HIPAA, Data Security and the Remote Workforce

HCCA Virtual Conference:
COVID-19 Essentials for Healthcare Compliance Programs

Tuesday, July 21, 2020
1:50 – 2:50 pm CDT

1

Speaker Introductions

Ashley Huntington, JD, CHC
Privacy Officer
Cook County Health

Mark Lanterman
Chief Technology Officer
ComputerForensic Services

Catie Heindel, JD, CHPC, CHPS
Managing Senior Consultant
Strategic Management, LLC

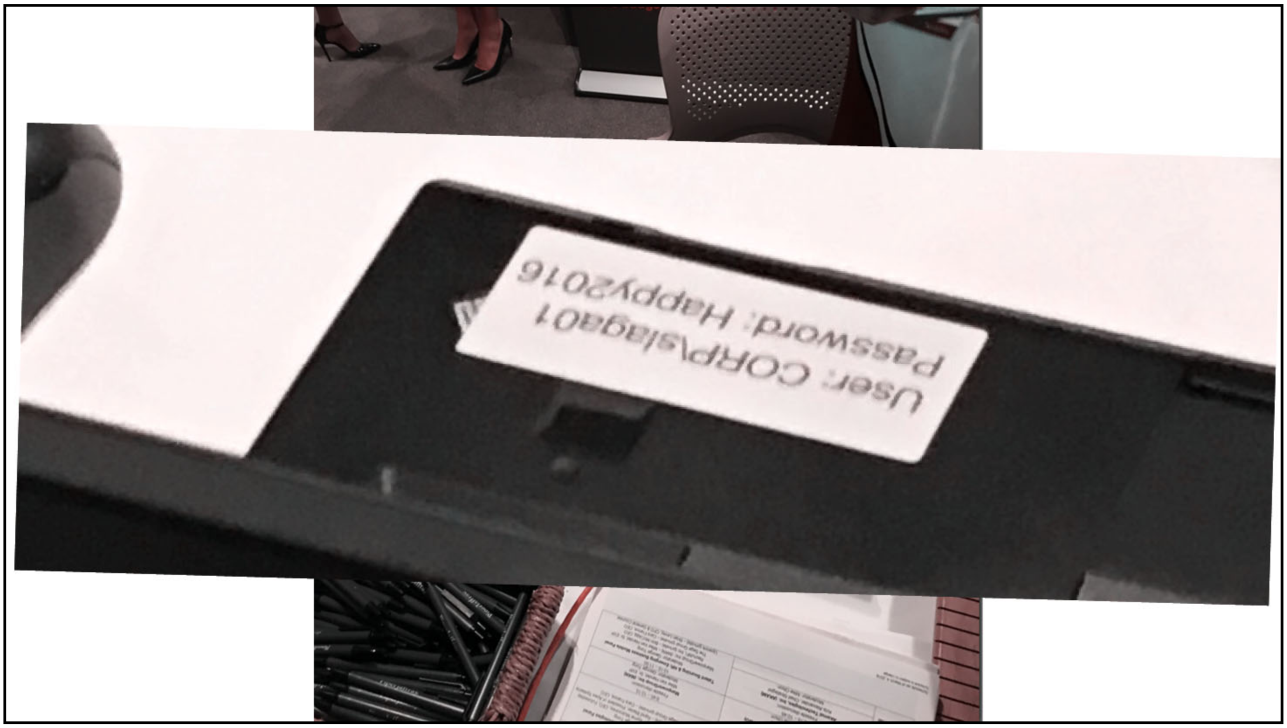
2

Today’s Agenda:

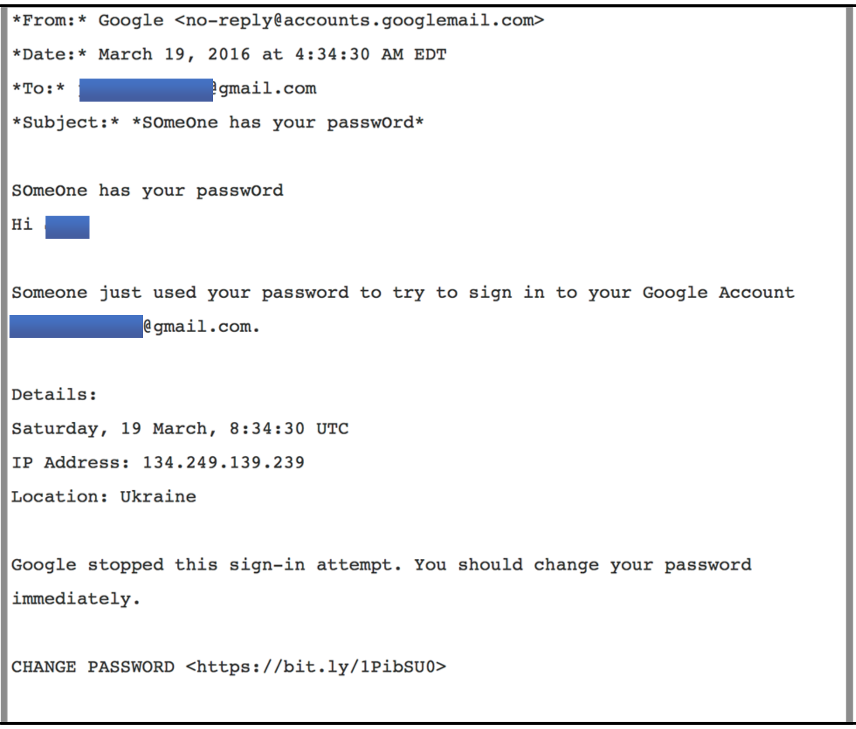
- Imagine with us … a data breach demonstration
- COVID-19 HIPAA considerations and workforce impact
- Strategies for defending against breaches and cyber attacks

3

4

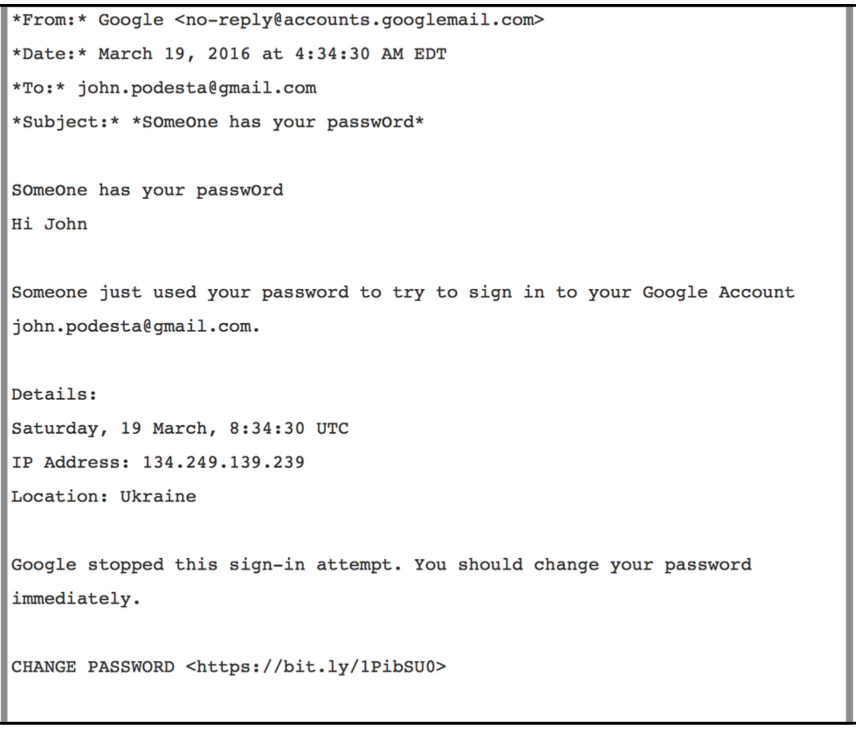


5



```
*From:* Google <no-reply@accounts.googlemail.com>
*Date:* March 19, 2016 at 4:34:30 AM EDT
*To:* [redacted]@gmail.com
*Subject:* *SOmeOne has your passwOrd*

SOmeOne has your passwOrd
Hi [redacted]

Someone just used your password to try to sign in to your Google Account
[redacted]@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password
immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>
```

6



From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: *SOmeOne has your passwOrd*

