NAVIGATING HIPAA AND TELEMEDICINE DURING COVID19

Lee Hamil Little , JD
Brian Tuttle, CPHIT, CPA, CHA, CBRA, CISSP

AMERICAN OSTEOPATHIC ASSOCIATION

AOIA
AMERICAN OSTEOPATHIC INFORMATION ASSOCIATION


CORONAVIRUS
OUTBREAK

Centers for Disease Control
Atlanta, Georgia

Centers for Disease Control Declares Public Health Emergency

Background

- The 2019–20 coronavirus pandemic is a pandemic of coronavirus disease 2019 (COVID-19) caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2).
- The disease was first identified in Wuhan, Hubei, China in December 2019

Centers for Disease Control Declares Public Health Emergency

Symptoms

- Flu-like
- Fever
- Cough
- Respiration difficulties
- Fatigue
- Myalgia

Centers for Disease Control Declares Public Health Emergency

Incubation Period

Estimated to be anywhere between 1 and 14 days

Mode of Transmission

Human-to-human transmission via respiratory droplets

Centers for Disease Control Declares Public Health Emergency

Prevention Tips

- Avoiding close contact with sick individuals;
- frequently washing hands with soap and water;
- not touching the eyes, nose, or mouth with unwashed hands;
- and practicing good respiratory hygiene

Health and Human Services
Washington, DC

Health and Human Services (HHS) Washington, DC

- Governing body of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- HIPAA is enforced be the Office for Civil Rights division of HHS
- Privacy and accessibility of ones health record is a civil right all Americans enjoy

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules contain privacy, security, and breach notification requirements that apply to individually identifiable health information created, received, maintained, or transmitted by health care providers who engage in certain electronic transactions, health transactions, health plans, health care clearinghouses, and their business associates.

March 2020
HHS

COVID19 and HIPAA Bulletin
Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency

Web Link:

https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf

March 2020

- The Novel Coronavirus Disease (COVID-19) outbreak imposes additional challenges on health care providers.
- Often questions arise about the ability of entities covered by the HIPAA regulations to share information, including with friends and family, public health officials, and emergency personnel.
- HIPAA Privacy Rule allows patient information to be shared to assist in nationwide public health emergencies, and to assist patients in receiving the care they need.

March 2020

- While the HIPAA Privacy Rule is **NOT** suspended during a public health or other emergency, the Secretary of HHS may waive certain provisions of the Privacy Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.
- In response to President Trump's declaration of a nationwide emergency concerning COVID-19, and Secretary of the U.S. Department of Health and Human Services (HHS) Alex M. Azar's earlier declaration of a public health emergency on January 31, 2020, Secretary Azar has exercised the authority to waive sanctions and penalties against a **covered hospital** that does not comply with certain provisions of the HIPAA Privacy Rule

Effective March 15, 2020
Provisions Temporarily Waived for Hospitals

- Requirement to obtain a patient's agreement to speak with family members or friends involved in the patient's care
- Requirement to honor a request to opt out of the facility directory
- Requirement to distribute a notice of privacy practices (NOPP)
- Patient's right to request privacy restrictions
- Patient's right to request confidential communications

NOTE

When the Secretary issues such a waiver, it only applies:

(1) in the emergency area identified in the public health emergency declaration;

(2) to hospitals that have instituted a disaster protocol; and

(3) for up to 72 hours from the time the hospital implements its disaster protocol.

When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if 72 hours have not elapsed since implementation of its disaster protocol.

More on HIPAA Privacy and Disclosures in Emergency Situations

Even without a waiver, the HIPAA Privacy Rule always allows patient information to be shared for the following purposes and under the following conditions.

Treatment: may disclose, without a patient's authorization in order to treat the patient or to treat a different patient. Includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment

More on HIPAA Privacy and Disclosures in Emergency Situations

Public Health Activities: recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to PHI that is necessary to carry out their public health mission.

- ***To a public health authority,*** such as the CDC or a state or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability
- ***At the direction of a public health authority***, to a foreign government agency that is acting in collaboration with the public health authority
- ***To persons at risk*** of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations

More on HIPAA Privacy and Disclosures in Emergency Situations

Disclosures to Family, Friends, and Others Involved in an Individual's Care and for Notification Family members, relatives, friends, or other persons identified by the patient as involved in the patient's care. May share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient's care, of the patient's location, general condition, or death.

- Should get verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object, when possible; if the individual is incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest
- May share protected health information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts

More on HIPAA Privacy and Disclosures in Emergency Situations

Disclosures to Prevent or Lessen a Serious and Imminent Threat may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider's standards of ethical conduct. Thus, providers may disclose a patient's health information to anyone who is in a position to prevent or lesson the serious and imminent threat, including family, friends, caregivers, and law enforcement without a patient's permission. HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health and safety

More on HIPAA Privacy and Disclosures in Emergency Situations

Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification Affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about treatment of an identifiable patient, such as specific tests, test results or details of a patient's illness, **may not** be done without patient authorization. Where a patient has not objected to or restricted the release of protected health information, a covered hospital or other health care facility may, upon a request to disclose information about a particular patient asked for by name, release limited facility directory information to acknowledge an individual is a patient at the facility, and may provide basic information about the patient's condition in general terms.

