YOUR LAWYER / YOUR BUSINESS ASSOCIATES:

UNDERSTANDING THE DUAL ROLES THAT LAWYERS PLAY FOR THEIR HEALTHCARE CLIENTS

DEBRA A. GEROUX, JD, CHC, CHPC
SHAREHOLDER
BUTZEL LONG, A PROFESSIONAL CORPORATION
GEROUX@BUTZEL.COM

JOAN M. PODLESKI, CCEP, CHC, CHPC, CHRC
CHIEF PRIVACY OFFICER
CHILDREN'S HEALTH
JOAN.PODLESKI@CHILDRENS.COM

1

POLLING QUESTION # 1
WHO IS OUR AUDIENCE?

WHO DO YOU WORK FOR?

1. COVERED ENTITY (PROVIDER/PLAN/CLEARING HOUSE)
2. BUSINESS ASSOCIATE
3. SUBCONTRACTOR TO BUSINESS ASSOCIATE
4. OTHER

2

POLLING QUESTION # 2
BUSINESS ASSOCIATES: WHO ARE YOU?

1. LEGAL (IN-HOUSE OR OUTSIDE)
2. FINANCIAL (ACCOUNTANT, CFO, ETC)
3. COMPLIANCE
4. IT/CIO/CISO
5. OTHER

3

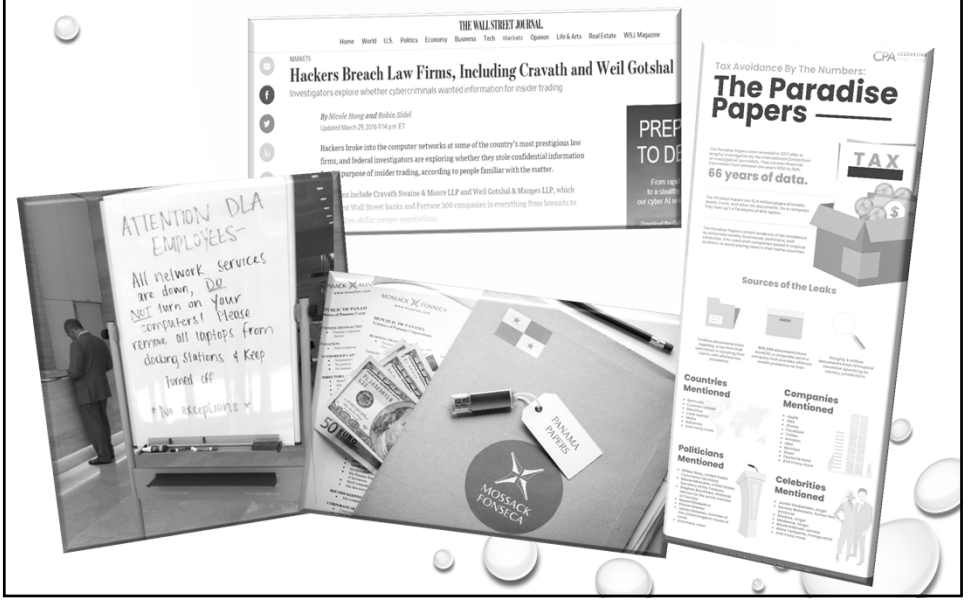
LAWYERS AS BUSINESS ASSOCIATES

THE MANY ROLES LAWYERS PLAY

- WHAT IS CONTEXT OF ENGAGEMENT?
  - EMPLOYMENT DISPUTE
  - CONTRACT REVIEW WITH MEDICAL DEVICE MANUFACTURER
  - MEDICAL MALPRACTICE DEFENSE
  - SALE OF PRACTICE / BUSINESS VALUATION
  - CIVIL / CRIMINAL LITIGATION (FCA/AKS)
- IS PHI NECESSARY TO SERVICES?