SOmeOne has your passwOrd
Hi John

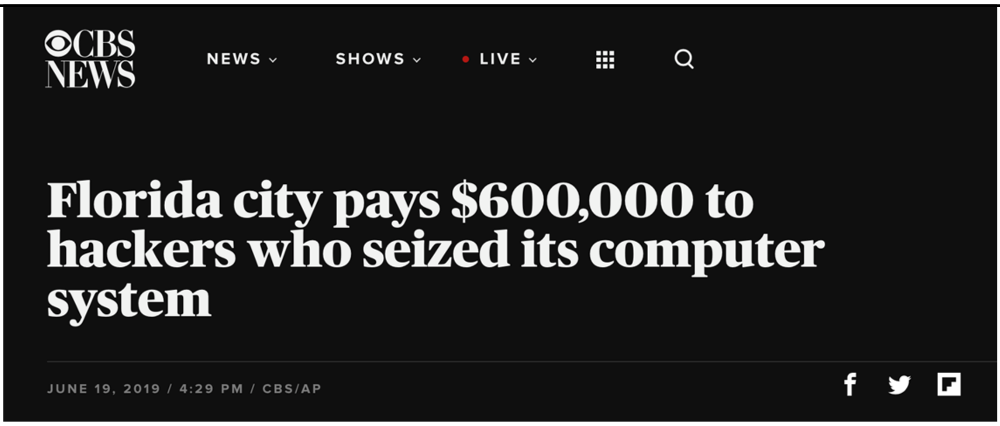
Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

7

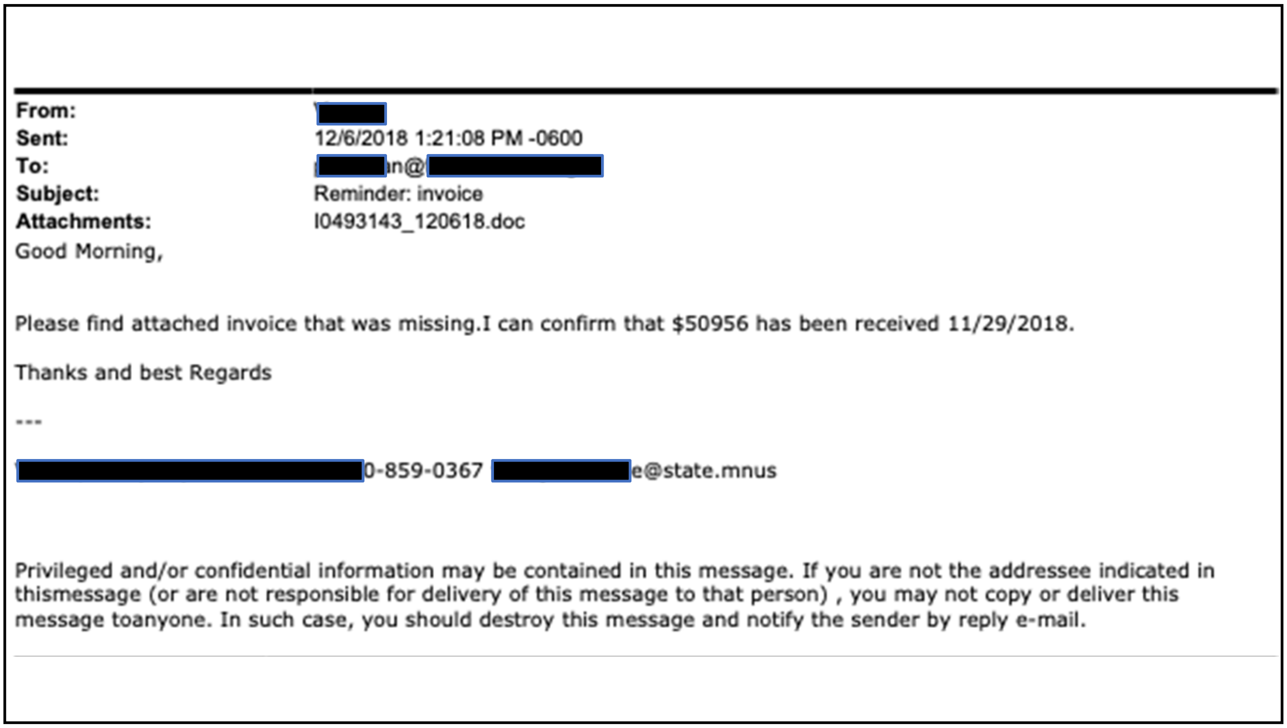


Florida city pays $600,000 to hackers who seized its computer system

JUNE 19, 2019 / 4:29 PM / CBS/AP

The hackers apparently got into the city's system when an employee clicked on an email link that allowed them to upload malware. The city had numerous problems, including losing its email system and 911 dispatchers not being able to enter calls into the computer.

