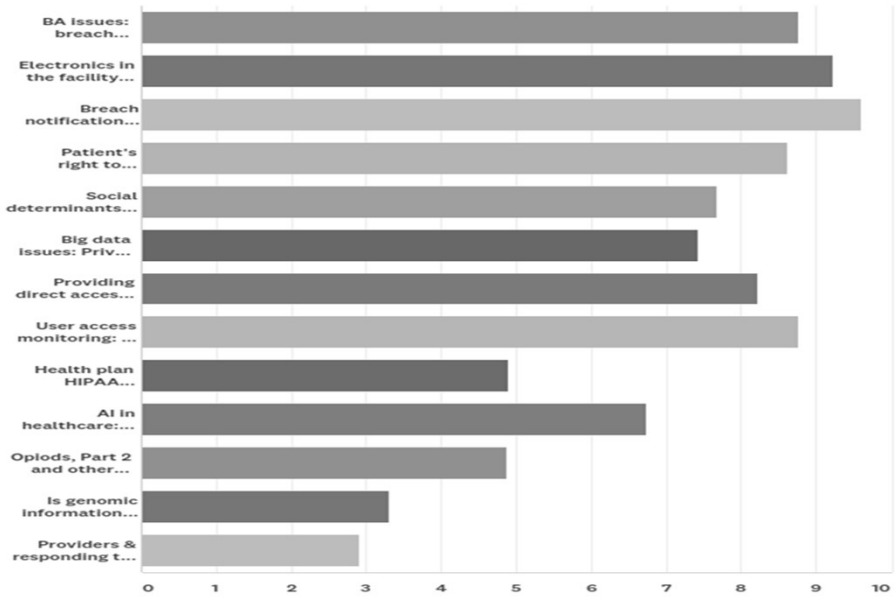
# PRIVACY OFFICER'S ROUNDTABLE

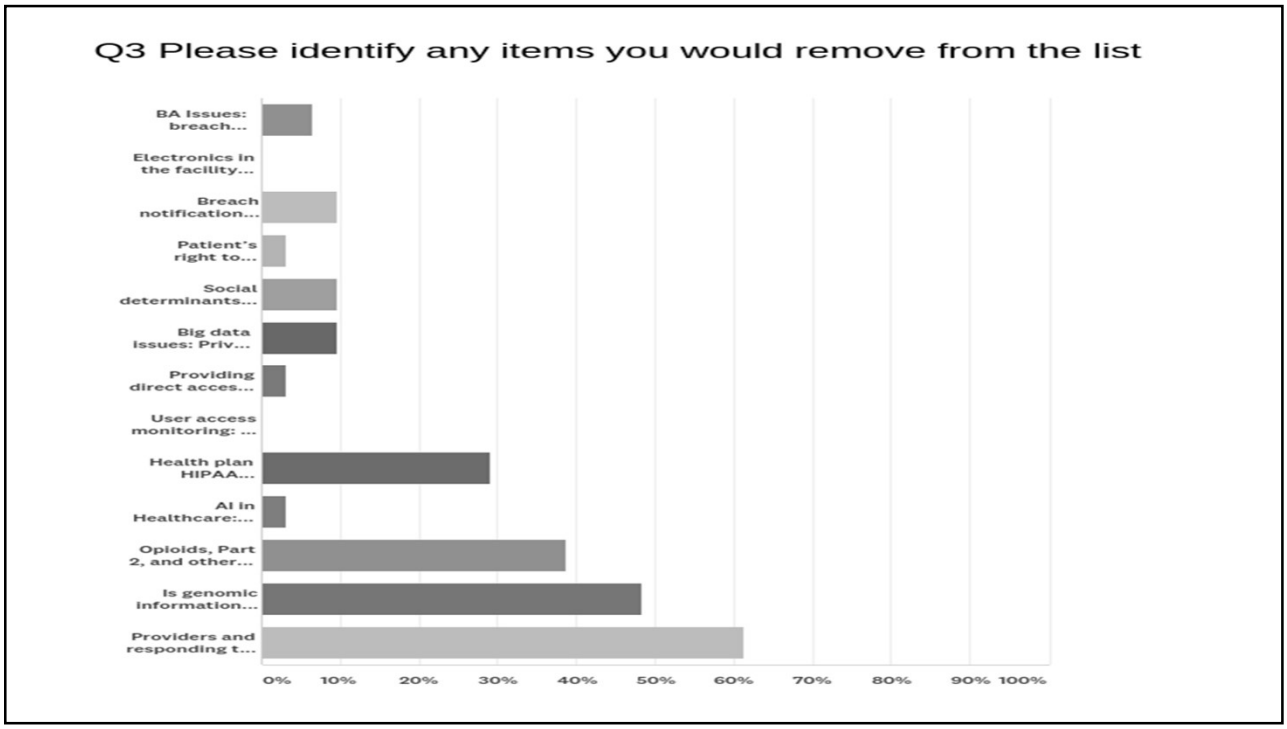
## BETTER KNOW AS THE SESSION WHERE YOU DO ALL THE WORK!

