

# WHAT COVID-19 AND OTHER CHANGES MEAN FOR YOUR PRIVACY IMPACT ASSESSMENT

HCCA | June 12, 2020

UC San Diego **BBK** **BDO**  
 CAMPUS PRIVACY OFFICE BEYOND BOUNDARIES ATTORNEYS AT LAW

1

## Introductions



**LEEANN HABTE**  
Partner

(213) 787-2572  
[leeann.habte@bbklaw.com](mailto:leeann.habte@bbklaw.com)  
 bbklaw.com



**PEGAH PARSI**  
Campus Privacy Officer

(858) 822-4439  
[pparsi@ucsd.edu](mailto:pparsi@ucsd.edu)  
 privacy.ucsd.edu



**SHIRLEY KOMOTO**  
Senior Manager, BDO

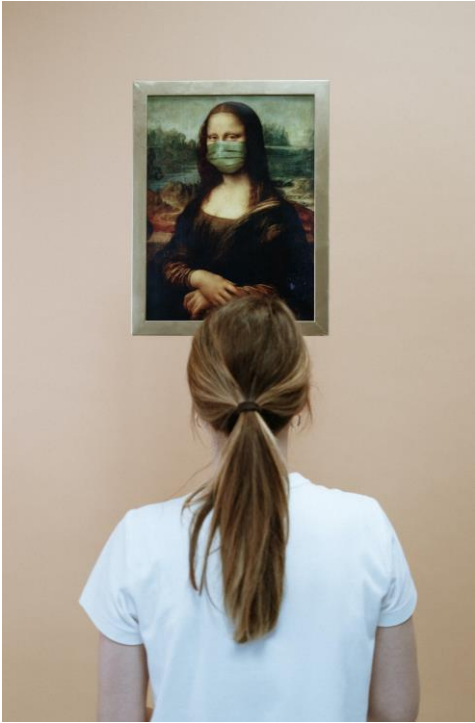
(310) 557-0300  
[skomoto@BDO.com](mailto:skomoto@BDO.com)  
 bdo.com

2 [www.bdo.com](http://www.bdo.com)



UC San Diego **BBK** **BDO**  
 CAMPUS PRIVACY OFFICE BEYOND BOUNDARIES ATTORNEYS AT LAW

2



## Agenda

- Privacy Landscape: Recent Changes & COVID-19 Impact
- COVID-19 Privacy Case Study: University of California, San Diego
- A Structured Approach to Privacy: Privacy Impact Assessment



3

## PRIVACY LANDSCAPE

Recent Changes & COVID-19 Impact

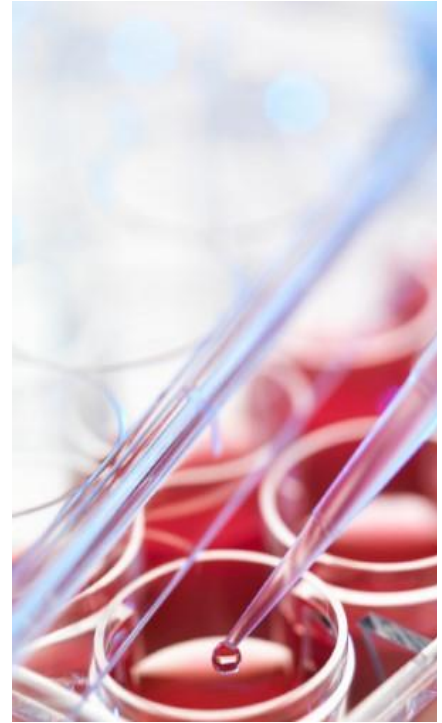


4

## Polling Question #1

How would you describe your organization?

