

PREPARING FOR HIPAA AUDITS

A THREE-PRONG APPROACH

TODAY'S SPEAKERS



Bobby Seegmiller
VP, Business Development



Yenu Wodajo
Associate Broker, Cybersecurity



Peter Teichert
Chief Security Officer



AGENDA

- Latest on HIPAA audits
- Conducting a HIPAA risk assessment
- Considering cyber insurance
- Securing key technologies

A decorative graphic on the left side of the slide consisting of three parallel, wavy vertical lines. The outermost line is white, the middle line is yellow, and the innermost line is white. They are set against a solid dark brown background.

Q1

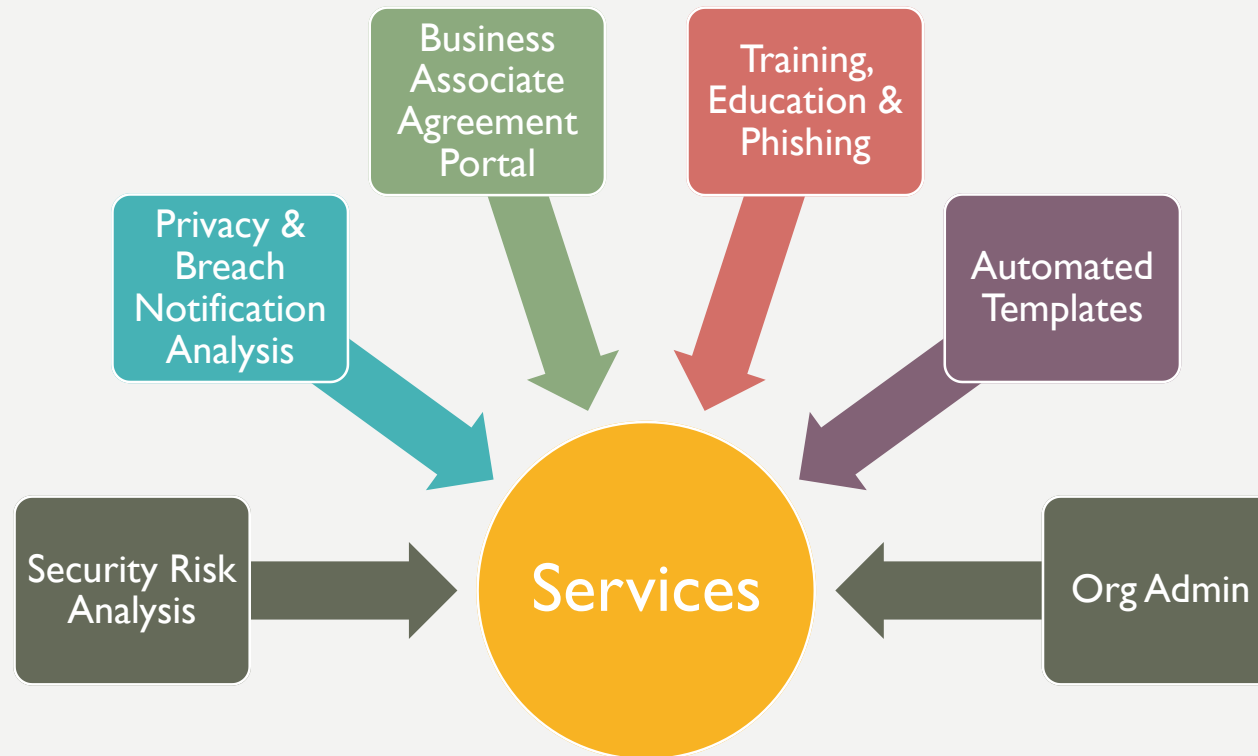
**WHAT IS YOUR ROLE IN THE
ORGANIZATION?**



