 with HITRUST controls audits

5

**Featured
Privacy,
Security,
& Incident
Response
Team
Members**

Sample of Privacy, Security, & Breach Response Team Members: Subject Matter / Industry Specialists



 William J. O'Connell, J.D., CIPP/US Partner, Chair of Cyber Security, Privacy and Breach Practice Group Georgia	 Lisa Marie Al-Dabbas, JD, CIPP/US Of Counsel, Breach Team Minnesota, Alabama	 William J. O'Connell, J.D., CIPP/US Of Counsel, Breach Team Alabama, VA	 Ashleigh Smith, JD, CIPP/US Senior Associate, Breach Team Marketing Liaison Georgia	 Patrick Ellis - Full-Field, Esq., CIPP/US Senior Counsel, Breach Team Denver, CO	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Security, Privacy Denver, CO	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Security, Privacy Denver, CO
 Craig Williams, J.D. Partner Atlanta, GA	 Robert J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Of Counsel, Breach Team Florida, Tennessee, Virginia, South Carolina, North Carolina	 Gabriel Torres, J.D. Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Raleigh, NC	 John D. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Oklahoma, PA	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Columbia, SC
 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Nashville, TN	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Nashville, TN	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Nashville, TN	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Nashville, TN	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Nashville, TN	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Nashville, TN	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Nashville, TN
 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Columbia, SC	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.
 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Atlanta, GA	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Dallas, TX	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Charlotte, NC	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team New York, NY	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Tallahassee, FL
 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Atlanta, GA	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Dallas, TX	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Washington, D.C.	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Charlotte, NC	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team New York, NY	 William J. O'Connell, J.D., CIPP/US Senior Counsel, Breach Team Tallahassee, FL

Atlanta • California • Colorado • District of Columbia • Florida • Georgia • Maryland • Massachusetts • Minnesota • Mississippi • Missouri • New York • North Carolina • Ohio • South Carolina • Texas • Virginia • Washington, D.C. • West Virginia

6

CYBER ATTACKS

Cyber attacks are in the headlines everyday. We are under constant attack by hackers trying to gain access to our computers and networks!

ChatGPT takes over at lightning speed - 2022-23

Ransomware cases up 400% in 2020 - Ransoms lead \$30 million plus demands

MoveIT – biggest breach of 2023 year

Uber Data Breach Exposed Personal Information of 20 Million Users

By Bloomberg April 12, 2018

Fundraising Platform Data Security Incidents Affects 55,000 Entities; millions of letters are sent

- 2020

Ransomware attack on an Alabama hospital alleged to have caused a baby death

-2021

Colonial Pipeline Allegedly Pays

Darkside Following Ransomware Attack

WARS:
Ukraine – Russia
Israel – Gaza



7

7

TRIAGE DILEMMA FOR PRIVACY / COMPLIANCE OFFICER

TRIAGE THE ISSUE

- Scope the Problem
 - CE vs. BA? Data Owner vs. Controller?
- Investigate
 - Assess Contractual Obligations
 - Live Tech Connections?
 - Direct Impact on Environment / Patient Population?
 - Follow-up
- Insurance Claim?