4

LAW FIRMS UNDER ATTACK



LAWYERS ARE NOT IMMUNE FROM HIPAA BREACH REPORTING

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Quarles & Brady, LLP	WI	Business Associate	1032	04/19/2016	Theft	Laptop
Consultants in Neurological Surgery, LLP	FL	Healthcare Provider	800	11/08/2016	Unauthorized Access/Disclosure	Paper/Films
Benesch, Friedlander, Coplan & Aronoff LLP	OH	Business Associate	1134	02/10/2017	Theft	Paper/Films

6

THE LEGAL PRIVILEGES

ATTORNEY-CLIENT COMMUNICATIONS & ATTORNEY WORK PRODUCT

7

LEGAL SERVICES OR BUSINESS?

WHATEVER I TELL MY ATTORNEY IS PRIVILEGED RIGHT?

- ATTORNEY-CLIENT - COMMUNICATIONS REGARDING ***LEGAL ADVICE;*** NOT ***BUSINESS ADVICE***
- BLURRED LINES - GENERAL COUNSEL PROVIDE BOTH LEGAL AND BUSINESS ADVICE
- GC SHOULD NOT BE INVOLVED IN COMPLIANCE ACTIVITIES

  THE CHIEF COMPLIANCE OFFICER SHALL BE A MEMBER OF SENIOR MANAGEMENT OF PFIZER, SHALL REPORT DIRECTLY TO THE CHIEF EXECUTIVE OFFICER OF PFIZER, SHALL MAKE PERIODIC (AT LEAST QUARTERLY) REPORTS REGARDING COMPLIANCE MATTERS DIRECTLY TO THE AUDIT COMMITTEE OF THE BOARD OF DIRECTORS OF PFIZER (AUDIT COMMITTEE), AND SHALL BE AUTHORIZED TO REPORT ON SUCH MATTERS TO THE AUDIT COMMITTEE AT ANY TIME. THE CHIEF COMPLIANCE OFFICER SHALL NOT BE, OR BE SUBORDINATE TO, THE GENERAL COUNSEL OR CHIEF FINANCIAL OFFICER. *SOURCE:* 2009 PFIZER CIA, AVAILABLE AT HTTP://OIG.HHS.GOV/FRAUD/CIA/AGREEMENTS/PFIZER_INC_08312009.PDF

8

LAWYERS PERFORMING "HEALTH CARE OPERATIONS" FOR CE

- 45 CFR 164.501
  - *HEALTH CARE OPERATIONS MEANS ANY OF* THE FOLLOWING ACTIVITIES OF THE COVERED ENTITY TO THE EXTENT THAT THE ACTIVITIES ARE RELATED TO COVERED FUNCTIONS:

    * * *

    (4) CONDUCTING OR ARRANGING FOR MEDICAL REVIEW, LEGAL SERVICES, AND AUDITING FUNCTIONS, INCLUDING FRAUD AND ABUSE DETECTION AND COMPLIANCE PROGRAMS;

9

NOT ALL MEDICAL INFORMATION IS PROTECTED

FROM WHOM DID THE INFORMATION COME?

- INDIVIDUAL DIRECTLY OR WITH WRITTEN AUTHORIZATION—NOT PROTECTED UNLESS QUALIFIED PROTECTIVE ORDER ("QPO") OR OTHERWISE LIMITED BY INDIVIDUAL
- COVERED ENTITY (CE) AS **EMPLOYER**—NOT PROTECTED
  - WORKERS COMPENSATION CLAIM / INFORMATION
  - EMPLOYER-REQUIRED DRUG TESTING RESULTS
  - FMLA HEALTH INFORMATION
  - DISABILITY CLAIM INFORMATION
  - STOP-LOSS INSURANCE
- *CAVEAT*—OTHER STATE LAWS MAY REQUIRE PROTECTION OF THIS INFORMATION
  - **IDENTITY THEFT PROTECTION ACT** (ITPA), MCL §§ 445.61 *ET SEQ.*
  - **SOCIAL SECURITY NUMBER PRIVACY ACT** (SSNPA), MCL §§ 445.81 *ET SEQ.*
  - **MICHIGAN CONSUMER PROTECTION ACT** (MCPA), MCL § 445.903