HIPAA AUDITS & RISK ASSESSMENT

BOBBY SEEGMILLER
HIPAA ONE

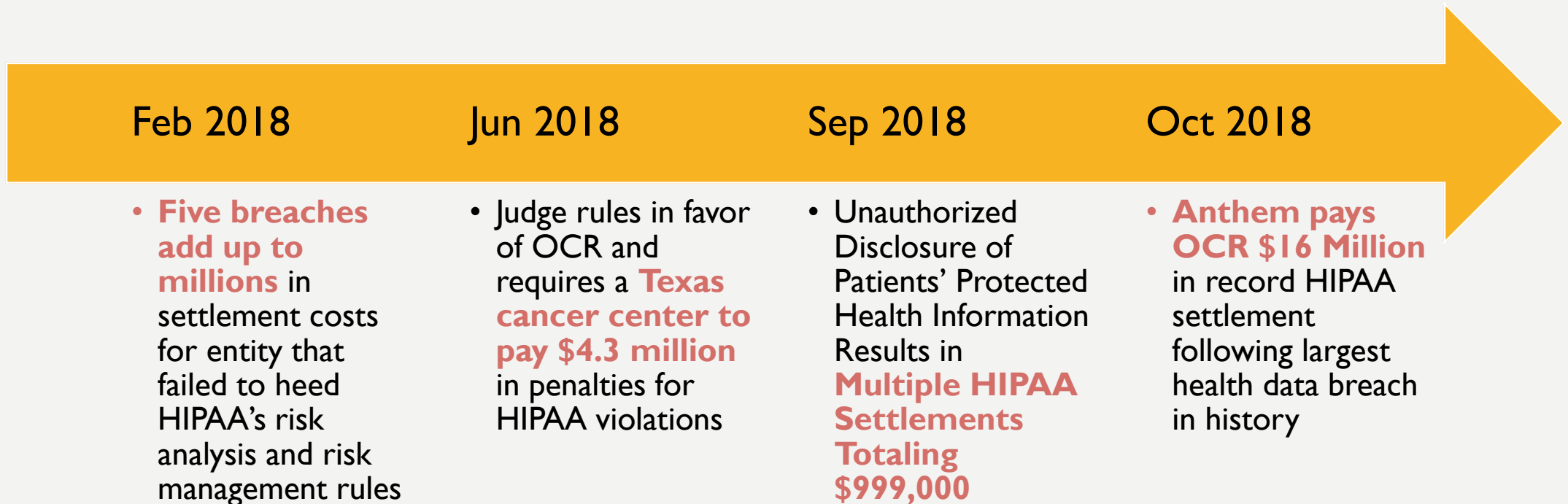
HIPAA ONE




LATEST NEWS ON HIPAA AUDITING

- **What Is It?** HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.
- **Who Audits?** Health and Human Services' Office for Civil Rights (OCR)
- **Previous Audits?** Educational to encourage best practices
- **Future Audits?** Harsher investigative tools to “**hold bad actors accountable,**” according to OCR Director, Roger Severino
- **Penalties?** Fines ranging from \$100 to \$50,000 **per violation**, with \$1.5 million per year maximum

EXAMPLES OF HEALTHCARE FINES





Q2

**HOW DID YOU CONDUCT YOUR LAST
HIPAA RISK ANALYSIS?**

RESULTS OF LAST WEBINAR POLL

Just over 50% completed
HIPAA risk analysis

- Most used external consultants
- Yet 75% did NOT feel confident of passing an audit



Of those who did NOT:

- Most cited was “lack of knowledge”
- Next cited was “didn’t know it was mandatory”

PROBLEM: HIGH CHANCE OF AUDIT

5 Ways Healthcare Providers Get Audited

Patient Complaint

- Privacy (PHI)
- Security (ePHI)

Whistleblower

- Employee files anonymous report to HHS

Breach Notice

- Includes malware
- Omnibus update - all unauthorized disclosures are breaches

Random Audits

- Fraud waste & abuse
- False claims
- Unauthorized disclosures

State Eligibility Audits

- Social Security audits
- State Attorneys General per HITECH
- Meaningful Use/MIPS

STATE ELIGIBILITY AUDITS



Connecticut Department of Social Services
Making a Difference

MYERS AND STAUFFER LLC
CERTIFIED PUBLIC ACCOUNTANTS

May 8, 2018

Re: Medicaid EHR Incentive Program Year 2014 Payment

Dear Dr. [REDACTED]:

As part of our ongoing program monitoring efforts, Connecticut's Department of Social Services is conducting reviews of Connecticut Medicaid Electronic Health Record (EHR) Incentive Program payments made to participating providers. Federal regulations governing the Medicaid EHR Incentive Program require States to conduct these post-payment reviews.