1. Health plan
2. Hospital or health system
3. Pharmacy
4. Pharmaceutical or medical device/diagnostics company
5. Physician practice
6. Skilled nursing, rehab or long term care facility
7. Academic medical center
8. Other

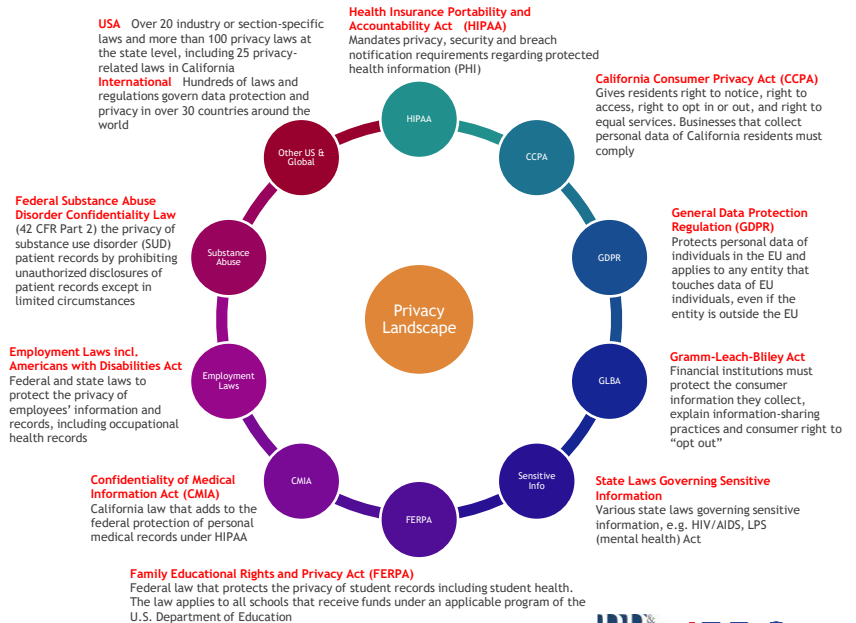


5

## The Privacy Landscape Not Just HIPAA

Data travels the world through borderless networks and the ways in which personal information is collected and used continues to transform. In response, the number of privacy laws has grown exponentially in recent years - hundreds of laws in over 30 countries.

Privacy can no longer be the domain of a single department or group. Privacy is more than HIPAA.



Note: this is for illustrative purposes only and is not intended to be inclusive of all US or global privacy laws and regulations.



6

## Recent Changes to Data Privacy Laws

### California Consumer Privacy Act - Effective January 1, 2020

- ▶ Grants new rights to California residents
  - The right to know what personal information is collected, used, shared or sold, both as to the categories and specific pieces of personal information
  - The right to delete personal information held by businesses and by extension, a business's service provider
  - The right to opt-out of sale of personal information
  - Children under the age of 16 must provide opt in consent, with a parent or guardian consenting for children under 13
  - The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA
- ▶ For those following CCPA, the final proposed regs were submitted to the California Office of Administrative Law (OAL) June 1<sup>st</sup>, 2020. The Rulemaking file can be found here: <https://www.oag.ca.gov/privacy/ccpa>
  - The OAL has 30 working days, plus an additional 60 calendar days under Executive Order N-40-20 related to the COVID-19 pandemic, to review the package for procedural compliance with the Administrative Procedure Act. Once approved by the OAL, the final regulation test will be filed with the Secretary of State and become enforceable by law
- ▶ Regulations continue to undergo modifications but enforcement begins on July 1, 2020
  - Proposed rules issued in October 2019, February 2020, and March 11, 2020
  - Final rule expected October 1, 2020

7

UC San Diego  
CAMPUS PRIVACY OFFICE

IBBk  
BANKING & FINANCIAL  
ATTORNEYS AT LAW

BDO

7

## Recent Changes to Data Privacy Laws

### California Consumer Privacy Act - Effective January 1, 2020

- ▶ Applies to certain businesses
  - Has gross annual revenues in excess of \$25 million
  - Buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices
  - Derives 50 percent or more of annual revenues from selling consumers' personal information
- ▶ Exempts many health care entity categories
  - **Common Rule Exemption.** Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects (also known as the "Common Rule") pursuant to good clinical practice guidelines is exempt from CCPA
  - **Medical Information and PHI Exemption.** "Medical information" governed by California's Confidentiality of Medical Information Act (CMIA) and "protected health information" (PHI) collected by a covered entity or business associate under HIPAA is exempt from HIPAA
  - **Provider and Covered Entity Exemption.** CCPA does not apply to a provider of health care governed by CMIA or a covered entity governed by HIPAA to the extent the entity maintains patient information in the same manner as CMIA and HIPAA. This exemption does not currently include "business associates" under HIPAA