10

ATTORNEY CLIENT PRIVILEGE

- COMMUNICATION PROTECTED WHEN:
  - BETWEEN LAWYER AND CLIENT (INCLUDES IN-HOUSE, BUT MORE SCRUTINIZED)
  - IN THE COURSE OF A PROFESSIONAL RELATIONSHIP
  - FOR THE PURPOSE OF OBTAINING / PROVIDING LEGAL ADVICE OR SERVICES
  - MADE IN CONFIDENCE (NOT SHARED WITH OR IN PRESENCE OF 3RD PARTY.*
- NOT PROTECTED:
  - BUSINESS ADVICE
  - CRIME-FRAUD EXCEPTION

11

ATTORNEY WORK PRODUCT

FRCP 26(B)(3)

- ATTORNEY WORK PRODUCT DOCTRINE PROTECTS **DOCUMENTS** AND **TANGIBLE** THINGS THAT ARE PREPARED IN **ANTICIPATION OF LITIGATION** OR FOR TRIAL BY OR **FOR ANOTHER** PARTY OR ITS REPRESENTATIVE.
- NOT AWP:
  - DOCUMENTS "ASSEMBLED IN THE ORDINARY COURSE OF BUSINESS, OR PURSUANT TO PUBLIC REQUIREMENTS **UNRELATED TO LITIGATION**"
  - DOCUMENTS PREPARED PURSUANT TO REGULATORY REQUIREMENTS*

12

WAIVING THE ATTORNEY-CLIENT PRIVILEGE

HOW? "Voluntary" production of privileged material to a third-party. BUT where regulations afford the government a legal right to access is "involuntary" See ***Securities and Exchange Commission v. Lavin,*** 111 F.3d 921 (D.C. Cir. 1997) ("Bankers Trust's production of the privileged materials to Federal Reserve Bank in response to Federal Reserve's exercise of its examination powers, and not pursuant to a subpoena, not a voluntary act)

EFFECT? Increase exposure for a company when privileged material falls into the hands of the plaintiffs' bar providing a "road map" for a third party's claims against company

13

LIMITED/SELECTIVE WAIVER

- **LIMITED** / **SELECTIVE WAIVER** PERMITS THE CLIENT WHO HAS DISCLOSED PRIVILEGED COMMUNICATIONS TO ONE PARTY (TYPICALLY ASSERTED WHEN PRODUCING PRIVILEGED MATERIAL TO THE GOVERNMENT AGENCIES) TO CONTINUE ASSERTING THE PRIVILEGE AGAINST OTHER PARTIES. ***DIVERSIFIED INDUSTRIES, INC. V. MEREDITH,*** 572 F.2D 596 (8TH CIR.1978) (EN BANC)(DISCLOSURE TO SEC NOT A WAIVER—FURTHERS PUBLIC POLICY OF ENCOURAGING VOLUNTARY COOPERATION WITH GOVERNMENT INVESTIGATIONS)
- SELECTIVE WAIVER MAY BE APPROPRIATE WHERE THE DISCLOSING PARTY TOOK STEPS (CONFIDENTIALITY AGREEMENT WITH SEC BEFORE DISCLOSURE) TO PRESERVE ITS PRIVILEGE. ***LAWRENCE E. JAFFE PENSION PLAN V. HOUSEHOLD INT'L, INC.***, 244 F.R.D. 412, 433 (N.D. ILL. 2006)
- OVERWHELMINGLY REJECTED –MOST JURISDICTIONS HOLD THAT ONCE THE PRIVILEGE IS WAIVED AS TO ONE, IT IS WAIVED TO ALL. ***IN RE COLUMBIA/HCA HEALTHCARE CORP. BILLING PRACTICES LITIGATION***, 293 F.3D 289, 307-14 (6TH CIR. 2002)(CODING AUDIT SHARED WITH DOJ WAIVED THE ATTORNEY-CLIENT AND AWP PRIVILEGES TO ALL)

