ESQUIRE CLE: Information law firms collect and store – what to do in the event of a cyber breach?

1. Introduction & Overview
    a. **DISCLAIMER – NOT LEGAL ADVICE**
    b. Isabella – Chief Compliance Officer, AGC @ District Medical Group
    c. Denise – Chief Risk Officer, AGC @ District Medical Group
    d. OVERVIEW: *Depending on area of law your firm practices you could house protected, confidential, and sensitive information such as*
        - health care/malpractice/personal injury - patient information, behavioral health and substance abuse information, genetics testing, HIV/STD diagnoses;
        - banking/financial – biometric (like fingerprint), SSN, DOB, contact information;
        - students/schools – as above plus any IEP or development plans;
        - trusts/estates – healthcare, banking financial information as discussed above
    e. Our EXPERIENCE – overview of a breach event and ***do you know what to do in the event of a cyber breach?***

2. Where and how does your organization or law firm store and send information?
    a. Store on paper
    b. Store digitally
        - Personal or work issued laptop
        - Shared computer workstation
        - System, files, or vendor application
        - One size does NOT fit all (i.e. size of firm and number of staff, applications used, servers or cloud, IT support – in house or contracted, patches up-to-date, current technology, balance between green practices and advances in technology with best-in-class privacy practices)
    c. When sending/receiving information consider
        - Email encryption – protected, legally compliant communication. Drop box encrypted
        - Phishing/Social Engineering/Imposters/Deep fakes (pretend to be the finance department)
        - What about texting policies and encryption?
    d. Most of us, its digital storage SO need to
        - understand and comply with laws and regulations governing information AND
        - conduct a risk assessment and write a plan to prevent a cyber breach
        - *ISABELLA start with review applicable laws & regulations*

3. Laws and Regulations
    a. Federal laws related to area of practice
    b. HIPAA, PHI, Covered Entity (CE), Business Associate, BAA)
    c. FTC, HITECH
    d. Consumer information
    e. Gramm-Leach Bliley Act (GLBA) – financial institutions
    f. FERPA – student information
    g. COPPA – market online to children <13 y.o.
    h. State laws related to area of practice (NY – Shield, CA – CCPA)
    i. Across state lines (i.e. properties in 2 states, CA, CT, NY)
    j. OCR guidance (< 500 over >500)
    k. GDPR (International clients)

ESQUIRE CLE: Information law firms collect and store – what to do in the event of a cyber breach?

4. Risk assessment and plan
    a. Our organization used Enterprise Risk Management (ERM) program based on 8 domains (i.e. human capital, information technology, legal/compliance, hazards/risks)
    b. Risk assessments – evaluate policies, procedures, and processes(triple P) AND support compliant environments and practices
    c. Risk plan – assists team or law firm in learning and then knowing what to do in the event of a cyber event or cyber breach
    d. Risk assessment and plan should include your due diligence in the evaluation of:
        - Legal obligations under the law, but also contractual obligations
        - Third party vendors (i.e. subcontractors) due diligence
        - Information sharing via email or e-sign
        - Cyber insurance policy - coverages and exclusions and conversation with broker
        - Legal hold policy and process (spoliation)
        - Education provided - Phishing/Social Engineering/Imposters/Deep fakes (pretend to be the finance department)
        - Employee knowledge of policies, procedures, and practices = everyday people terms. NOT THE TIME for legal ease.
        - Outsourced staff (paralegal, answering service, IT support) = know required by triple P
        - Access controls (physical [person or vendor follows employee into the building w/o badging], administrative [papers on desk]), technical [all things computer])
        - Employee terms and role changes (timely discontinuation of access)
        - If confidential information to the wrong person – how do you respond
        - Environment = no retaliation for reporting potential deviations from triple P
        - WHAT IF THE B WORD HAPPENS = Breach
        - *Pass it over to Isabella to discuss -*
          The notification process & requirements & statutory time-period for compliance

5. Breach – no such thing as too much preparation or due diligence!
    a. ABA model rule 1.6 – confidentiality of information
    b. What is a breach? Hack? Defined.
    c. Notify your internal team/leaders.
    d. Notify insurance carrier (get a breach coach, IT security investigation)
    e. Notify patients, clients students,
        - Healthcare – notify covered entity
        - Finance – GLBA and state law/regulations
        - School – FERPA and state law/regulations

2. Future trends and wrap up lessons learned
    a. ESG movement and relationship to breach
    b. Role AI – plain language, do due diligence
    c. LESSONS LEARNED from breach event?
        - Value of a good risk assessment & plan = ability timely respond to event/Breach
        - Use resources provided by broker/insurance carrier (education and support)
        - HOTWASH, post mortem, lessons learned
        - TABLETOP – mirrored Breach incident