8



From: [redacted]
Sent: 12/6/2018 1:21:08 PM -0600
To: [redacted]n@[redacted]
Subject: Reminder: invoice
Attachments: I0493143_120618.doc

Good Morning,

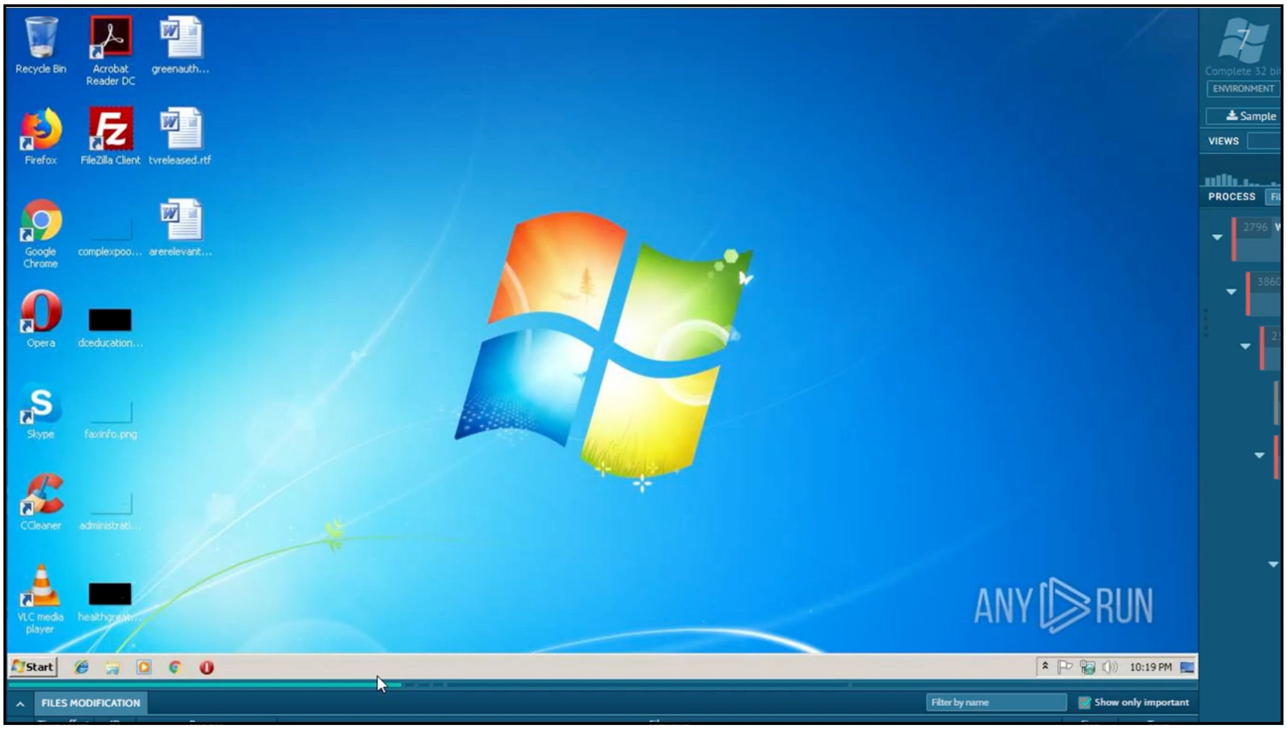
Please find attached invoice that was missing.I can confirm that $50956 has been received 11/29/2018.

Thanks and best Regards

[redacted]0-859-0367 [redacted]e@state.mnus

Privileged and/or confidential information may be contained in this message. If you are not the addressee indicated in thismessage (or are not responsible for delivery of this message to that person) , you may not copy or deliver this message toanyone. In such case, you should destroy this message and notify the sender by reply e-mail.