1

Q1 Please rank the following topics by order of importance to you




2




3

# REVISED LIST IN ORDER OF PRIORITY

Breach notification: Changes to state laws & interactions with HIPAA & continuing questions the HIPAA breach risk assessment

Electronics in the facility: Use of smart-speakers (Alexa, Echo, etc.), smartphones & cameras by patients, visitors, law enforcement, & the covered entity

Tie - BA issues: breach notification timing & responsibilities, BA's user access monitoring, direct access to EHR, de-identification of CE's PHI for BA use, etc.

Tie - User access monitoring: How much is enough?

Patient's right to access: CIOX case, OCR enforcement, & other issues

Providing direct access to the EHR for non-BA, non-provider 3rd parties (Health plan, social service orgs. etc.)

4

## REVISED LIST IN ORDER OF PRIORITY

- Social determinants of health: Sharing PHI with social services & other organizations to benefit the patient
- Big data issues: Privacy when partnering with 3rd parties like Google, Amazon, etc., & sharing data for research
- AI in healthcare: privacy and security concerns
- Tie - Health plan HIPAA compliance issues: Is anyone looking at the self-funded group health plan?
- Tie - Opioids, Part 2 and other behavioral health issues
- Is genomic information alone considered identifiable?
- Providers & responding to a bad Yelp review: What can a covered entity do?

5

## ADDITIONAL QUESTIONS LIGHTENING ROUND

- Direct access to your EHR by non-BA, non-provider 3rd parties
- Sharing PHI with social services & other organizations
- Big data: Privacy & partnering with 3rd parties
- AI in Healthcare
- Part 2 and other behavioral health issues

6

# CORONAVIRUS: PRIVACY AND SECURITY ISSUES



7

## CORONAVIRUS

- When is COVID-19 information PHI?
- When can you disclose <u>negative</u> test results?
- To whom can you disclose employee-patient COVID-19 information?

8

# POLLING QUESTION 1

"On March 27th, XYZ Medical Center had a confirmed COVID-19 case." Assume that there are not public media reports identifying the COVID-19 case. Is this PHI?

- Yes
- No

9

# POLLING QUESTION 2

A patient's family member is concerned about the patient in the next bed coughing excessively. The patient in the next bed tests negative for COVID-19. Can you inform the patient's family member the neighboring patient tested negative to put her at ease?

- Yes
- No

10

# POLLING QUESTION 3

An employee has come in as a patient & tested positive for COVID-19, but was sent home with mild symptoms. You have notified everyone who was exposed to the person. The employee's supervisor was not in contact with the employee over the past 2 weeks. Can you inform the employee's supervisor?

- Yes
- Maybe under some circumstances
- No

11

# BREACH NOTIFICATION: CHANGES TO STATE LAWS & INTERACTIONS WITH HIPAA & CONTINUING QUESTIONS THE HIPAA BREACH RISK ASSESSMENT

12

12

# BREACH NOTIFICATION ISSUES

- Performing the breach assessment
  - Who is involved
  - Process, consistency and documentation
- Defining "low probability of compromise"
- Tracking trends
- Keeping leadership informed

13

# BREACH ASSESSMENT PROCESS

- Who is involved in the process
  - Privacy officer or staff only
  - Multi-department team
  - Legal – in or out
- What is your process
  - Do you use a consistent form or numeric scoring system
  - How do you document your rationale for notification/no notification
  - How do you ensure internal consistency
- Does the number of affected individuals make a difference

14

# "LOW PROBABILITY OF COMPROMISE"

- Must review the 4 key breach risk assessment factors
- Should not be based on risk of harm
- Exceptions
- Disclosures to another CE
- Is inappropriate access always reportable
- Is ransomware of encrypted data a reportable breach

15

# TRACKING TRENDS

- Aggregate numbers
- Year to year and period to period trends
- Sort by operational unit
- Sort by type of breach (verbal, written, electronic, EMR access)
- Sort by risk areas (registration errors; giving papers to the wrong individuals, etc.)
- Sort by source of report (hotline, internal report, patient/customer)

16

# POLLING QUESTION 4

- Who do you inform about breaches?
  - Local management of area where the 'error' occurred
  - Senior leadership
  - C-suite
  - Audit Committee or Board
  - All of the above
  - None of the above

17

# STATE BREACH NOTIFICATION LAW ISSUES

- Analyzing under HIPAA versus state law which comes first
- Increasing trend of adding medical/health information to state breach laws.
- HIPAA exemption? Full, partial (e.g., only applies to content requirements), or none.
- Timing confusion. When partial HIPAA exemption, is timing based on the state law or HIPAA.
- Legislative jurisdiction questions – when does another state's law apply?