8

UC San Diego  
CAMPUS PRIVACY OFFICE

IBBk  
BANKING & FINANCIAL  
ATTORNEYS AT LAW

BDO

8

## Recent Changes to Data Privacy Laws

### California Consumer Privacy Act

- ▶ Exemptions Do Not Cover
  - Health information collected directly from individuals (e.g., via an app) is not PHI if it is not created or received by or on behalf of a health care provider or plan.
  - The definition of personal information under CCPA is broad and includes inferences drawn from information. If inferences drawn from PHI are used to create a second data set, CCPA may apply to this new data set.
  - Certain data outside the scope of PHI, including information collected via cookies as well as collection of geolocation data via a website or app.
  - PHI used for research purposes that does not meet the standard of a clinical trial subject to the Common Rule.
  - PHI de-identified in accordance with HIPAA is no longer PHI and thus no longer carved-out of CCPA compliance. The de-identification standard under CCPA is higher.

## Recent Changes to Data Privacy Laws

### Coronavirus Aid, Relief, and Economic Security Act (CARES Act) - Changes to Substance Use Disorder Privacy Law <https://www.congress.gov/116/bills/s3548/BILLS-116s3548is.pdf>

- ▶ Amends the statutory authority for disclosures with patient consent to provide that once a patient gives prior written consent, the contents of a record “may be used or disclosed by a covered entity, business associate, or a [Part 2 program] for purposes of treatment, payment, and health care operations as permitted by the HIPAA regulations.”
- ▶ Redisclosures may then be made in accordance with HIPAA, until the patient revokes the consent.
- ▶ Adds requirements consistent with HIPAA for:
  - Breach Notification
  - Civil and Criminal Penalties
  - Notice of Privacy Practices
  - Accounting of Disclosures
- ▶ Regulations in 12 months



## COVID-19 Impact on Privacy Practices During Public Health Emergency

California Law - Governor Newsom's Suspended a Wide Range of Enforcement Related to Good Faith Use of Telehealth <https://www.gov.ca.gov/wp-content/uploads/2020/04/4.3.20-EO-N-43-20.pdf>

- ▶ Requirements to obtain verbal or written consent (Business & Professions Code § 2290.5(b).)
- ▶ Penalties and causes of action arising out of section 56.35; administrative fines, civil penalties, and private right of action and other causes of action specified in Civil Code § 56.36 (CMIA)
- ▶ Civil penalties related to timely notification to patients of a breach of the security system (Civil Code § 1798.29 and 1798.82)
- ▶ Extension of deadlines for notification to the Department of Public Health and to patients of breach of medical information from 15 days to a period of 60 days and suspension of administrative penalties (Health & Safety Code § 1280.15)
- ▶ Administrative penalties related to safeguards of health information (Health and Safety Code § 1280.17)
- ▶ Criminal penalties specified to persons who knowingly release or possess information about Medi-Cal beneficiaries and related cause of actions (Welfare and Institutions Code § 14100.2(h))

11

11

UC San Diego  
CAMPUS PRIVACY OFFICE

IBBk  
BANK OF AMERICA  
ATTORNEYS AT LAW

BDO

## COVID-19 Impact on Privacy Practices During Public Health Emergency

### Substance Abuse and Mental Health Services Administration (SAMHSA)

*"There has been an increased need for telehealth services, and in some areas without adequate telehealth technology, providers are offering telephonic consultations to patients. In such instances, providers may not be able to obtain written patient consent for disclosure of substance use disorder records. ... Under 42 U.S.C. §290dd-2(b)(2)(A) and 42 C.F.R. §2.51, patient identifying information may be disclosed by a part 2 program or other lawful holder to medical personnel, without patient consent, to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained."* <https://www.samhsa.gov/sites/default/files/covid-19-42-cfr-part-2-guidance-03192020.pdf>

### U.S. Equal Employment Opportunity Commission (EEOC)

- ▶ EEOC issues guidance on pandemic preparedness in the workplace and provides guidance on what an employer can and cannot do with regards to COVID-19 testing and information
- ▶ What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws, <https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws>