14

HHS'S TAKE ON LAWYERS AS BAS AND THE A/C PRIVILEGE

"THE PRIVACY RULE IS NOT INTENDED TO INTERFERE WITH ATTORNEY-CLIENT PRIVILEGE. NOR DOES THE DEPARTMENT ANTICIPATE THAT IT WILL BE NECESSARY FOR THE SECRETARY TO HAVE ACCESS TO PRIVILEGED MATERIAL IN ORDER TO RESOLVE A COMPLAINT OR INVESTIGATE A VIOLATION OF THE PRIVACY RULE. HOWEVER, THE DEPARTMENT DOES NOT BELIEVE THAT IT IS APPROPRIATE TO EXEMPT ATTORNEYS FROM THE BUSINESS ASSOCIATE REQUIREMENTS."

PREAMBLE TO HIPAA FINAL RULE, 67 FR 53253 (AUGUST 14, 2002), AVAILABLE AT HTTP://WWW.HHS.GOV/OCR/PRIVACY/HIPAA/ADMINISTRATIVE/PRIVACYRULE/PRIVRULEPD.PDF.

15

HHS AUDIT REQUIREMENT

SECTION 13411 OF THE AMERICAN RECOVERY & REINVESTMENT ACT, P.L 111-5, 42 USC 17940 ("ARRA") REQUIRES HHS TO PROVIDE FOR PERIODIC AUDITS OF COVERED ENTITIES ("CE") AND BUSINESS ASSOCIATES (BA) TO ENSURE COMPLIANCE WITH THE HIPAA PRIVACY, SECURITY AND BREACH NOTIFICATION RULES.

IF LEGAL ASSISTS IN THE RISK ASSESSMENT OR A PRIVACY COMPLAIN INVESTIGATION, IS WORK PRODUCT AND/OR ADVICE PROTECTED?

16

MANDATORY DISCLOSURE TO HHS-OCR

45 CFR §160.310 - RESPONSIBILITIES OF COVERED ENTITIES AND BUSINESS ASSOCIATES.

(a) PROVIDE RECORDS AND COMPLIANCE REPORTS

(b) COOPERATE WITH COMPLAINT INVESTIGATIONS AND COMPLIANCE REVIEWS.

(c) PERMIT ACCESS TO INFORMATION

17

THE ETHICS OF CONFIDENTIALITY

18

LAWYER'S ETHICAL OBLIGATIONS

ABA MODEL RULES OF PROFESSIONAL CONDUCT

RULE 1.1: COMPETENCE

A LAWYER SHALL PROVIDE COMPETENT REPRESENTATION TO A CLIENT. COMPETENT REPRESENTATION REQUIRES THE LEGAL KNOWLEDGE, SKILL, THOROUGHNESS AND PREPARATION REASONABLY NECESSARY FOR THE REPRESENTATION.

COMMENT [8]:

TO MAINTAIN THE REQUISITE KNOWLEDGE AND SKILL, A LAWYER SHOULD KEEP ABREAST OF CHANGES IN THE LAW AND ITS PRACTICE, INCLUDING THE BENEFITS AND RISKS ASSOCIATED WITH **RELEVANT TECHNOLOGY**, ENGAGE IN CONTINUING STUDY AND EDUCATION AND COMPLY WITH ALL LEGAL EDUCATION REQUIREMENTS TO WHICH THE LAWYER IS SUBJECT. (EMPHASIS ADDED)

19

LAWYER'S ETHICAL OBLIGATIONS

ABA MODEL RULES OF PROFESSIONAL CONDUCT

RULE 1.6 CONFIDENTIALITY OF INFORMATION

A. A LAWYER SHALL NOT REVEAL INFORMATION RELATING TO THE REPRESENTATION OF A CLIENT UNLESS THE CLIENT GIVES INFORMED CONSENT, THE DISCLOSURE IS IMPLIEDLY AUTHORIZED IN ORDER TO CARRY OUT THE REPRESENTATION OR THE DISCLOSURE IS PERMITTED BY PARAGRAPH (B).