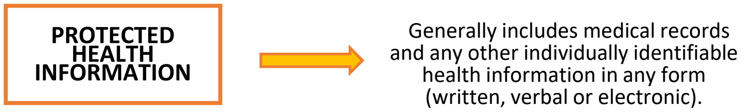
9



10

HIPAA, GENERALLY

- The **HIPAA Privacy Rule** regulations address:
  - Authorized uses and disclosures of protected health information (PHI); and
  - The rights of patients with regard to their PHI.
- The **HIPAA Security Rule** regulations address:
  - Administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI (ePHI).
- The **HIPAA Breach Notification Rule** regulations address:
  - Notification and reporting requirements following a breach of unsecured PHI.



PROTECTED HEALTH INFORMATION

Generally includes medical records and any other individually identifiable health information in any form (written, verbal or electronic).

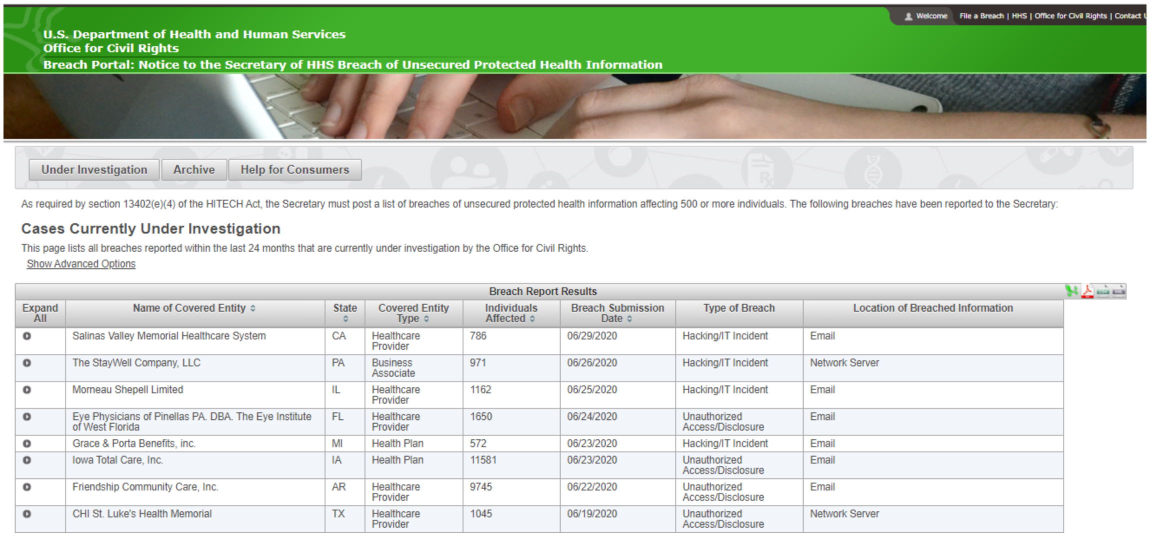
11

HIPAA and BREACH NOTIFICATION

- BREACH = An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI.
- An impermissible use or disclosure of unsecured PHI is *presumed* to be a breach unless the covered entity (or business associate) can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the protected health information or to whom the disclosure was made;
  - Whether the protected health information was actually acquired or viewed; and
  - The extent to which the risk to the protected health information has been mitigated.
- A covered entity must notify the impacted individual, HHS OCR and, possibly, the media where it discovers a breach of unsecured PHI.