May also disclose information when the patient is incapacitated, if the disclosure is believed to be in the best interest of the patient.

More on HIPAA Privacy and Disclosures in Emergency Situations

Minimum Necessary Must make reasonable efforts to limit the information disclosed to that which is the "minimum necessary" to accomplish the purpose. (Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.)

Covered entities may rely on representations from a public health authority or other public official that the requested information is the minimum necessary for the purpose, when that reliance is reasonable under the circumstances. Example: a covered entity may rely on representations from the CDC that the protected health information requested by the CDC about all patients exposed to or suspected or confirmed to have COVID-19 is the minimum necessary for the public health purpose.

More on HIPAA Privacy and Disclosures in Emergency Situations

Safeguarding Patient Information

In an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures.

Further, covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information. (i.e. ensure a HIPAA Security Risk Assessment has been completed)


FREQUENTLY
ASKED
QUESTIONS

What disclosures are we permitted to make to “Public Authorities” relating to COVID19 cases?

May disclose PHI about individuals who are suspected of having contracted COVID-19 to public health authorities that are authorized by law to receive. This includes agencies or authorities of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency.

NOTE: some states have *mandatory* legal requirements to report infectious disease cases, such as COVID-19, to state or local public health authorities.

All disclosures should be based on the “minimum necessary” standard

What about responding to the media?

Disclosures to the media **ARE NOT** permitted unless authorization is provided by the patient! However, if the information is deidentified the disclosure may occur.

For Example: aggregate information like the total number of patients being treated may be disclosed

What about risks relating to internal staff access?

Under the HIPAA Security Rule – if a staff member accesses a patient record without need to access or necessity to perform job function, the staff member has broken the law. This is a direct violation of a patients Federal Civil Right of Privacy.

Staff should always be made aware that everything done electronically within an EHR system is tracked.

Audit logs must be reviewed periodically by the appointed HIPAA Security Officer or other designee

Can YOU and ME be arrested for wrongful disclosure of protected health information?

YES!!

CONSTANTLY REINFORCE THIS TO STAFF

Director
Office For Civil Rights
Roger Severino

TELEMEDICINE

Quote from Roger Severino

“We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities.” – Roger Severino, OCR Director.

TELEMEDICINE

TELEMEDICINE

March 17th, 2020 – the Office for Civil Rights (OCR) suspended enforcement of penalties relating to telemedicine

From OCR:

"During the COVID-19 national emergency, which also constitutes a nationwide public health emergency, covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules"

TELEMEDICINE

From OCR:

*"OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the **good faith** provision of telehealth during the COVID-19 nationwide public health emergency. This notification is effective immediately."*

TELEMEDICINE

What does **"good faith"** mean exactly?

From OCR:

*"A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any **non-public** facing remote communication product that is available to communicate with patients. …This exercise of discretion applies to telehealth provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19."*

TELEMEDICINE

What does **"good faith"** mean exactly?

From OCR:

"For example, a covered health care provider in the exercise of their professional judgement may request to examine a patient exhibiting COVID- 19 symptoms, using a video chat application connecting the provider's or patient's phone or desktop computer in order to assess a greater number of patients while limiting the risk of infection of other persons who would be exposed from an in-person consultation. Likewise, a covered health care provider may provide similar telehealth services in the exercise of their professional judgment to assess or treat any other medical condition, even if not related to COVID-19, such as a sprained ankle, dental consultation or psychological evaluation, or other conditions."

TELEMEDICINE

What does a **"non-public"** facing technology mean?

From OCR (continued):

*"Under this Notice, covered health care providers may use popular applications that allow for video chats, including **Apple FaceTime**, **Facebook Messenger** video chat, **Google Hangouts** video, or **Skype,** to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 nationwide public health emergency. Providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications."*

TELEMEDICINE

What is considered “non-public”? What can’t we use?

From OCR (continued):

*“Under this Notice, however, **Facebook Live**, **Twitch, TikTok**, and similar video communication applications are public facing, and **should not*** be *used in the provision of telehealth by covered health care providers.”*

TELEMEDICINE

From OCR (continued):

"Covered health care providers that seek additional privacy protections for telehealth while using video communication products should provide such services through technology vendors that are HIPAA compliant and will enter into HIPAA business associate agreements (BAAs) in connection with the provision of their video communication products"

TELEMEDICINE

From OCR (continued):

"…vendors that represent that they provide HIPAA-compliant video communication products and that they will enter into a HIPAA BAA."