B. A LAWYER MAY REVEAL INFORMATION RELATING TO THE REPRESENTATION OF A CLIENT TO THE EXTENT THE LAWYER REASONABLY BELIEVES NECESSARY

C. A LAWYER **SHALL MAKE REASONABLE EFFORTS TO PREVENT THE INADVERTENT OR UNAUTHORIZED DISCLOSURE OF, OR UNAUTHORIZED ACCESS TO, INFORMATION RELATING TO THE REPRESENTATION OF A CLIENT**.

20

LAWYER'S ETHICAL OBLIGATIONS

ABA MODEL RULES OF PROFESSIONAL CONDUCT

RULE 1.7: CONFLICT OF INTEREST (LOYALTY)

A LAWYER SHALL NOT REPRESENT A CLIENT IF THE REPRESENTATION INVOLVES A CONCURRENT CONFLICT OF INTEREST. A CONCURRENT CONFLICT OF INTEREST EXISTS IF: . . . THERE IS A SIGNIFICANT RISK THAT THE REPRESENTATION OF ONE OR MORE CLIENTS WILL BE MATERIALLY LIMITED BY THE LAWYER'S RESPONSIBILITIES TO ANOTHER CLIENT, A FORMER CLIENT OR A THIRD PERSON OR BY A PERSONAL INTEREST OF THE LAWYER.

[A] LAWYER MAY REPRESENT A CLIENT IF: (1) THE LAWYER REASONABLY BELIEVES THAT THE LAWYER WILL BE ABLE TO PROVIDE COMPETENT AND DILIGENT REPRESENTATION TO EACH AFFECTED CLIENT; (2) THE REPRESENTATION IS NOT PROHIBITED BY LAW; (3) THE REPRESENTATION DOES NOT INVOLVE THE ASSERTION OF A CLAIM BY ONE CLIENT AGAINST ANOTHER CLIENT REPRESENTED BY THE LAWYER IN THE SAME LITIGATION OR OTHER PROCEEDING BEFORE A TRIBUNAL; AND (4) EACH AFFECTED CLIENT GIVES INFORMED CONSENT, CONFIRMED IN WRITING.

21

LAWYER'S ETHICAL OBLIGATIONS

ABA MODEL RULES OF PROFESSIONAL CONDUCT

RULE 1.16: DECLINING OR TERMINATING REPRESENTATION

(D) UPON TERMINATION OF REPRESENTATION, A LAWYER SHALL TAKE STEPS TO THE EXTENT REASONABLY PRACTICABLE TO PROTECT A CLIENT'S INTERESTS, SUCH AS GIVING REASONABLE NOTICE TO THE CLIENT, ALLOWING TIME FOR EMPLOYMENT OF OTHER COUNSEL, SURRENDERING PAPERS AND PROPERTY TO WHICH THE CLIENT IS ENTITLED AND REFUNDING ANY ADVANCE PAYMENT OF FEE OR EXPENSE THAT HAS NOT BEEN EARNED OR INCURRED. THE LAWYER MAY RETAIN PAPERS RELATING TO THE CLIENT TO THE EXTENT PERMITTED BY OTHER LAW.

22

COMPETENCY AND CONFIDENTIALITY

RECOGNIZING TODAY'S TECHNOLOGY PRACTICES

ABA ETHICS 2000 COMMISSION: COMMENTARY 12, 16& 17 TO RULE 1.6 AMENDED TO RECOGNIZE CHANGES IN TECHNOLOGY USE IN PRACTICE AND OTHER REQUIREMENTS OF CONFIDENTIALITY:

- [12] RECOGNIZING A LAWYER'S DUTY TO DISCLOSE INFORMATION ABOUT A CLIENT PURSUANT TO "OTHER LAWS"
- [16] RECOGNIZING A LAWYER'S DUTY TO ACT COMPETENTLY IN RELATION TO SAFEGUARDING CLIENT INFORMATION AGAINST INADVERTENT OR UNAUTHORIZED DISCLOSURE BY THE LAWYER OR SUBORDINATES
- [17] RECOGNIZING A LAWYER'S DUTY TO USE SPECIAL SECURITY MEASURES WHEN TRANSMITTING CONFIDENTIAL INFORMATION BY TAKING "REASONABLE PRECAUTIONS TO PREVENT THE INFORMATION FROM COMING INTO THE HANDS OF UNINTENDED RECIPIENTS." FACTORS FOR DETERMINING REASONABLENESS INCLUDE:
  - SENSITIVITY OF THE INFORMATION
  - EXTENT TO WHICH THE PRIVACY OF THE COMMUNICATION IS PROTECTED BY LAW OR AGREEMENT.

23

DEFINING THE COMPETENT ATTORNEY

- 32 STATES OFFICIALLY REQUIRE TECH COMPETENCY OF ITS LAWYERS.
  - AZ BAR ETHICS OPINION: "COMPETENCE TO EVALUATE THE NATURE OF THE POTENTIAL THREAT"
  - OCTOBER 2018 VT SUPREME COURT ETHICS ORDER
- COMMUNICATING WITH CLIENTS VIA EMAIL?
  - ACP WAIVER / EXPECTATION OF PRIVACY?
  - SECURE EMAIL?
- DETERMINING THE PROPER NORM FOR COMMUNICATION
  - ASSESS THE FACTS, CIRCUMSTANCES & RISKS

24

THE ETHICS OF COMPETENCY & CONFIDENTIALITY

- **COMPETENCY**—KNOW WHAT TECHNOLOGY IS NECESSARY AND HOW IT IS USED
- **CONFIDENTIALITY**—EMPLOY COMPETENT AND REASONABLE STEPS TO ASSURE CLIENT'S CONFIDENCES ARE NOT DISCLOSED
- **REASONABLE ≠ ABSOLUTE:**

  A LAWYER IS REQUIRED TO EXERCISE SOUND PROFESSIONAL JUDGMENT ON THE STEPS NECESSARY TO SECURE CLIENT CONFIDENCES AGAINST FORESEEABLE ATTEMPTS AT UNAUTHORIZED ACCESS. "REASONABLE CARE," HOWEVER, DOES NOT MEAN THAT THE LAWYER ABSOLUTELY AND STRICTLY GUARANTEES THAT THE INFORMATION WILL BE UTTERLY INVULNERABLE AGAINST ALL UNAUTHORIZED ACCESS. SUCH A GUARANTEE IS IMPOSSIBLE, AND A LAWYER CAN NO MORE GUARANTEE AGAINST UNAUTHORIZED ACCESS TO ELECTRONIC INFORMATION THAN HE CAN GUARANTEE THAT A BURGLAR WILL NOT BREAK INTO HIS FILE ROOM, OR THAT SOMEONE WILL NOT ILLEGALLY INTERCEPT HIS MAIL OR STEAL A FAX.

25

POLLING QUESTION # 3

DO YOU (LAWYER) / YOUR HIRED COUNSEL (IF CE) HAVE SECURITY MEASURES IN PLACE FOR CONFIDENTIAL INFORMATION AT REST AND IN TRANSIT?

1. YES
2. NO
3. DON'T KNOW

26

WHAT SHOULD CLIENTS EXPECT?

- ARE YOU TECHNOLOGICALLY COMPETENT TO REPRESENT THE CLIENT?
- DOES YOUR FIRM HAVE APPROPRIATE IT / SECURITY PROTECTIONS TO SAFEGUARD HIGHLY SENSITIVE INFORMATION (*i.e.* , IP, FINANCIAL INFORMATION)?
- DO YOU AS CE KNOW THE QUESTIONS TO ASK?