This letter is confirmation that Myers and Stauffer LLC, a contractor for Connecticut's Medicaid EHR Incentive Program, is a representative of this agency and is authorized to conduct post-payment audits through desk reviews or on-site examinations. This letter is notification that you have been selected for a **Program Year 2014 desk review**. The purpose of the desk review is to validate certain information utilized in the eligibility calculation and meaningful use for the incentive payment you received. During this review our contractors may require, at a minimum:

Eligibility Analysis Documentation Request for Program Year 2014:

- Numerator: A detailed list of Medicaid encounters during your selected eligibility period for which Medicaid was the patient's guarantor regardless of the amount paid.
- Denominator: A detailed list of all patient encounters (the numerator should be an identifiable subset of the denominator) that occurred during the eligibility period.
- At a minimum, the detailed information to validate the numerator and denominator should include patient name, date of service, payer source, and rendering provider.
- Documentation to support an eligible professional's affiliation with a group practice when that eligible professional utilized the group proxy to report encounter volume;

Meaningful Use Documentation Request for Program Year 2014:

- System generated core, menu, and clinical quality measures reports for the EHR reporting period to which you attested;
- Documentation supporting all reported measure which do not require a numerator and denominator (i.e., "yes: attestation and data transmission tests);
- Additional documentation may be requested based on the review work performed.

A representative of Myers and Stauffer LC will contact you within five (5) business days to discuss the documentation request and answer any questions you may have. Please submit all PHI in a secure manner.

The regulations and guidelines used were in effect for the EHR Reporting Period under review. These include:

- Code of Federal Regulations (CFR) 42 §495 *Standards for the EHR Incentive Program*;
- CFR 45 §164.306 *Security Standard: General Rules*,
CFR 45 §164.308 *Administrative Safeguards*;
- Federal Register (FR) and other Federal guidelines pertaining to Health Information Technology and the Electronic Health Record (EHR) Incentive Program.

V. AUDIT PROCESS

This HCA provider audit was conducted in the following manner:

Provider Selection

Any Provider who has received an EHR incentive payment may be subject to an audit. This provider was randomly selected.

Documentation Reviewed

The audit was conducted as a desk review. The provider was sent an audit questionnaire to fill out. The auditor reviewed responses from the questionnaire, the provider's 2016 attestation and all documentation supplied during attestation along with documentation and information supplied during the audit.

VI. FINDINGS

An EHR incentive payment was made to [REDACTED] Health on behalf of MD, for EHR Program Year 3, 2016, on 6/22/17, in the amount of \$8,500.

Payment List							
Year	Program Year	Date	RA Number	Warrant	Amount	Method	Status
3	2016	06/22/2017			\$8,500.00	EFT	Paid

An audit was conducted to ensure the appropriateness of the payment for having met eligibility and meaningful use requirements.

There was one finding for this audit. The audit finding was on the meaningful use Objective 1, Protect Health Information.

All meaningful use objectives/measures must be met in order to qualify for an incentive payment.

HOW HIPAA ONE RISK ASSESSMENT WORKS



Step 1 – Gather Information, Interviews, Inventory, etc.

- Participant login, answer simple questions and interview
- Import last year's work



Step 2 – Remediation Planning

- Results of Step 1,
- Develop and Assign tasks



Step 3 – Sign and Add Reviewers

- Download PnP examples
- Ongoing remediation and documentation



Q3

**IF AUDITED TOMORROW, ARE YOU 100%
CONFIDENT YOU WOULD PASS?**



CONSIDERING CYBER INSURANCE

YENU WODAJÓ
WILLIS TOWERS WATSON

WILLIS TOWERS WATSON: GLOBAL CYBER TEAM

Global Connectivity – Highly experienced, dedicated FINEX cyber/E&O consultants, placement brokers & Claim Specialists

45+



U.S. brokers/professionals,
product and thought leaders
and consultants with a
footprint in eight cities

50+



London, Canada,
Western Europe,
LatAm & AsiaPac based
brokers/professionals

20+



Claim
Advocates

20+



Global locations
with cyber
locations

100+



Cyberinsurance
specialists

750+



Cyber
clients

CHALLENGES WITH CYBERSECURITY WORK

84% of cyber functions are anticipating headcount growth

Is there clarity on how you are building capacity and capability for cyber work?