- ***Skype for Business / Microsoft Teams***
- ***Updox***
- ***VSee***
- ***Zoom for Healthcare***
- ***Doxy.me***
- ***Google G Suite Hangouts Meet***
- ***Cisco Webex Meetings / Webex Teams***
- ***Amazon Chime***
- ***GoToMeeting***

TELEMEDICINE

From OCR (continued):

"Note: OCR has not reviewed the BAAs offered by these vendors, and this list does not constitute an endorsement, certification, or recommendation of specific technology, software, applications, or products. There may be other technology vendors that offer HIPAA-compliant video communication products that will enter into a HIPAA BAA with a covered entity."

"OCR will not impose penalties against covered health care providers for the lack of a BAA with video communication vendors or any other noncompliance with the HIPAA Rules that relates to the good faith provision of telehealth services during the COVID-19 nationwide public health emergency. "

It's always a good idea for patient's to acknowledge when a non-compliant solution is used:

I authorize that the following communications from the practice be delivered to me by the provided electronic means. I understand that some forms of electronic communications may not be secure, creating a risk of improper disclosure to unauthorized individuals.

I am willing to accept that risk, and will not hold the practice responsible should such incident occur.

Communications (check all that apply): Email, SMS Text Messaging, Video communications (i.e. Skype), Other (list specifically):

Acknowledgement and Agreements: I understand and agree that the requested communication method is not secure, making my PHI at risk for receipt by unauthorized individuals. I accept the risk and will not retaliate against the practice in any way should this occur.

Risks of Telemedicine (Telecommuting)

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

- HIPAA is the most critical aspect to ensure compliance as it relates to the practice's ability to achieve the goal of telecommuting.

- Protecting protected health information (PHI), electronic protected health information (EPHI) and the other confidential information is every employee's responsibility

- Just because there are some lax provision currently does not mean we can be careless (negligence still applies)

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

- Any practice or patient-related materials taken to the remote work area will be maintained in your designated remote work area and will not be made accessible to others, such as viewing your computer display.

- Everyone must agree that all confidential information, including PHI and EPHI, will only be accessed through and stored on within the practice's internal network or cloud-hosted electronic health records (EHR) system.

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

DO NOT COPY OR STORE PROTECTED HEALTH INFORMATION ON HOME COMPUTERS OR LAPTOPS

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

Loss of portable media with EPHI downloaded to the hard drive is the #2 way health records are breached in the USA

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

- Ensure any wireless used is encrypted – avoid public WiFi
- Where possible, any portable laptop which maintains PHI must be encrypted via “hardware encryption” also known as “whole disk encryption”
- If hardware encryption is not passible, file or folder level encryption should be used (i.e. encrypt one specific folder which hosts PHI or the specific file)

NOTE: if a device is lost or stolen and also encrypted – it is not a reportable breach under HIPAA

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

- The security of practice owned property in your home is as important as it is in the office (this also includes personal devices if used to access, transmit, or store EPHI).
- As such, the use of passwords and other practice policies are in effect.
- If you are not able to access a network drive or electronic health records (EHR) system (but have the need to save files locally to the computer), staff members must be trained notify the HIPAA Security Official or practice manager to discuss available options.

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

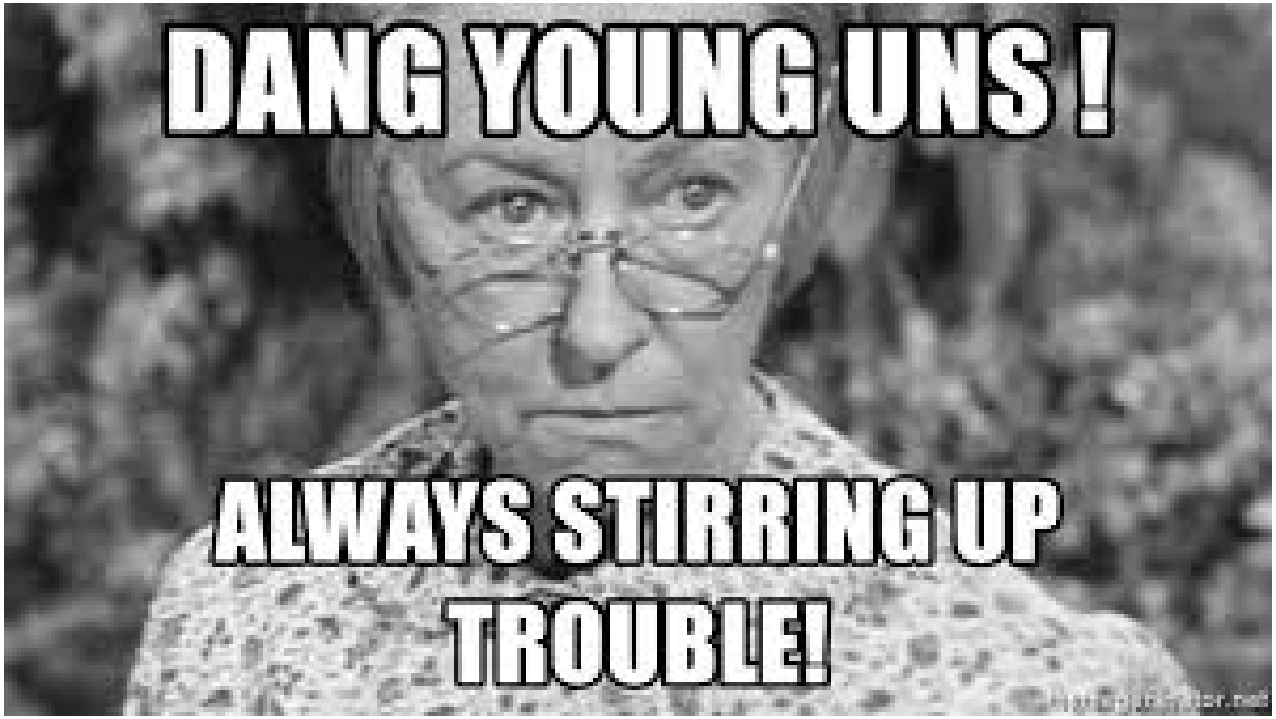
- All patient information and network connections must be secured when not in use. Staff must all be expected to take reasonable precautions to protect practice owned equipment from theft, damage, or misuse.
- Should any practice owned or personal equipment used while telecommuting be lost, stolen or destroyed, the staff members must be trained to notify the HIPAA Security Official or practice manager immediately

