May 6, 2020

Reducing Health Risk While Protecting Privacy:

How the Coronavirus Pandemic will alter privacy and security

Krista Cattanach
CVS Health

Ken Jones
FTI Consulting

Dan Caprio
The Providence Group

Ron Plesco
KPMG

Jim Halpert
DLA Piper

Doron Rotman
KPMG

Privacy+ Security Forum

Reducing Health Risk While Protecting Privacy during COVID-19

Privacy + Security Forum

- **Purpose of Session**

  Panel discussion about how privacy and security will evolve due to the Coronavirus Pandemic, including weighing public health risks against individual privacy and how cybersecurity threat actors have shifted focus

- **Focus on privacy and security**
  - Prior to the pandemic
  - During social distancing / quarantine
  - Our new normal “after” COVID-19

Part 1: Prior to the pandemic

Regulatory compliance; threats to personal and financial Information

Privacy+ Security Forum

Privacy

- Regulatory compliance: California Consumer Privacy Act (CCPA); State privacy laws (biometrics, breach, information security); federal legislation
- Privacy by design

Security

- Threat actor focus on exploiting sensitive personal information (e.g., credit cards, social security numbers)
- Risk-based Information security programs
- New technologies (e.g., cloud computing)

Part 2: During social distancing / quarantine

Federal and state waivers; critical system security and vulnerabilities

Privacy+ Security Forum

Federal waivers

- Covered Hospitals
- Telehealth
- Emergency personnel
- Community based testing sites
- BA disclosures for public health / health oversight

State bulletins / FAQs

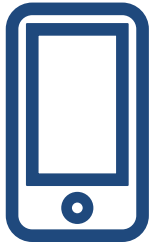
- Provider telehealth guardrails; public health reporting
- State breach laws still in force

Significant data being collected and disclosed

- Public health
- Employee safety
- Treatment
- Research

Use of new technologies

- Telehealth
- Widespread work-at-home
- Biometric devices / digital authentication



Threat actor shift to target critical systems

- Supply chains
- Healthcare
- Retail
- Agriculture

Likely Surge in Fraud

- COVID CARES Act programs
- Account takeovers via cyber intrusions
- Financial fraud (insider trading, financial advisors)

Part 3: Our new normal “after” COVID-19

Contact tracing; employee safety; retail

Privacy+ Security Forum

Implications for employee safety and privacy

- Phased approach to return to work
- Employee risk scoring, testing requirements
- Continued work-at-home options

Public Safety Measures

- Contactless payment / pickup at retail
- Temperature checks; testing

Contact Tracing: In the workplace and beyond

- Private development (Apple, Google)
- Individual right to privacy / consent
- Limits to accuracy and impact to individuals
- Data minimization

Features of Privacy and Security by Design Approach

- Legal review of applicable law (federal /state law privacy, health and employment law, Wicker?)
- Choose highly accurate tracking, testing, and screening techniques
- Transparency about what is collected, uses, disclosures
- Clear purpose specifications and reasonable use and retention limitations
- Bar secondary use of the information not reasonably related to COVID-19 prevention or not reasonably anticipated by data subjects, including commercial uses or disclosures
- Controls to avoid unintended discriminatory uses of information
- Robust security and confidentiality safeguards

Additional Considerations outside the Workplace

- Data minimization
- Transparent notice combined with affirmative consent, including how to withdraw consent
- Allow withdrawing consent as easily as consent was provided
- In California, only place app on employee personal device if the employee specifically requests that you do so, and document that request

Questions + Contact

Krista Cattanach
CVS Health
cattanachk@Aetna.com

Dan Caprio
The Providence Group
dcaprio@providencegroupdc.com

Jim Halpert
DLA Piper
jim.halpert@dlapiper.com

Ken Jones
FTI Consulting
Ken.Jones@fticonsulting.com

Ron Plesco
KPMG
rplesco@kpmg.com

Doron Rotman
KPMG
drotman@kpmg.com