Cyber: employee ratio
1:900 with permanent employees
1:600 with contractors

Cybersecurity is shifting to be “co-led” with the business as the most predominant partner model

86% of cyber functions plan to change their structure

The need for IS and IT to work together more effectively is driving structural changes

Pivotal roles in cyber tend to take longer to recruit and develop, are more “**expensive**” to buy, and **difficult to retain** due to high in demand skills and experiences

CYBER CONDITIONS IN HEALTHCARE

2018 Largest Breaches

Organization's Name	Records Compromised
AccuDoc Solutions, Inc.	2.65M
Iowa Health System d/b/a UnityPoint Health	1.42M
Employees Retirement System of Texas	1.25M
CA Dept. of Developmental Services	582,000
MSK Group	566,000
CNO Financial Group, Inc.	566,000
Health Management Concepts, Inc.	502,416
Airway Oxygen, Inc.	500,000
AU Medical Center, Inc.	417,000
SSM Health St. Mary's Hospital – Jefferson City	301,000
Women's Health Care Group of PA, LLC	300,000

Five Largest 2018 OCR Fines

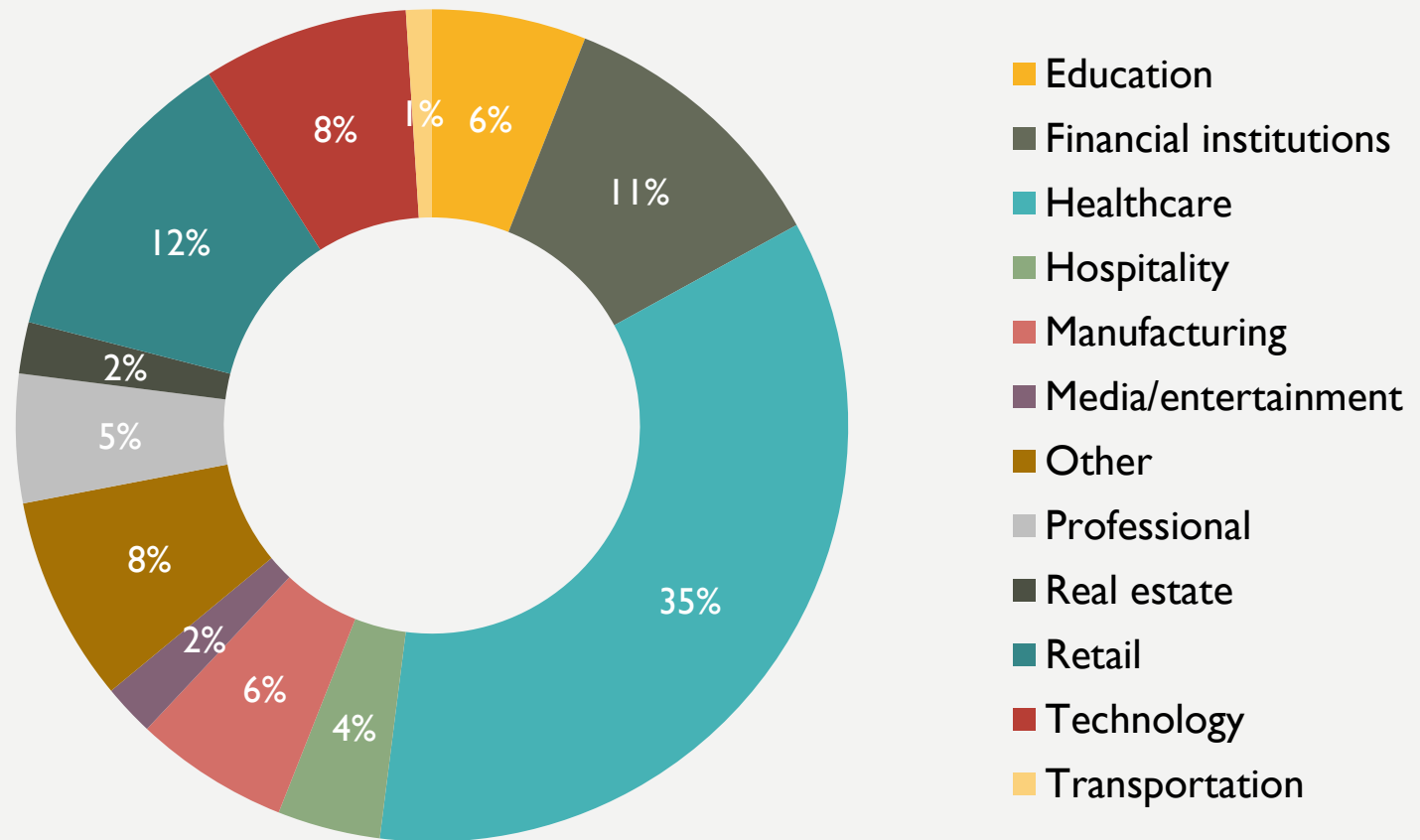
Organization's Name	OCR Fine/Settlement Amount
Anthem, Inc.	\$16M
The University of Texas MD Anderson Cancer Ctr	\$4.35M
Fresenius Medical Care North America (FMCNA)	\$3.5M
Boston Medical Center, Brigham and Women's Hospital and Massachusetts General Hospital	\$1M
Allergy Associates of Hartford, P.C.	\$125,000