RESPOND AS NEEDED

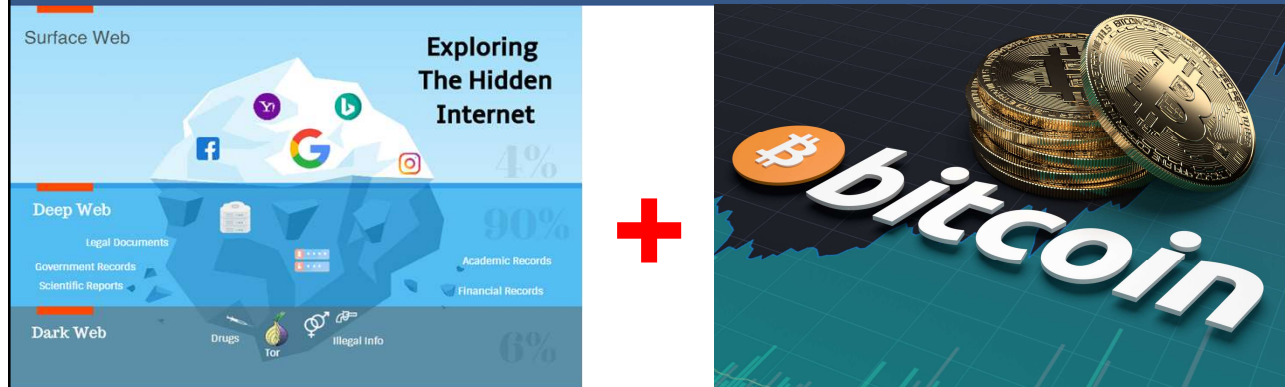
- Mitigate
- Sanction
- Documentation of the HIPAA Notice Assessment
 - Notify
 - Patients
 - Consumer
 - OCR
 - AGs, etc.
- Policies and Procedures – Review and Revise
- Retraining
- Security Rule Risk Assessment

8



8

Cyber Attacks: Why Now? Why the Increase?

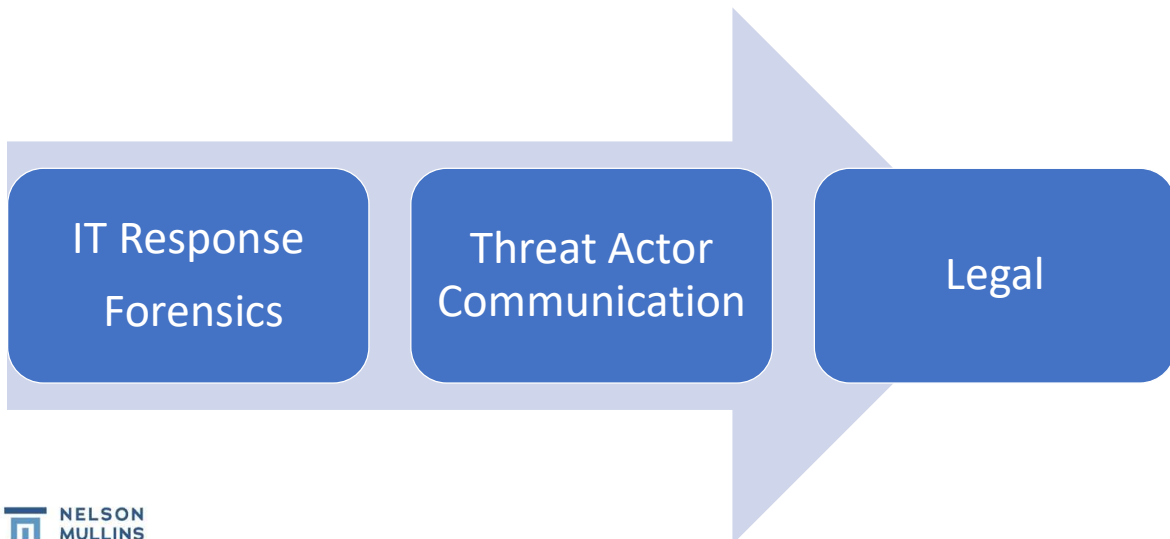


= Increase in Cyber Attacks!!

9

9

Incident Response Plan of Ransomware



10

10



WHAT TO EXPECT? RANSOMWARE ACTION STEPS (Many of these happen concurrently and/or not necessarily in this order)

- Network outage/computers malfunctioning
- Encryption / Ransom notes found
- Employees calling IT, CISO for support; C-Suite calling for details.
- CISO institutes Incident Response Plan (likely takes servers offline and prepares for the domino effect of a network outage) and reports to the appropriate parties.
- Insurance notified
- Contracts are executed: Breach Counsel (outside legal) engaged and Forensics are engaged by attys under privilege.
 - - Legal puts the appropriate departments on legal hold for preservation of forensic evidence.
- Endpoint Monitoring Software Deployed:
 - End Point monitoring reviewed: Evaluates the network triages the primary servers/critical systems for access and exfiltration.
- Specialized hostage negotiators are brought in by cyber attys to communicate with the threat actor for multiple reasons. Decisions are made re: whether to pay or not.
- NOTE: MUST CHECK OFAC and file IC3 Report before ransom can be paid. Unlikely that it can be paid right now with the World in flux.
- Forensics simultaneously investigates and gives a preliminary update and provides other indicators of compromise; offers advice on booting the TA out of the system.