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

- Ideally a good telecommuting program includes working a paperless work environment (less risks)

- Under no circumstances should practice business information or participant information be disclosed in any way to individuals who are not privy to such information.


DANG YOUNG UNS !
ALWAYS STIRRING UP TROUBLE!

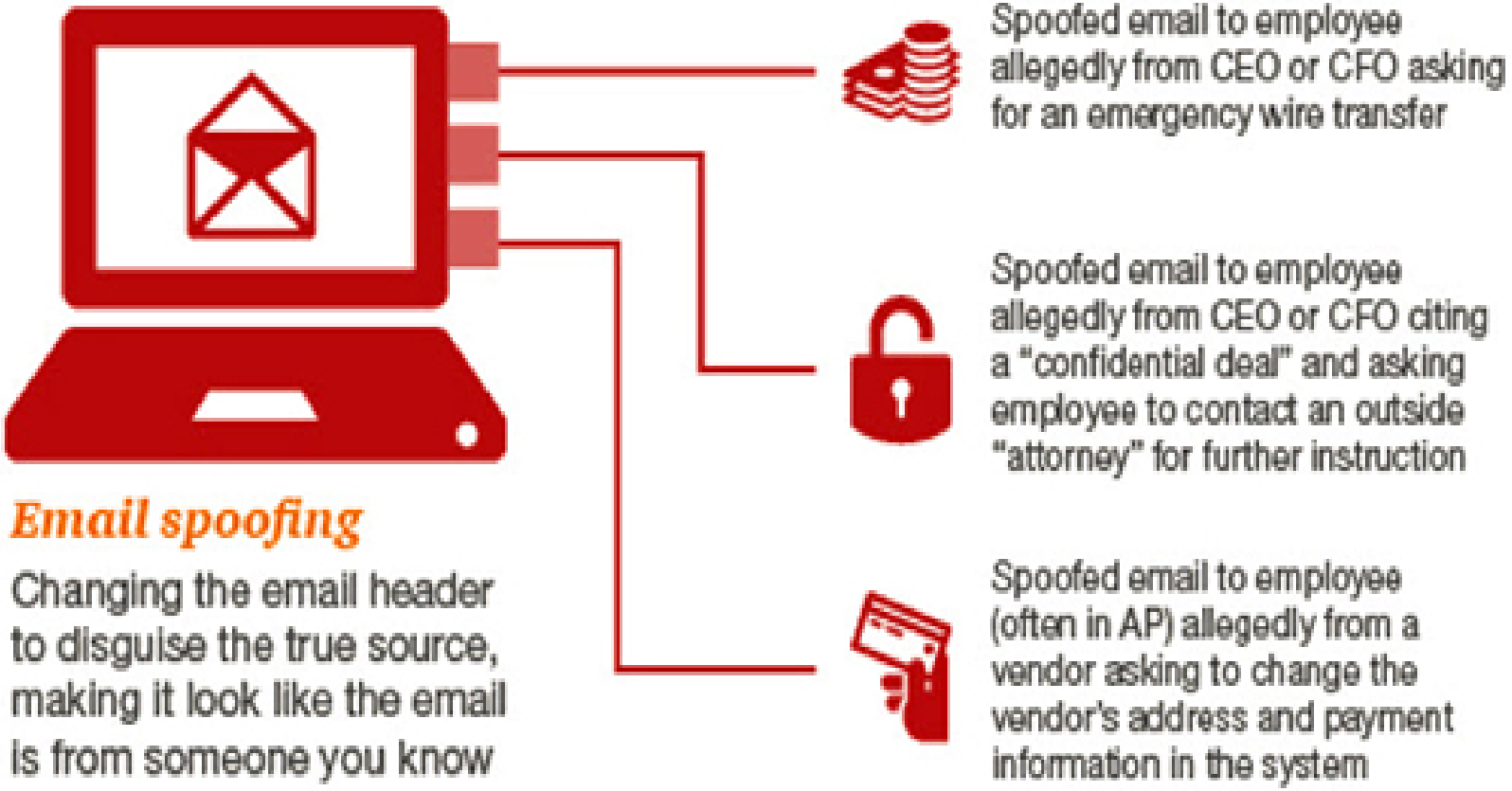
Risks of Telemedicine (Telecommuting)