Top 10 HIPAA OCR Fines to Date

Organization's Name	OCR Fine/Settlement Amount
Anthem, Inc.	\$16M
Advocate Health System	\$5.5M
Memorial Healthcare System	\$5.5M
NY-Presbyterian Hospital and Columbia Univ	\$4.8M
The University of Texas MD Anderson Cancer Ctr	\$4.35M
Cignet Health Center	\$4.3M
Triple-S	\$3.5M
Fresenius Medical Care North America (FMCNA)	\$3.5M
Children's Medical Center of Dallas	\$3.2M
University of Mississippi Medical Center	\$2.75M

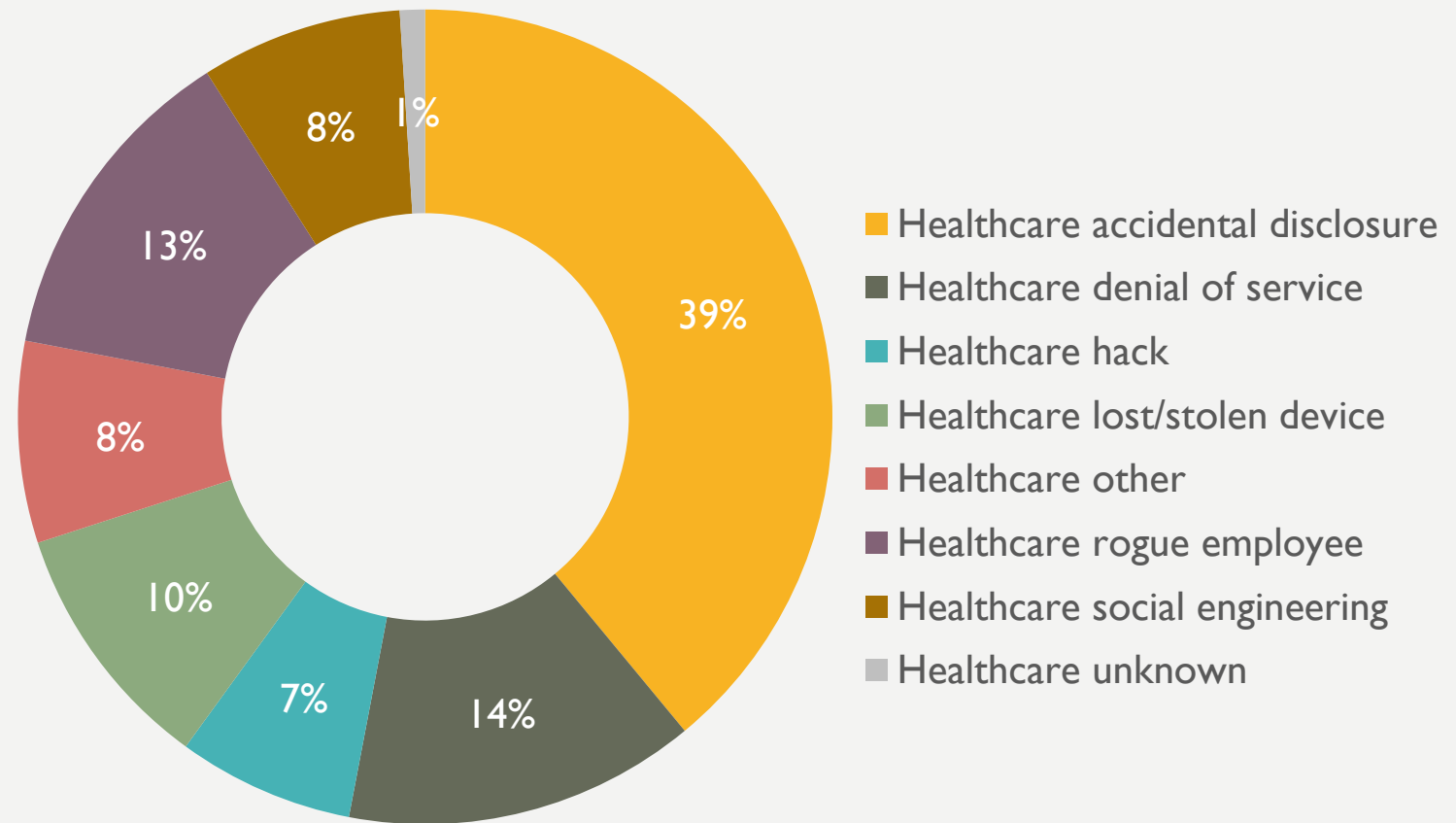
CYBER CLAIMS BY INDUSTRY

Proprietary Willis Towers Watson Data
2017-2018



CYBER CLAIMS LOSS IN HEALTHCARE

Willis Towers Watson Proprietary Data
2017-2018



WHAT INFORMATION IS AT RISK?

- **Personally Identifiable Information (PII)**
 - SSN
 - Date and place of birth
- **Protected Health Information (PHI)**
 - Medical history
 - Health insurance information
- **Payment Card Information (PCI)**
 - Credit Card #
 - CVV/Service Code
 - Expiration date
- **Corporate**
 - Trade secrets
 - Merger and acquisition plans/information
 - New product plans

CYBER COVERAGE OVERVIEW

LIABILITY COVERAGE ('THIRD PARTY' COVERAGE)	
Privacy Liability	Liability costs associated with an inability to protect personally identifiable information, personal health information or a third party's corporate confidential information.
Network Security Liability	Liability costs associated with an inability to prevent a computer attack against your computer network or a third party's network.
Regulatory Fines	Fines assessed by a federal, state, local or international regulatory body due to a data breach.
PCI Fines	Costs associated with any written demand from a Payment Card Association (Mastercard,VISA,AMEX) or bank processing payment card transactions for a monetary assessment in connection with non-compliance with PCI Data Security Standard as a result of a security breach.
Media Liability	Liability associated with disseminated content, including social media content.

CYBER COVERAGE OVERVIEW

LIABILITY MITIGATION COVERAGE