11

RANSOMWARE ACTION STEPS (Continued)

- Once determined what data the TA had access to (and whether it was exfiltrated, if possible),
- Breach Atty assists in evaluating whether PHI, PCI or other Personally Identifiable Information is involved and whether there are reporting obligations to individuals/regulators or pursuant to contracts.
- Forensics continues investigation and provides more details of the intrusion and narrows the scope of what data is at issue.
- Breach Counsel assists in practical issues--i.e. Can we process payroll? What do we tell the public and employees? Should we address the gossip on Facebook about the network shut down?
- Forensics works with CISO/IT to clean up/rebuild the network from back ups or from decryption codes if the ransom is paid or are decryption codes available; systems are stood back up and brought back online as able. Evidence is preserved.
- Forensics provides a final report of the who, what, when, where, and how, as best they can, based on the evidence available.
- Breach Counsel assists in finishing the notification process—drafting individual notice letters, procuring ID Theft Protection codes if SSNs, etc. at issue, setting up a tollfree call center, providing FAQs for the call center, handling escalation calls, notifying regulators and other contractual obligations.
- Etc.



12

PRIOR TO MAKING A RANDOM PAYMENT: MUST UNDERSTAND LEGAL REPORTING / NOTICE OBLIGATIONS

- **File the IC3 Report (early on)**
- **Check the OFAC list to ensure not paying terrorists**
- **Check to ensure not dealing with prohibited (embargoed or sanctioned) countries.**
- **Notify your Cyber Carrier and Get Approval**



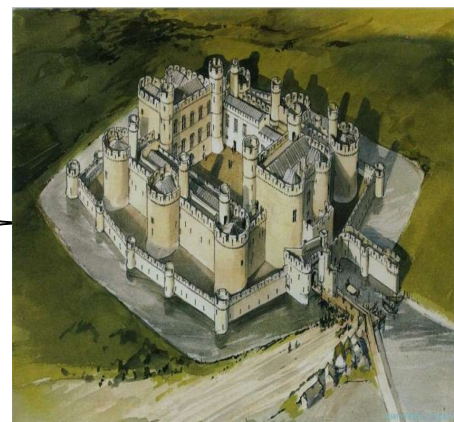
9



13

GOOD NEWS: SECURITY RISK MANAGEMENT DECREASES THE RISK OF EVENT

USER TRAINING: ESTABLISHING SAFE HABITS
INCIDENT RESPONSE / EMERGENCY PREPAREDNESS PLAN
PRIVACY AND SECURITY POLICIES / PROCEDURES FACTORING IN APPLICABLE LAW
TESTING SYSTEMS / TABLETOPS
CYBER LIABILITY INSURANCE
BACK-UP FILES / CONTAINMENT / BLOCKING
MANAGING ADMIN AND ACCESS RIGHTS – MULTIFACTOR AUTHENTICATION
VENDOR MANGEMENT
END POINT MONITORING / ANTI-MALWARE / ANTI-VIRUS SOFTWARE
WEEKLY PATCH UPDATES: WORKSTATION & SERVER
FIREWALLS / ENCRYPTION
DATA MAPPING / DEVICE MANAGEMENT



14

Think

Before You Click!



PHISHING SCAM EDUCATION IS KEY



11

15

Educate About Wire Transfer Scams

- This email appears to be from a familiar company executive. The executive claims to be unable to talk with you in person but needs you to wire or send funds immediately.
- A hacker may be in the CEO's account or may have ghosted the CEO's account such that the email address looks accurate. NEVER send or wire funds without face-to-face confirmation or without otherwise following company's procedures.