- Telecommuting does not replace the need for child or dependent care.
- All staff members should be expected to make arrangements for children or dependents that require care to ensure that they do not interfere with your performance expectations and/or be privy to any confidential patient interactions.
- Acceptable arrangements include an off-site day care or another primary caregiver in your home.
- No one other than the employee should be allowed to use the practice owned computer or personally owned computers (if used to access, transmit, or store PHI)

Unscrupulous Hackers are Taking Advantage of this Pandemic

Email Spoofing Tricks

Train Staff on Email Hacking Tricks



Ransomware

What is Ransomware?

- Type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.
- More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key

What does OCR say?

What does OCR say?

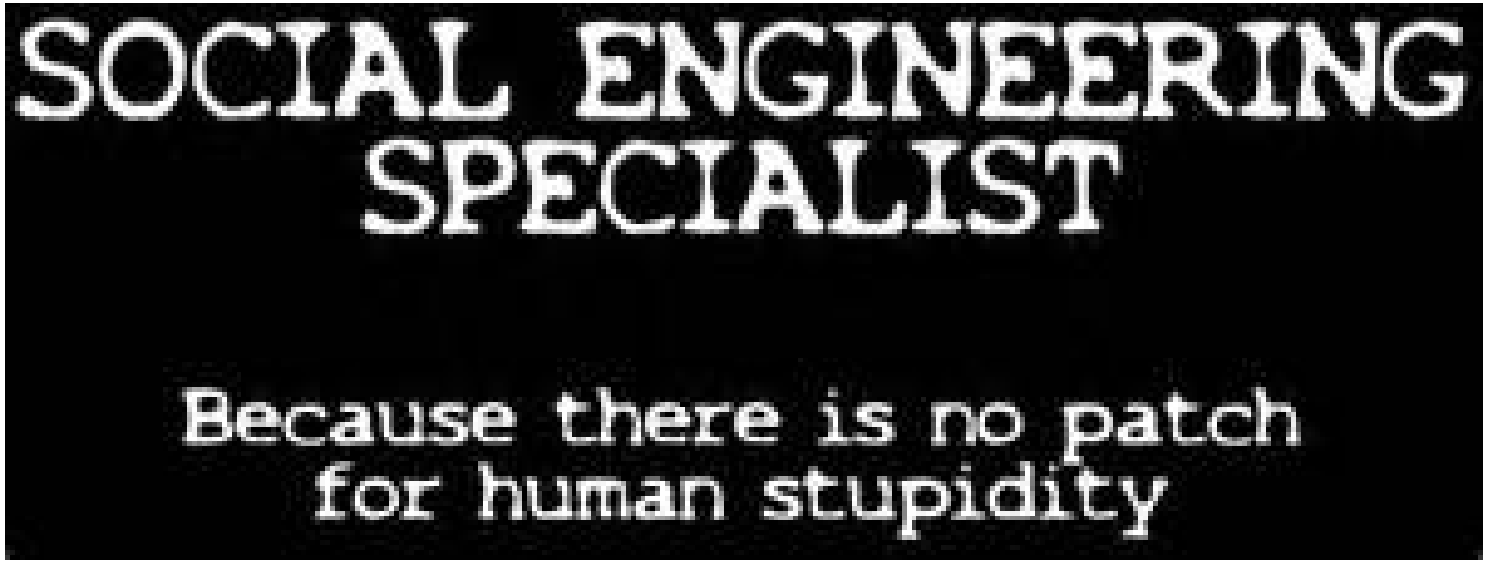
OCR Makes It Official:

Ransomware Attacks ARE HIPAA Breaches!!

What does OCR say?