12

12

UC San Diego  
CAMPUS PRIVACY OFFICE

IBBk  
BANK OF AMERICA  
ATTORNEYS AT LAW

BDO

## COVID-19 Impact on Privacy Practices During Public Health Emergency

### HIPAA Notices of Enforcement Discretion During Nationwide Public Health Emergency

- ▶ The U.S. Department of Health and Human Services Office of Civil Rights (HHS-OCR) will not impose penalties for noncompliance with the security requirements under the HIPAA Rules:
  - For telehealth remote communications (using non-public facing apps)
  - In connection with the good faith participation in the operation of **COVID-19 testing sites** during a public health emergency
  - OCR HIPAA Announcements Related to COVID-19, <https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html>

### Guidance on Disclosure of PHI During Public Health Emergency

- ▶ **Release of Data to 911 and Other First Responders:** Clarifies that covered entities may disclose PHI such as the name or other identifying information about an individual who has been infected with, or exposed to, COVID-19, with law enforcement, paramedics, other first responders, and public health authorities without the individual's HIPAA authorization, in certain circumstances, including when first responders may be at risk of infection.

13

13



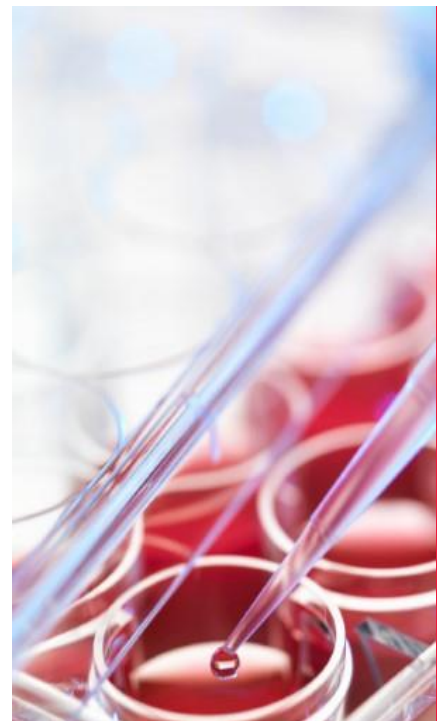
## Polling Question #2

Aside from HIPAA, for which of the following personal information is your privacy/compliance program responsible:  
(select all that apply)

1. Employee information
2. Website privacy
3. Third party vendor practices
4. Mobile applications and wearables
5. Research information

14

14



# COVID-19 PRIVACY CASE STUDY

University of California, San Diego



15

## UC San Diego on March 13<sup>th</sup>, 2020

- ▶ 39,000 students in wide array of fields such as medicine, engineering, marine sciences, and the arts
- ▶ UC San Diego Health, School of Medicine, and Skaggs School of Pharmacy
- ▶ Largest employer in town: 36,000 employees
- ▶ \$5 billion in revenues; \$1.35 billion in research funding
- ▶ Preparing for Winter Quarter final exams beginning the next day

16

16







## UC San Diego on March 16<sup>th</sup>, 2020

- ▶ Fully remote on Day 2 of final exams!
- ▶ 5,000 students in isolation on campus
- ▶ UC San Diego Health became a key part of the San Diego County's COVID response



17

## Evolving Privacy Challenges

### Day One Issues

- ▶ Health disclosures to public health
- ▶ What can we ask employees? Students?
- ▶ Online exams, online proctoring

### Day Two Issues

- ▶ Zoom, Zoom, Zoom
- ▶ Online instruction, advising, work
- ▶ Student health, counseling

### Day Three Issues

- ▶ Analytics: students, patients, employees
- ▶ Changed legal risks (e.g., GDPR)

### Current Focus

### How to Reopen?

- ▶ Symptom Surveys/Monitoring
- ▶ Temperature checks
- ▶ Diagnostic testing
- ▶ Antibody testing
- ▶ Building/job site access, sign-ins
- ▶ Contact tracing/case investigations
- ▶ Proximity tracking
- ▶ Isolation housing

18

18



## Considerations Impacting Privacy

- ▶ Differing roles with regard to students, employees, public, patients
- ▶ Differing laws for student health vs. other patients
- ▶ Differing understanding of privacy during an emergency (aka, how to balance values)
- ▶ Rapidly changing landscape and program design
- ▶ Differing equity, diversity, and inclusion (EDI) impacts of portions of the reopening effort
- ▶ Students and employees in other states, other countries accessing systems
- ▶ Capacity of service providers to scale and provide adequate privacy and security
- ▶ Unclear data lifecycles and purpose specification
- ▶ Difficulty assessing data minimization
- ▶ So many chefs in so many kitchens: communication plan?