From: Brenda Director <brendaceo@companya.com>
Date: April 2, 2017 at 2:12:01 PM EDT
To: Luke CFO <lukecfo@companya.com>
Subject: AT&T Payment – URGENT

Hi Luke,
I'm out of the office in a meeting with Dr. John Smith. He is a major physician recruit. The payment is overdue. This needs to go out now by wire transfer to avoid interruption of service.

Please immediately wire \$505,348.45 to South State Bank, Routing # 351578040, Account # 5831365839887. Let me know when complete. It can't wait.

Regards,
Brenda
CEO




12

16

Educate About MalDoc Trends through Phishing

FedEx Service <details@fedex.com> August 13, 2012 6:54 AM
To: bocking@hopefortheyoung.com
FedEx delivery problem # Error ID4900 [Details](#)



Federal Express

Unfortunately we failed to deliver the postal package you have sent on the 27th of July in time because the recipient's address is erroneous.

Please print out the label copy attached and collect the package at our office.

[Print a shipping Label](#)

Source: DynaSis


Voicemail Message
You have received a voicemail at 2013-19-12 05:31:25 CST.

You are receiving this message because we were unable to deliver it, voice message did not go through because the voicemail was unavailable at that moment.

* The reference number for this message is qv5_cj00-9107319001-2120079009-02.

The length of transmission was 24 seconds.
The receiving machine's ID: YJH35-TW410-F37JZL.

Thank you,
AT&T Online Services

Contact Us
AT&T Support - quick & easy support is available 24/7.

Receiving ID: YJH35-TW410-F37JZL
From Number(s): 459-330-7200


Getting To Know AT&T
Watch helpful videos to get you better acquainted with your new AT&T service.
[View the videos](#)

We value and appreciate your business!

*Mobile Broadband coverage not available in all areas.
** Based on U.S. carriers.

Attention New Jersey customers and small businesses: FREE e-cycling for electronic devices with video screens more than 4 inches at nearby collection sites. <http://www.nj.gov/dep/rb/what/ewaste/collection/sites.pdf> or 1-800-DEPKNOW

This is a system-generated message from a send only address. Please do not reply to this email.




13

17

Scams Often Make You Feel You are Missing Out If You Don't Click on the Link!

From: Drop-box. [<mailto:sasimakis@houston.org>]
Sent: Wednesday, May 10, 2017 10:45 AM
To: Peterson, Scott
Subject: You Received PDF_9980







Hi,

You Have Received An Invoice Sent By dropbox - User Due to It's Large Size.

[View Here To Access Your Invoice.](#)

Dropbox-Team!