12

OCR BREACH REPORT



U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

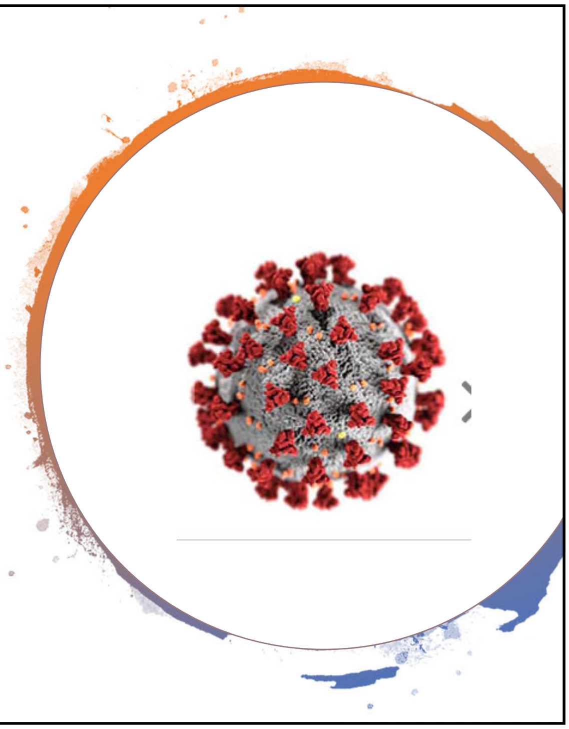
Breach Report Results

Expand All	Name of Covered Entity ⇕	State ⇕	Covered Entity Type ⇕	Individuals Affected ⇕	Breach Submission Date ⇕	Type of Breach	Location of Breached Information
●	Salinas Valley Memorial Healthcare System	CA	Healthcare Provider	786	06/29/2020	Hacking/IT Incident	Email
●	The StayWell Company, LLC	PA	Business Associate	971	06/26/2020	Hacking/IT Incident	Network Server
●	Morneau Shepell Limited	IL	Healthcare Provider	1162	06/25/2020	Hacking/IT Incident	Email
●	Eye Physicians of Pinellas PA. DBA. The Eye Institute of West Florida	FL	Healthcare Provider	1650	06/24/2020	Unauthorized Access/Disclosure	Email
●	Grace & Porta Benefits, inc.	MI	Health Plan	572	06/23/2020	Hacking/IT Incident	Email
●	Iowa Total Care, Inc.	IA	Health Plan	11581	06/23/2020	Unauthorized Access/Disclosure	Email
●	Friendship Community Care, Inc.	AR	Healthcare Provider	9745	06/22/2020	Unauthorized Access/Disclosure	Email
●	CHI St. Luke's Health Memorial	TX	Healthcare Provider	1045	06/19/2020	Unauthorized Access/Disclosure	Network Server

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HIPAA and COVID-19

- OCR Notification of Enforcement Discretion
  - Telehealth
  - Business Associates
  - Community Based Testing Sites
- OCR Guidance
  - FAQs on HIPAA and Telehealth
  - Disclosures of PHI to Law Enforcement, Paramedics, Other First Responders and Public Health Authorities
  - Restrictions on Media Access to PHI about Individuals in Health Care Facilities
  - Contacting Former COVID-19 Patients about Blood and Plasma Donation
- OCR Bulletins
  - February 2020 – HIPAA and Novel Coronavirus
  - March 2020 – HIPAA and COVID-19
  - March 2020 -Civil Rights, HIPAA and COVID-19



HIPAA Security Rule Standards

Administrative Safeguards

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation

Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Technical Safeguards

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Policies and Procedures

Business Associates/ Subcontractors

OCR - REMOTE USE

- OCR Guidance on Remote Use - Discusses various risks related to remote workforce use and outlines strategies for risk management and mitigation.
- Covered entities must analyze the risks associated with accessing, storing and transmitting ePHI remotely and develop policies/procedures and training designed to protect sensitive information.
  - Data access policies should focus on ensuring that users only access data for which they are appropriately authorized. Remote access to ePHI should only be granted to authorized users based on their role within the organization and their need for access to ePHI.
  - Storage policies address the security requirements for media and devices which contain ePHI and are moved beyond the covered entity's physical control.
  - Transmission policies focus on ensuring the integrity and safety of ePHI sent over networks and include both the direct exchange of data (for example, in trading partner relationships) and the provisioning of remote access to applications hosted by the organization (such as a provider's home access to ePrescribing systems or "web mail" in organizations where ePHI might be included in internal communications).
- Workforce awareness and training should specifically address any vulnerabilities associated with remote access to ePHI and provide clear and concise instructions for accessing, storing and transmitting ePHI.

OCR - REMOTE USE

- Some examples of the risks related to remote use that are discussed for accessing, storing and transmission of PHI include:
  - ✓ Lost or stolen log-on/password information.
  - ✓ Access to ePHI by employees when not authorized to do so while working offsite.
  - ✓ Home or other offsite workstations left unattended.
  - ✓ Contamination of systems by a virus introduced from an infected external device.
  - ✓ Laptop or other portable device is lost or stolen.
  - ✓ Use of external device to access corporate data resulting in the loss of operationally critical ePHI on the remote device.
  - ✓ Data is left on an external device (accidentally or intentionally), such as in a library or hotel business center.
  - ✓ Loss or theft of ePHI left on devices after inappropriate disposal by the organization.
  - ✓ Data intercepted or modified during transmission.