UC San Diego  
CAMPUS PRIVACY OFFICE

BBK  
BANKS & BONDURANT  
ATTORNEYS AT LAW

BDO

19

## A STRUCTURED APPROACH TO PRIVACY

Privacy Impact Assessment

UC San Diego  
CAMPUS PRIVACY OFFICE

BBK  
BANKS & BONDURANT  
ATTORNEYS AT LAW

BDO

20

## Consider Your Organization

Where are you now?



What have you seen?



What have you done?



How have you stayed current?



What obstacles have you encountered?

21

21

UC San Diego  
CAMPUS PRIVACY OFFICE

BBK  
BANKS & BREWER  
ATTORNEYS AT LAW

BDO

## What is a privacy impact assessment (PIA) and why does it matter?

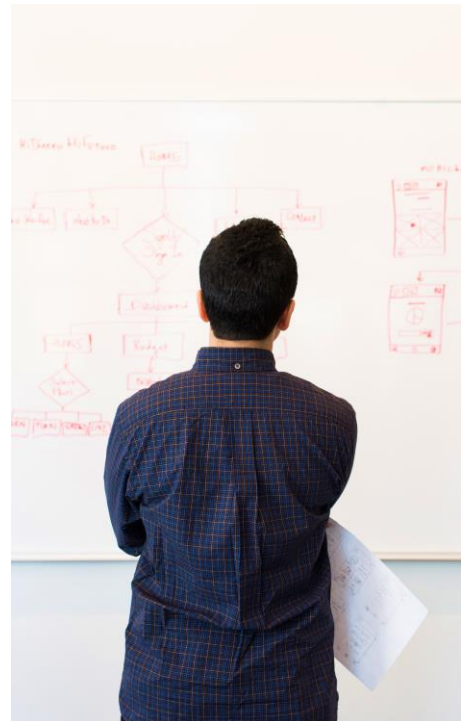
*A disciplined tool for spotting privacy and compliance risks, tracking implementation of privacy controls, and continuously assessing your changing privacy risk environment to protect individuals from inappropriate or inadvertent sharing of their personal information.*

Opportunities to...

- ▶ Pause to consider what and from where unforeseen challenges will arise
- ▶ Spot problems before they occur
- ▶ Educate users on source, use and disclosure of sensitive information
- ▶ Identify opportunities to avoid or reduce collection, storage and disclosure where possible
- ▶ Provide a record of due diligence in the event of a breach