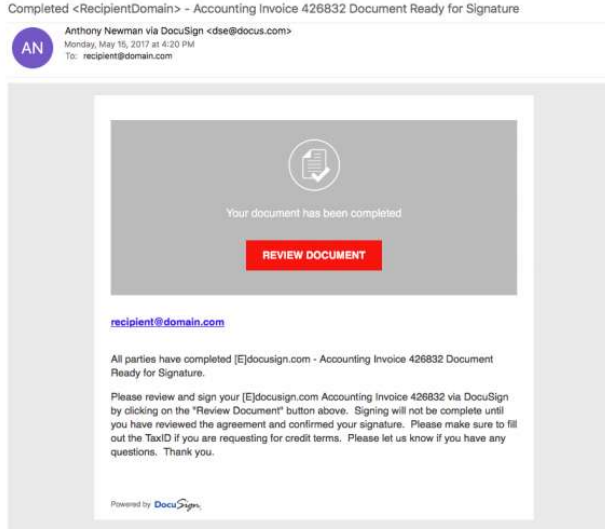

Click PDF to view the document





14

18

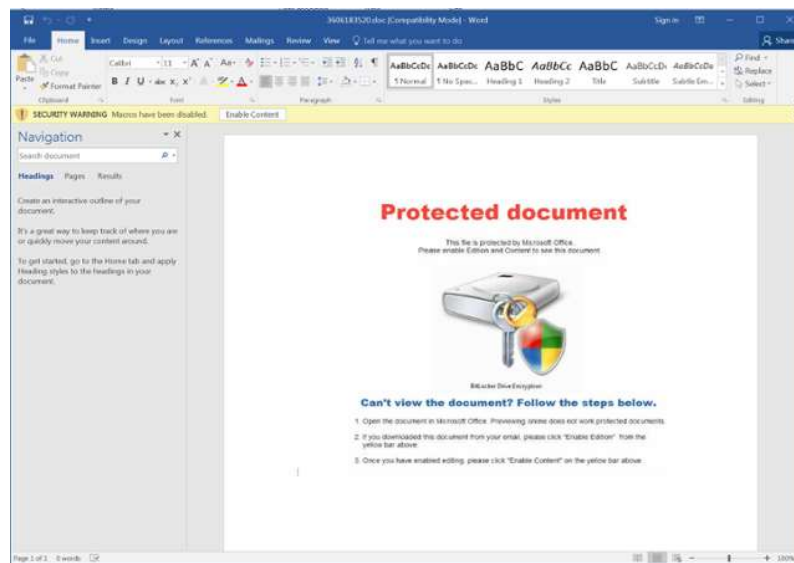
MalDoc Trends through Phishing Disguised as DocuSign



15

19

Some Scams Use our Security against Us! Scams Even Involve Encrypted Emails!!



16

20

HIPAA / HITECH BREACH NOTIFICATION RULE REPORTING

- HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.



20



21

HIPAA – HITECH Breach Notification Rule – Summary

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the unsecured 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:

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

There are three exceptions to the definition of “breach.”

- The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
- The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

22

Breach Risk Assessment Factors



Nature and extent of PHI involved

Unauthorized person who used or received the PHI

Whether PHI was actually acquired or viewed:
and

Extent to which the risk to the PHI has been mitigated

23

MUST COMPLY WITH U.S. CONSUMER PROTECTION NOTIFICATION LAWS FOR EACH OF THE 50 STATES

- Must assess laws in the states of residency of all the consumers (which includes employees) affected.
- Must assess the triggers for breach of personal information or personally identifiable information (“PII”).
- Each state has a different definition of PII and different triggers for notice.
- Many states require notice to the State Attorney General and/or Credit Bureaus.
- May have exceptions for HIPAA compliance.



17

24

EU REPORTING: GENERAL DATA PROTECTION REGULATION (“GDPR”)

Two different standards for notification under Article 33/34 of GDPR:

- Art. 33 - Notify the supervisory authority **within 72 hours** UNLESS it is unlikely to result in a risk to the rights or freedoms of the individuals. In this case, it's not a crazy amount of PI but it probably meets that threshold.
- Art. 34 - Notify the individuals if the breach is likely to result in a **HIGH** risk to the rights and freedoms of the individuals.



18



25

DEPARTMENT OF DEFENSE REPORTING OBLIGATIONS

The key Department of Defense regulation is DFARs 252.204–7012.

- Prime contractors with DoD must make a rapid report of a “cyber incident” involving Covered Defense Information (“CDI”).
 - Rapid report = within 72 hours of discovery of a cyber incident
- Subcontractors who are part of the supply chain are bound by DFARs if there are “flow down” provisions in their contracts. The DFARs regulation must appear in a contract, purchase order, change order, requisition form, etc. for a sub to be bound.
 - If bound by DFARs, subcontractors must comply in the same way as a prime.
 - Must report work to DoD and must alert prime contractors to the event.
- CDI is broadly defined.
 - CDI should be marked within the Company -- but it's not always marked.
- Under DFARs, contractors should be implementing measures to meet NIST 800-171 standards. Under the standard, contractors should know where CDI is located.
 - In reality, a lot of Companies have CDI in a lot of places.
- A cyber incident is reportable if a system that contains CDI is compromised or has been adversely impacted by a cyber incident. This is a very broad standard.
 - Reporting is also required if a cyber event causes a contractor to be unable to provide critical support under its DoD contract.
- DoD wants contractors to voluntarily disclose events quickly so DoD can timely conduct a damage assessment.