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf?language=es

OTHER REMOTE WORKFORCE CONSIDERATIONS

- Only authorized users have access rights to work remotely & onboarding process for new employees who are remote

  ACTION ITEM: Have standardized procedures in place for requesting, reviewing and approving remote access requests. IT resources should be in place to ensure that these processes are followed.

- Ensure all wired/wireless connections are secure

  ACTION ITEM: Have standard criteria for use of internet in homes and/or public places and set up secure connections for email.

- Set up and require VPN use for access to PHI

  ACTION ITEM: Remote workforce should only be able to access organization systems through VPN. Grant VPN access when processing remote access requests.

- Require encryption for PHI in transmission and at rest

  ACTION ITEM: Set up strong encryption solutions for laptops/mobile devices, as well as transmission of PHI (SSL, HTTPS) and educate workforce.

- Ensure IT processes for inventorying/tracking which equipment is being used/where it is and how equipment will be collected/inventoried upon end of remote locations

  ACTION ITEM: Where possible, have employees sign an agreement prior to giving out equipment. Include where device will be kept, time period for remote access, etc.

OTHER REMOTE WORKFORCE CONSIDERATIONS

- Configure all devices that will be accessing your network (either on site or remotely)

  ACTION ITEM: Have clear BYOD policy and accompanying agreement. Employees should be required to have IT configure any personal devices prior to allowing access to the network. Organization devices should be configured before giving them to employees.

- Providing proper education regarding how to safely secure technology and PHI at home (Security Awareness and Training standard)

  ACTION ITEM: Written guidance on any new policies and procedures that are adopted in response to telework. Reminders on existing policies and procedures for safeguarding PHI – some things apply regardless of being at a physical workplace or at home.

- Plan to review remote access and activity logs

  ACTION ITEM: Have a plan to audit remote access and activity logs. Reevaluate access, change permissions, and enforce organization Sanction Policy where appropriate.

19

OCR - TELEHEALTH

- Telehealth = the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration (HRSA).
- Telehealth services provided via various technologies: Audio, text messaging, or video communication technology, including videoconferencing.

OCR Enforcement Discretion: Covered health care providers will **NOT** be subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules that occur **in the good faith provision** of telehealth during the COVID-19 nationwide public health emergency.

OCR FAQs: https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

20

“BAD FAITH” PROVISION OF TELEHEALTH

- What is considered “bad faith provision” of telehealth?
  - Conduct or furtherance of a criminal act, such as fraud, identity theft, and intentional invasion of privacy;
  - Further uses or disclosures of patient data transmitted during a telehealth communication that are prohibited by the HIPAA Privacy Rule (e.g., sale of the data, or use of the data for marketing without authorization);
  - Violations of state licensing laws or professional ethical standards that result in disciplinary actions related to the treatment offered or provided via telehealth (i.e., based on documented findings of a health care licensing or professional ethics board); or
  - Use of public-facing remote communication products which OCR has identified as unacceptable forms of remote communication for telehealth because they are designed to be open to the public or allow wide or indiscriminate access to the communication.

OCR FAQs: https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

21

TELEHEALTH RELATED CONSIDERATIONS

- Use of HIPAA compliant options for telehealth operations
  - Use non-public facing remote communication products with end-to-end encryption. Examples include: Apple FaceTime, Facebook Messenger video or chat, Google Hangouts video or chat, Whatsapp video or chat, Zoom, or Skype.
    - What not to use: TikTok, Facebook Live, Twitch, or a public chat room
- Providers are encouraged to notify patients that third-party applications may introduce privacy risks
  - Providers should enable all available encryption and privacy modes when using these applications.
- Use of compliant telehealth setting
  - Provide telehealth operations using private locations. Patients should not receive telehealth services in public or semi-public settings, absent patient consent or exigent circumstances.
    - If telehealth cannot be provided in a private setting, reasonable precautions to take could include using lowered voices, not using speakerphone, or recommending that the patient move to a reasonable distance from others when discussing PHI.