27

COMPETENCY & CONFIDENTIALITY
KNOW THE RISKS—CYBER-ATTACKS ON THE RISE

- SHANE M. MCGEE FROM MANDIANT CORP: **LAW FIRMS ARE VULNERABLE AND THE PERFECT TARGET FOR ATTACKERS**
- NOVEMBER 17, 2009—FBI ISSUES ADVISORY REGARDING LAW FIRMS AND PR FIRMS BEING THE TARGETS OF SPEAR PHISHING E-MAILS. HTTP://WWW.FBI.GOV/SCAMS-SAFETY/E-SCAMS/ARCHIVED_ESCAMS
- JANUARY 2010—CALIFORNIA LAW FIRM GIPSON HOFFMAN & PANCIONE SUBJECT OF CYBER-ATTACK BY CHINA FOLLOWING THE FILING OF $2.2B LAWSUIT AGAINST CHINA AND OTHERS FOR COPYRIGHT INFRINGEMENT
- JANUARY 2015—CRAINE'S CHICAGO BUSINESS WARNS AGAINST PHISHING EXPEDITIONS USING "BIG NAME" LAW FIRMS AS BAIT TO INJECT MALWARE INTO FIRM SYSTEMS HTTP://WWW.CHICAGOBUSINESS.COM/ARTICLE/20150109/NEWS04/150109834/SCAMMERS-GO-PHISHING-USING-LAW-FIRMS-AS-BAIT

28

WHY LAW FIRMS ARE EASY TARGETS

- MOBILE LAWYERS & STAFF
  - UBIQUITOUS "PUBLIC" WIFI
  - NO VPN
  - BYOD
- DIVERSE "WORK" VENUES
  - CONFERENCE CENTERS
  - HOTELS
  - HOME
  - FOREIGN TRAVEL
- INTERNET OF THINGS (IoT)
- LARGE IOLTA ACCOUNTS
- CLIENT TRADE SECRETS / IP
- CLIENT CONTACTS
- WEBSITE "SUCCESS STORIES"
- DOCUMENT MANAGEMENT SYSTEMS—LACK OF ENCRYPTION
- PCI COMPLIANCE

29

KNOW THE WHO'S AND HOW'S

- WHO: INTERNAL –V- EXTERNAL THREATS
- HOW:
  - POOR ACCESS CONTROLS
  - IMPROPER/WEAK AUTHENTICATION
  - INSUFFICIENTLY PROTECTED CREDENTIALS
  - POOR PATCH MANAGEMENT; WEAK TESTING
  - NO DEFINED SECURITY PERIMETER; LACK OF NETWORK SEGMENTATION
  - IMPROPER DEVICE CONFIGURATION; POOR MONITORING
  - LACK OF SECURITY AUDITS, LOGGING PRACTICES
  - WEAK ENFORCEMENT OF REMOTE LOGIN POLICIES
  - SPEARPHISHING (EMAIL WITH CORRUPT LINK)

30

LIABILITY FOR A BREACH

- FEDERAL LAW & REGS:
  - HIPAA/HITECH
  - FTC HEALTH BREACH NOTIFICATION RULE (ENTITIES NOT COVERED BY HIPAA, *I.E.*, VENDORS OF PERSONAL HEALTH RECORDS (PHRS), PHR-RELATED ENTITIES AND THIRD-PARTY SERVICE PROVIDER FOR A VENDOR OF PHRS OR A PHR-RELATED ENTITY).
  - GRAHAMM-LEACH-BLILEY ACT
  - OCC
  - PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)—ANYONE THAT ACCEPTS CREDIT CARD PAYMENTS
- STATE DATA BREACH LAWS
- GDPR
- CYBERSECURITY FRAMEWORK (NIST STANDARD)
- FRCP 37(E)—PRESERVATION OF ESI AND SPOLIATION

31

32

THE CE RELATIONSHIP WITH OUTSIDE COUNSEL

- CLEARLY DEFINE THE ROLE THAT OUTSIDE COUNSEL IS TO PLAY
  - IF YOU HAVE INTERNAL COUNSEL, WHO WILL LEAD?
  - HOW WILL DECISIONS BE MADE?
  - DEFINE ROLES BETWEEN COMPLIANCE, INTERNAL AND EXTERNAL COUNSEL UP FRONT TO AVOID CONFUSION AND POTENTIAL LOSS OF PRIVILEGE
- HOW WILL COMMUNICATIONS OCCUR?
  - AGREE WHAT WILL BE HANDLED VERBALLY
  - IMPLEMENT SECURE DOCUMENT TRANSMISSIONS AND STORAGE