- OCR confirms that ransomware attacks constitute a breach, because unauthorized individuals have taken possession or control of the ePHI, constituting an unauthorized disclosure.
- However, if the database, file share, folder, or file was encrypted prior to the attack it, Safe Harbor may apply

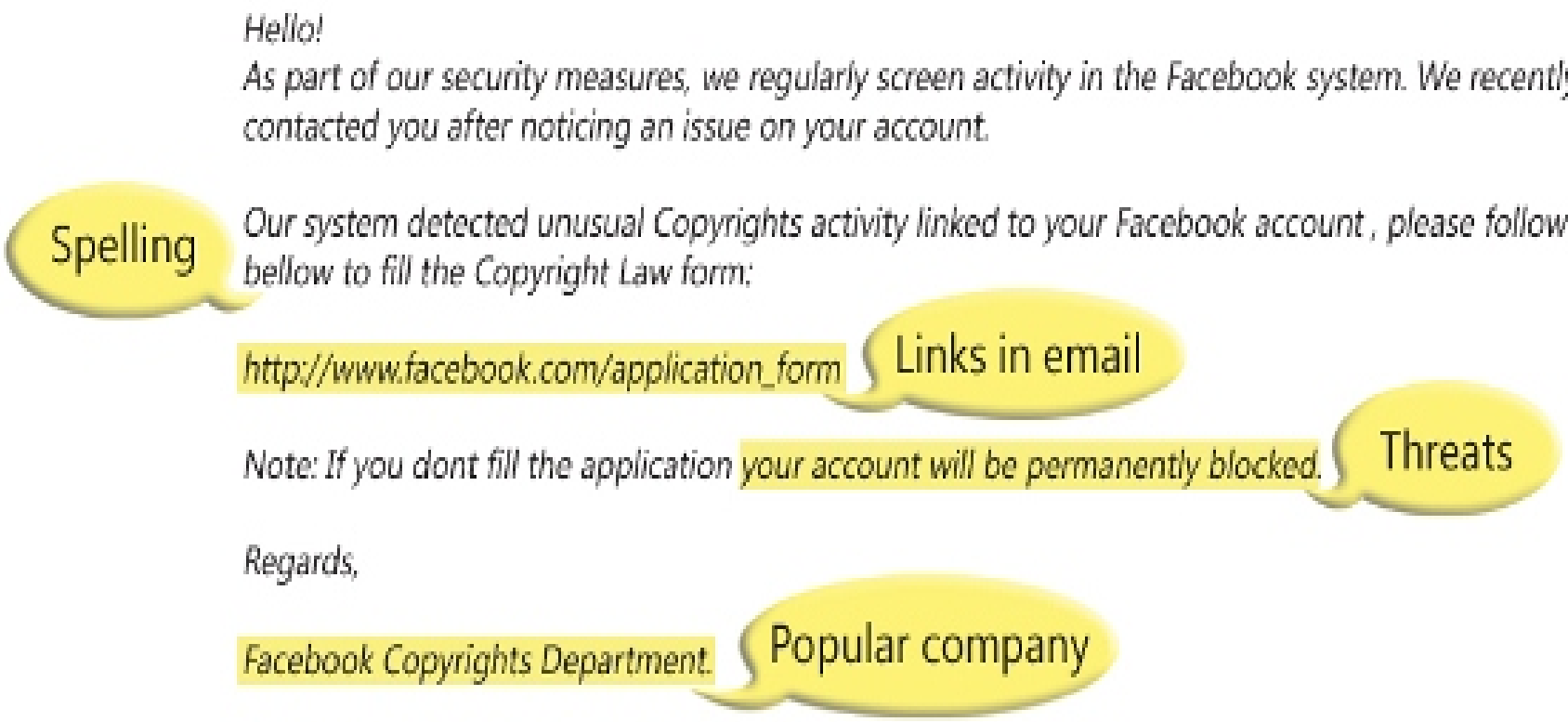
Social Engineering Hack



Social Engineering Hack

- **Phishing – most common**
  - Seek to obtain personal information, such as names, addresses and social security numbers.
  - Use link shorteners or embed links that redirect users to suspicious websites in URLs that appear legitimate.
  - Incorporates threats, fear and a sense of urgency in an attempt to manipulate the user into acting promptly.

What Does a Phishing E-mail Look Like?



I ♥ Texting

ENCRYPTION MUST BE USED WHEN TRANSMITTING PHI WHERE POSSIBLE

- When encryption is not possible or feasible always abide by the minimum necessary principle
- If a patient requests their information be sent via non-encrypted means they should acknowledge the risk of this type of transmission
- Texting with patients can be done if they opt in
- Texting among staff members of PHI should never be done without encryption

https://www.hhs.gov/hipaa/for-professionals/faq/2061/is-a-covered-entity-responsible-if-it-complies/index.html

Is a covered entity responsible if it complies with an individual's access request to receive PHI in an unsecure manner (e.g., unencrypted e-mail) and the information is intercepted while in transit?