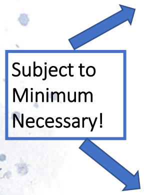
22

OTHER COVID-19 RELATED CONSIDERATIONS

- Adequate processes for rolling out IT updates and IT troubleshooting for remote users
  ACTION ITEM: Use of software to be able to access remote workforce devices/computers and install patches/updates
- Adequate policies, procedures and guidance for workforce related to COVID-19 operational changes
  ACTION ITEM: Draft/update policies and procedures and provide training to workforce
- Adequate HIPAA related training and security reminders for workforce
  ACTION ITEM: Circulate security reminders or training to workforce of relevant operational expectations as related to COVID-19 changes
- Adequate identification, tracking and remediation of COVID-19 related risk
  ACTION ITEM: Update your organization's Risk Analysis and Risk Management Plan

USING & SHARING PHI DURING THE PHE

- Patient or health plan member written authorization is **NOT** required for:
  - Disclosures for treatment, payment or healthcare operations
  - Disclosures to public health authorities (limited)
  - Disclosures to law enforcement / first responders (limited)
  - Disclosures for health oversight activities (limited)
  - Uses or disclosures of de-identified information
- Patient or health plan member written authorization is required:
  - Disclosures to the media
  - Any other types of disclosures


Subject to Minimum Necessary!

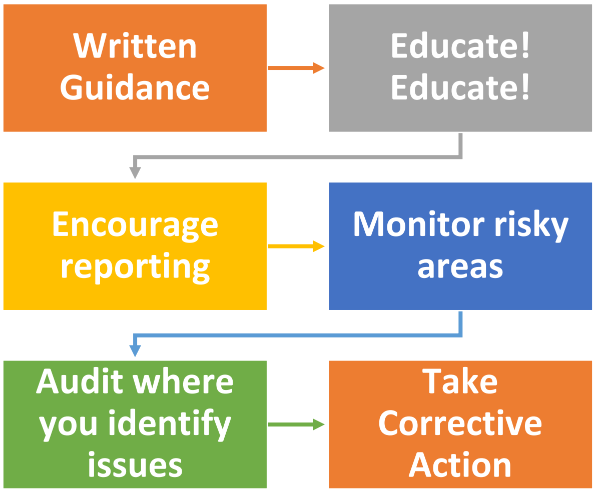
HIPAA Privacy Rule & COVID-19 Implications

- Providing Individual Rights to PHI
  - Access Requests
  - Restriction Requests
- Provision of Notice of Privacy Practices
- Disclosures of PHI per Written Authorization
- Reporting COVID-19 Related PHI to Third Parties
- Research Involving COVID-19 Patients or COVID-19 Drug Trials

25

BREACH DEFENSE STRATEGIES

PUT A FRAMEWORK IN PLACE


Written Guidance → Educate! Educate!

Encourage reporting → Monitor risky areas

Audit where you identify issues → Take Corrective Action

26

AS A STARTING POINT…

- **Policies and Procedures**
  - Remote Workforce/Access to PHI
  - Use of Telehealth Technology
- **Training & Educational Reminders**
  - Remote Workforce Training – Dos and Don'ts
  - Guidance on Permissible Use of Telehealth Technology
  - Permissible Use and Disclosure of PHI – COVID-19 Specific
  - Mock phishing exercises
  - HIPAA Reporting Reminder – How and When to Report
- **Monitoring**
  - Virus Protection
  - Data Loss Prevention
  - Security Information Event Management
- **Auditing**
  - Remote Access Requests
  - VIP/COVID Patient Record Access
  - Disclosure of PHI for Public Health Purposes

Contact us with questions:

Ashley Huntington, JD, CHC
Privacy Officer
Cook County Health
ashley.huntington@cookcountyhhs.org

COOK COUNTY HEALTH

Catie Heindel, JD, CHC, CHPC, CHPS
Managing Senior Consultant
Strategic Management, LLC
cheindel@strategicm.com

StrategicManagement
STRATEGIC MANAGEMENT SERVICES, LLC

Mark Lanterman
Chief Technology Officer
ComputerForensic Services
mlanterman@compforensics.com

ComputerForensic Services