18

# POLLING QUESTION 5

You suffer a breach that involves a Massachusetts resident. You don't have any minimum contacts in Massachusetts. Do you notify the Massachusetts AG?

- Yes
- No

19

# ELECTRONICS IN THE FACILITY: USE OF SMART-SPEAKERS, SMARTPHONES & CAMERAS BY EVERYONE

20

20

# POLLING QUESTION 6

- Does your organization use smart-speakers?
  - Yes
  - No
  - I don’t know

21

# POLLING QUESTION 7

- Does your organization allow patients to bring in smart-speakers?
  - Yes
  - No
  - I don’t know

22

# ELECTRONICS IN THE FACILITY

- Issues
  - Who owns the device?
  - Who has the legal liability for what the device records?
  - What are the potential benefits of using such devices to support care?
  - What is your process for approving?
  - Law enforcement body cams – still an issue


15

23

# POLLING QUESTION 8

- Do you have a policy on address law enforcement and their use of body cams in your organization?
  - Yes
  - No
  - I don't know

24

# BUSINESS ASSOCIATE ISSUES



25

## THE CHALLENGES

- Breach notification timing & responsibilities
  - Timeliness of notifications
  - Assistance in investigation/risk assessment
  - Indemnification for certain costs
  - Notifications to public
- BA's user access monitoring
  - Are they doing it?
  - What happens with findings?

26

# POLLING QUESTION 9

- Does your organization verify whether your BA's perform user access monitoring?
  - Yes
  - No
  - I don't know

27

# THE CHALLENGES

- Direct access to EHR
  - By your business associates
  - By the business associates of other contracted parties
- De-identification of CE's PHI for BA use
  - Do you permit it?

28

# POLLING QUESTION 10

- Does your organization allow BA's and the BA's of affiliated third parties to access your EHR directly?
  - Yes for both
  - Yes for your BA's only
  - No for both
  - No for BA's of third parties
  - I don't know

29

# POLLING QUESTION 11

- Does your organization allow BA's to de-identify the PHI of your organization for their own use?
  - Yes
  - No
  - Sometimes, is it situational
  - I don't know

30

# USER ACCESS MONITORING: HOW MUCH IS ENOUGH?





## ACCESS MONITORING ISSUES

- Selection Criteria – what do you want to monitor
- Resources – what does it take to do the work
- Findings – be prepared to deal with everything you find!

## ACCESS MONITORING ISSUES – SELECTION CRITERIA

- What do you monitor
  - Random vs. risk adjusted
  - Special protections/sensitive records
  - Employee risk areas
    - Access to own records
    - Access to extended family
    - Access to co-workers

33

## ACCESS MONITORING ISSUES - RESOURCES

- How regularly do you plan to monitor
- What resources do you have and what can you afford to buy
  - Do you have staff to effectively do the work – 'spin-off investigations'
  - Do you use an external vendor
  - Do you purchase special use EMR monitoring software

34

# POLLING QUESTION 12

- Does your organization use any of the following for monitoring?
  - Built-in reports from your EMR system
  - Vendor system for EMR access audits (Protenus, Fair Warning, Maize, etc.)
  - Outsource vendor for all or part of access audits
  - None of the above

35

# ACCESS MONITORING ISSUES - FINDINGS

- Expect the number of reportable breaches to go up
- Warn the organization what's coming before you start
  - Senior leadership
  - Key operational leaders
  - HR
  - Legal
- If a risk or a violation is identified, it MUST be addressed

36

# PATIENT'S RIGHT TO ACCESS



37

## PATIENT'S RIGHT TO ACCESS

- CIOX case
- OCR enforcement
- Other issues

38

# POLLING QUESTION 13

If a patient requests disclosure of hard copy protected health information to a third party and cites 45 C.F.R. § 164.524 (the right of access), do you require a full HIPAA-compliant authorization?

- Yes
- No

39

# POLLING QUESTION 14

If a patient requests disclosure of hard copy protected health information to a third party and cites 45 C.F.R. § 164.524 (the right of access), do you charge the state fee schedule (even though higher than actual costs)?

- Yes
- No

40

# CONTACT INFORMATION

Adam Greene, Partner

David Wright Tremaine

adamgreene@dwt.com (202) 973-4213

Joan Podleski, Chief Privacy Officer

Children's Health of Texas
joan.podleski@childrens.com 214.456.6068

Marti Arvin, Executive Advisor

Cynergistek, Inc

Marti.Arvin@cynergistek.com 512-402-8550, ext 7051

41