22

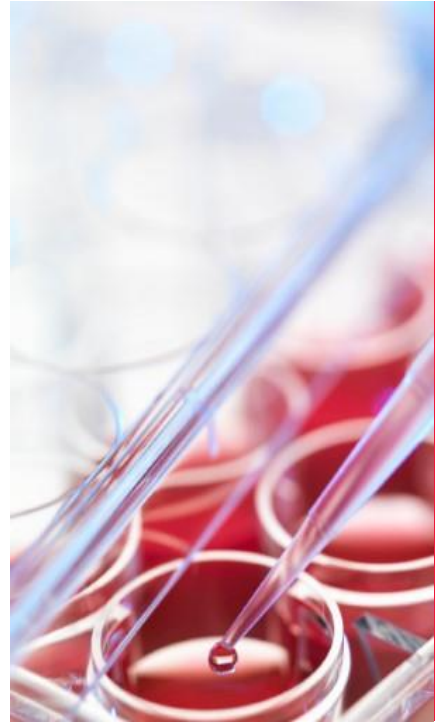
22



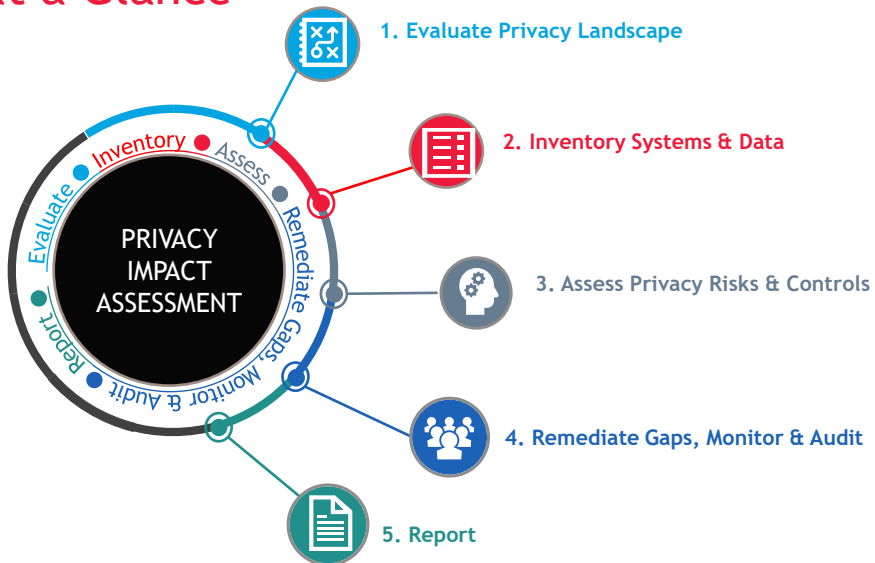
### Polling Question #3

How do you conduct your organization’s periodic privacy impact assessment?

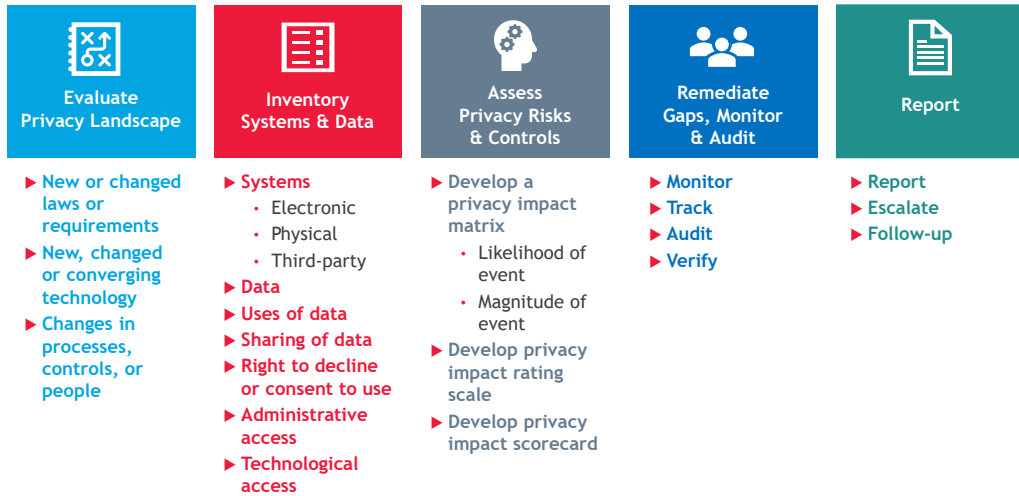
- 1. We use manual processes and tools
- 2. We use a tool from a third-party provider
- 3. Not sure
- 4. Do not perform



### PIAs at a Glance



## Our Privacy Impact Assessment Approach



25

25



## Privacy Impact Assessment and COVID-19

- ▶ Policies
- ▶ Monitoring
- ▶ Adjustments
- ▶ Acknowledgements
- ▶ Education
- ▶ Access changes
- ▶ Third-party risks



26

## Polling Question #4

What is the biggest challenge of COVID-19 as relates to privacy for your organization going forward? (pick one)

1. Supporting COVID-19 testing, reporting and tracing measures while adhering to privacy and record-keeping requirements
2. Changing threat landscape overall
3. Transforming workers to a remote environment
4. Staying on top of changing privacy requirements from state and federal governments
5. Unclear data lifecycles and purpose specification
6. Differing understanding of privacy during a rapidly evolving emergency



27



27

## Practical Privacy Looking Forward

 Public Policy Changes	 Contact Tracing & HCP Interface
 Changing Threat Environment	 Remote Working Issues

28



28

## Privacy in a COVID-19 World

*The future is uncertain, uncertainty propels change, and change diminishes controls*

WITHOUT A PIA



WITH A PIA



# ARE YOU READY?

29

29

# Questions?

30

30