33

THE CE RELATIONSHIP WITH OUTSIDE COUNSEL

- IF POSSIBLE, IDENTIFY POTENTIAL OUTSIDE COUNSEL RESOURCES BEFORE AN EVENT OCCURS
  - IDENTIFY WHO CAN BE USED UNDER YOUR CYBERSECURITY COVERAGE
  - CONSIDER A 'TRIAL RUN' WITH POTENTIAL FIRMS
  - CONSIDER CULTURAL AS WELL AS COMPETENCY 'FIT' WITH YOUR ORGANIZATION
  - ENSURE THEY UNDERSTAND THE RISK TOLERANCE OF YOUR ORGANIZATION
  - REVIEW THEIR INTERNAL CONTROLS
  - HAVE YOUR BAA IN PLACE

34

BA BEST PRACTICES

- KNOW YOUR CE'S EXPECTATIONS & PRACTICES (COMMON GOALS)
- KNOW YOUR RISKS (PHYSICAL PLANT, INFORMATION SYSTEMS & WORKFORCE)
- SEGREGATE & SECURE HIGH RISK INFORMATION, OPERATIONS & WORKERS
- ENCRYPT SENSITIVE DATA/IMPLEMENT ROBUST PASSWORD POLICY (DUALFACTOR)/VPN
- ROBUST TRAINING OF WORKFORCE
- INCORPORATE SECURITY BY DESIGN
- ACQUIRE CYBER LIABILITY INSURANCE ($1M MIN)
- ENABLE NETWORK SECURITY MONITORING & REVIEW OF LOG FILES (LESSON LEARNED FROM TARGET)
- DEMAND COMPLIANCE FROM CONTRACTORS & SUPPLIERS (ANOTHER LESSON FROM TARGET)

35

BEST PRACTICES

- CONDUCT TABLE-TOP DRILLS
- HAVE EXPERTS AT THE READY IF/WHEN AN ATTACK OCCURS
- RESTRICT / SECURE REMOTE ACCESS
- ENFORCE PASSWORD POLICIES
  - CHANGE FREQUENTLY
  - PASS-PHRASE V PASSWORD
- RESTRICT ACTIVITIES ON POS SYSTEMS TO SALES
- DEPLOY ANTI-VIRUS SYSTEMS ON POS
- FOR LARGE, MULTI-SITE COMPANIES
  - SEGMENT POS NETWORK FROM CORPORATE NETWORK
  - MONITOR NETWORK TRAFFIC FROM POS TO NETWORK
  - USE TWO-FACTOR AUTHENTICATION

36

BEST PRACTICES

- **ELIMINATE UNNECESSARY DATA** (ENFORCE MINIMUM NECESSARY FROM CE)
- COLLECT, ANALYZE & SHARE INCIDENT DATA
- COLLECT, ANALYZE & SHARE TACTICAL THREAT INTELLIGENCE, ESPECIALLY INDICATORS OF COMPROMISE
- FOCUS ON BETTER & FASTER DETECTION
- ESTABLISH METRICS: "NUMBER OF COMPROMISED SYSTEMS" & "MEAN TIME TO DETECTION" IN NETWORKS; USE METRICS TO DRIVE SECURITY
- EVALUATE THREAT LANDSCAPE TO PRIORITIZE TREATMENT STRATEGY (IT'S NOT A "ONE-SIZE FITS ALL" WORLD)
- TRACK WORKFORCE: WHO'S WHO, WHAT THEY DO & WHEN THEY GO

37

Debra A. Geroux, JD, CHC, CHPC
Shareholder
Butzel Long, a professional corporation
geroux@Butzel.com

Joan Podleski, CCEP, CHC, CHPC, CHRC
Chief Privacy Officer
Children's Health
Joan.Podleski@childrens.com

38