Breach Response Costs	Direct costs expended to respond to a privacy incident. Costs typically include legal, public relations, notification, identity theft restoration, credit monitoring and forensic investigation expenses.
-----------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

FIRST PARTY COVERAGE

Income Loss / Extra Expense	Income Loss / Extra Expense associated with a computer attack or system failure which disables your network.
Data Reconstruction	Costs to recreate, recollect data lost, stolen or corrupted due to an inability to prevent a computer attack against your network.
Extortion Costs	Costs expended to comply with a cyber extortion demand.



SECURING KEY TECHNOLOGIES

**PETER TEICHERT
PRIME CARE TECHNOLOGIES**

KEY SECURITY AREAS

- Application security
- Network security
- Operations security
- Information security
- User training

APPLICATION SECURITY



Check app security features

- Review all
- Check usage

Control passwords

- Ensure not obvious or accessible
- Change every 90 days

Audit user access regularly

- Check who/what/when as often as quarterly

NETWORK SECURITY



Firewalls

Intrusion detection and
prevention services (IDS/IPS)

Anti-virus and anti-malware

OPERATIONS SECURITY

- **Access control**
 - Where are servers and network equipment?
 - Do your facilities have same protection?
- **Backup power and connectivity**
 - Do you have redundancy?
- **Data backup**
 - Can you recover after a crash?



INFORMATION SECURITY




USER TRAINING & AWARENESS



HIPAA
Training

5 most
common
threats

Everyone
owns security

A decorative graphic on the left side of the slide consisting of two parallel, wavy vertical lines. The inner line is yellow and the outer line is white, both set against a dark brown background.

Q4

**WHICH OF THESE TOPICS ARE YOU
INTERESTED IN HEARING MORE
ABOUT?**

QUESTIONS & REWARDS



Willis Towers Watson 



MORE INFORMATION

- For questions, or to schedule an assessment, contact:
MARKETING@PRIMECARETECH.COM
- Available assessments include:
 - HIPAA One Risk Analysis
 - Willis Towers Watson Insurance Assessment
 - Prime Care Technologies IT Assessment

SCHEDULE IN JANUARY...