NO

While covered entities are responsible for adopting reasonable safeguards in implementing the individual's request (e.g., correctly entering the e-mail address), covered entities are not responsible for a disclosure of PHI while in transmission to the individual based on the individual's access request to receive the PHI in an unsecure manner (assuming the individual was warned of and accepted the risks associated with the unsecure transmission). This includes breach notification obligations and liability for disclosures that occur in transit. Further, covered entities are not responsible for safeguarding the information once delivered to the individual. Covered entities are responsible for breach notification for unsecured transmissions and may be liable for impermissible disclosures of PHI that occur in all contexts **except when fulfilling an individual's right of access under 45 CFR 164.524 to receive his or her PHI or direct the PHI to a third party in an unsecure manner.**

NO SPEAKER PHONES WHEN COMMUNICATING WITH PATIENTS!

Quiet Voices

2020

Can YOU and ME be arrested for wrongful disclosure of protected health information?

YES!!

CONSTANTLY REINFORCE THIS TO STAFF

Trial Attorneys – the most dangerous aspect to HIPAA moving forward

CANNOT SUE UNDER HIPAA

There is no private cause of action allowed to an individual to sue for a violation of the federal HIPAA or any of its regulations. This means you do not have a right to sue based on a violation of HIPAA by itself. What most people don't get about HIPAA is that, as extensive as the statute is, and as serious as its potential penalties are, Congress, in its infinite wisdom, chose not to include a private right of action.

NEGLIGENCE IS NEGLIGENCE

- Although there are some loosened requirements during this dark time – we must always stay diligent with compliance under HIPAA
- If we are negligent and do not met “good faith” we can be held accountable in state laws of negligence

OMNIBUS and Suing

The Omnibus modifications to HIPAA made no impact on an individual's right of action. However, they do affect individuals in tangential ways.

Omnibus grants state attorneys general the ability to bring civil action and seek damages on behalf of their residents for HIPAA violations.

State Laws

States are falling like dominos

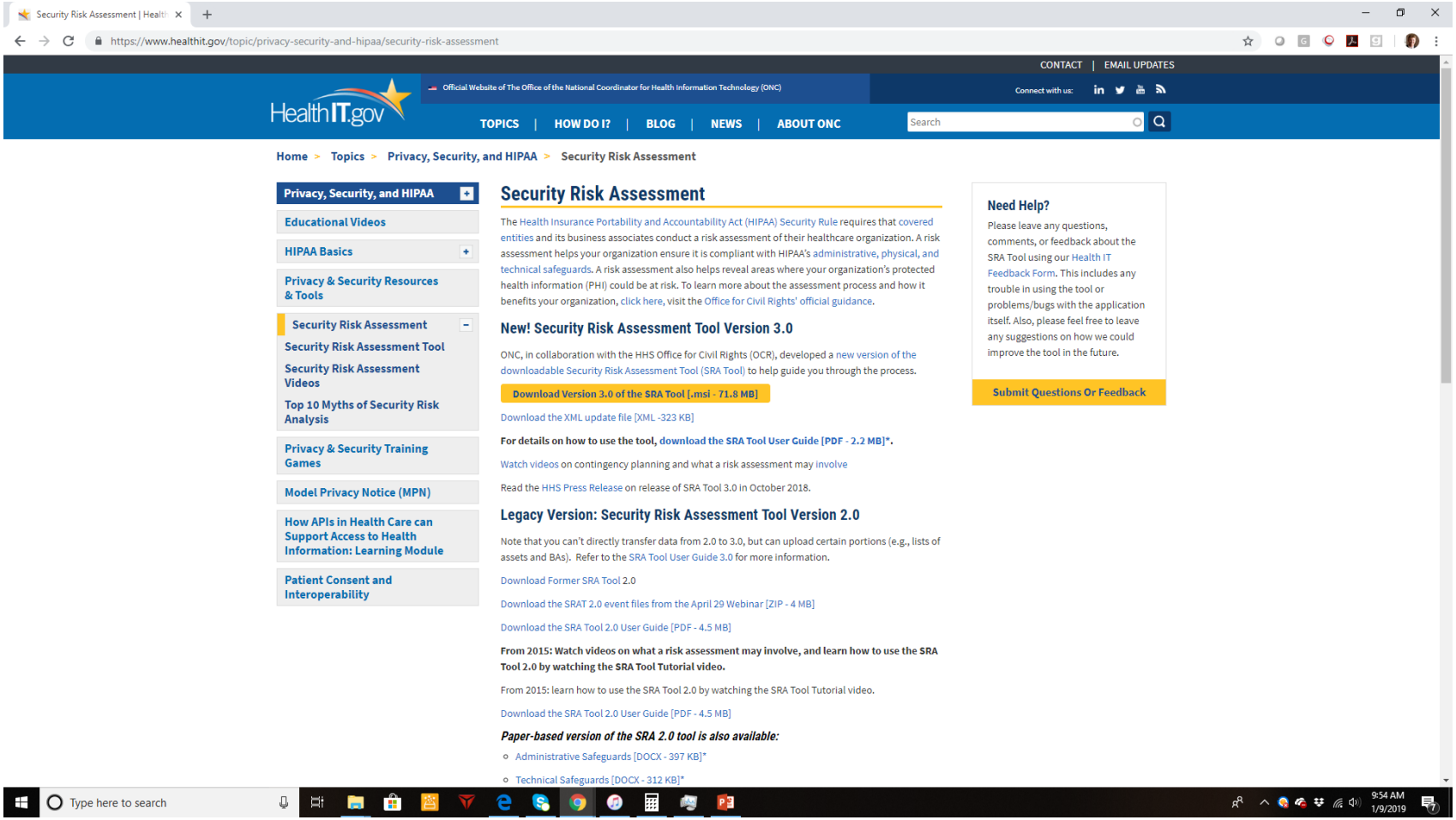
- Individual court cases filed citing HIPAA violations are creating precedence