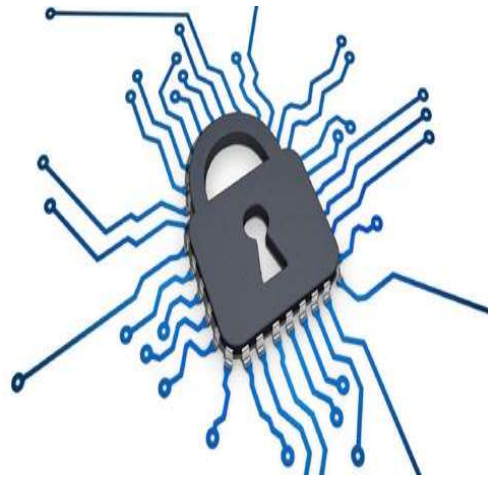
19



26

ADDITIONAL NOTICE OBLIGATIONS TO CONSIDER

- Other Foreign Laws – Consumer Notification?
- Parent and/or Affiliated Companies?
- Business Associate Agreement Notification?
 - Remember to Negotiate Terms in Light of Breaches



**DEVELOP INCIDENT RESPONSE PLAN and
CONDUCT RANSOMWARE
TABLETOP SIMULATIONS TO TEST IRP**

JOAN M. PODLESKI, CCEP, CHRC, CHC, CHPC



Joan Podleski, CCEP, CHRC, CHC, CHPC
VP & Chief Privacy Officer
Children's Health
Dallas, Texas
Office: 214.456.6068
joan.podleski@childrens.com

- Joan has been in the academic health care and research administration field for over 30 years.
- Joan is currently the Chief Privacy Officer for Children's Health System of Texas - which is the pediatric partner to UTSW.
- Prior to that, she served as Director of the Institutional Ethics & Compliance Program at Duke University, where she was responsible for the oversight program related to all compliance issues for the University and also served as the HIPAA Privacy Officer for the academic units of Duke.
- Prior to that, Joan spent more than 20 years at Washington University at St. Louis where she held multiple positions – including HIPAA Privacy Officer and Assistant Chancellor for Clinical Affairs.



29

GINA G. GREENWOOD, JD, CIPP/US



Partner
(404) 322-6790 (Office)
(404) 909-0665 (Mobile)
gina.greenwood@nelsonmullins.com



Gina Greenwood chairs the Privacy & Security Team & Breach Team and advises clients across the country and abroad from the Atlanta Office of Nelson Mullins. She concentrates her practice in HIPAA and health care regulatory matters and legal privacy / security compliance, breach preparedness and response, legal defense of government investigations, and litigation. Gina has a 20-year career in data privacy and also healthcare regulatory law, practicing her entire career at three Am Law 100 law firms. She is a recognized authority in Emergency Medical Treatment and Labor Act (EMTALA) compliance, investigations, hearings, and survey responses. She has extensive experience defending governmental investigations involving immediate jeopardy licensure surveys and many other regulatory, operational and compliance matters pertinent to healthcare and behavioral health entities.

Gina was selected by the U.S. Commission on Civil Rights as a **national EMTALA legal expert** and provided oral testimony for a U.S. Commission on Civil Rights (USCCR) hearing in Washington, D.C. and corresponding written testimony, which was included in the USCCR "Patient Dumping" report as Congressional testimony to the United States Congress (submitted September 2014). Gina is a frequent speaker on the topics of Cyber Liability and Data Breaches and EMTALA. Gina has been recognized by Chambers USA and by *Georgia Trend* Magazine as a Legal Elite. She is listed in Best Lawyers in America (2017 - 2021). Her full bio is available at Nelson Mullins - Gina Ginn Greenwood, JD, CIPP/US

30



31

31