Private Legal Remedies

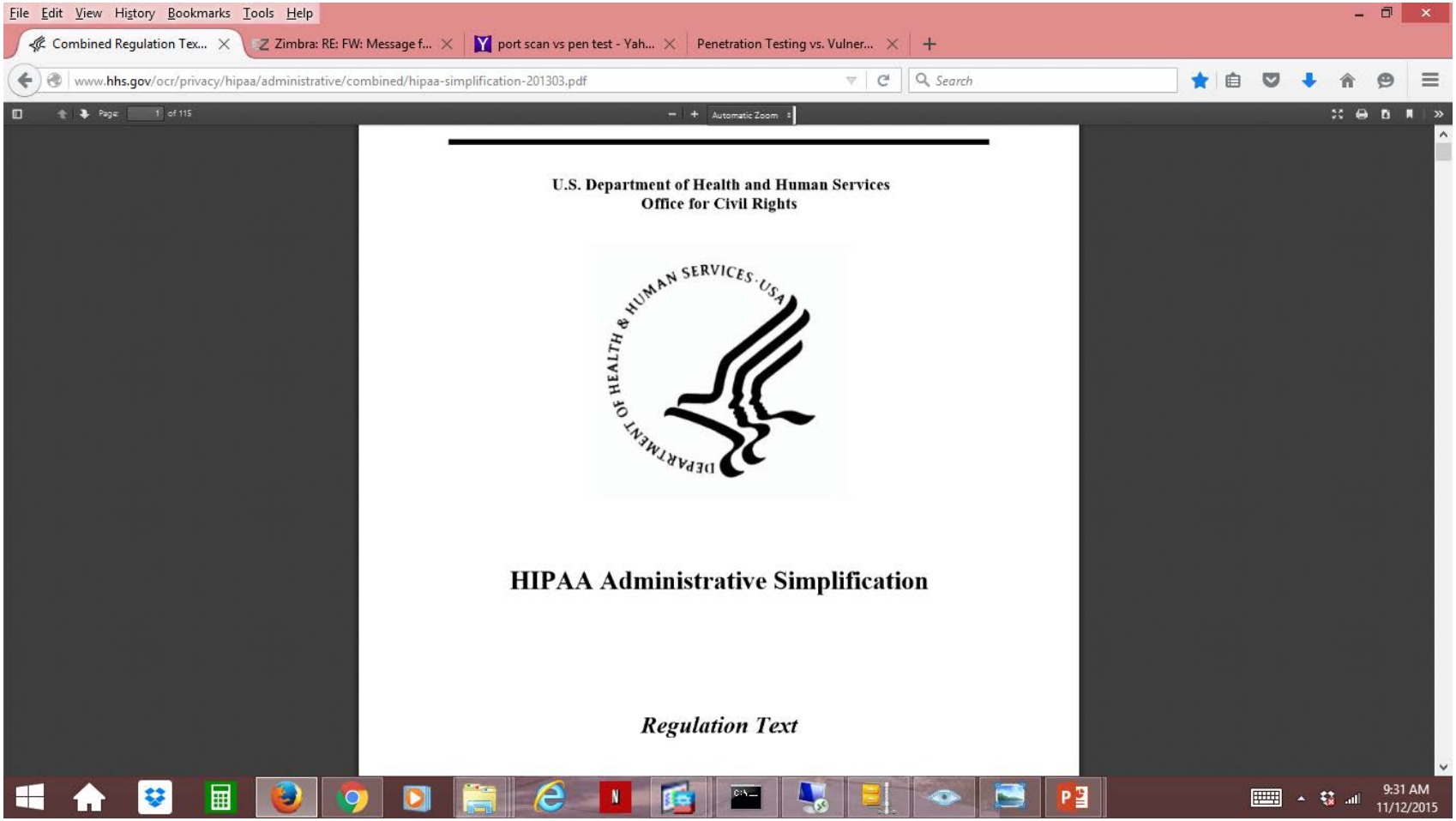
- If the violation resulted in damages, meaning you suffered some kind of verifiable financial loss, slander or defamation you may have a civil claim against the individual who violated your HIPAA rights.

http://www.healthit.gov/providers-professionals/security-risk-assessment-tool

UPDATED SRA TOOL Version 3.0

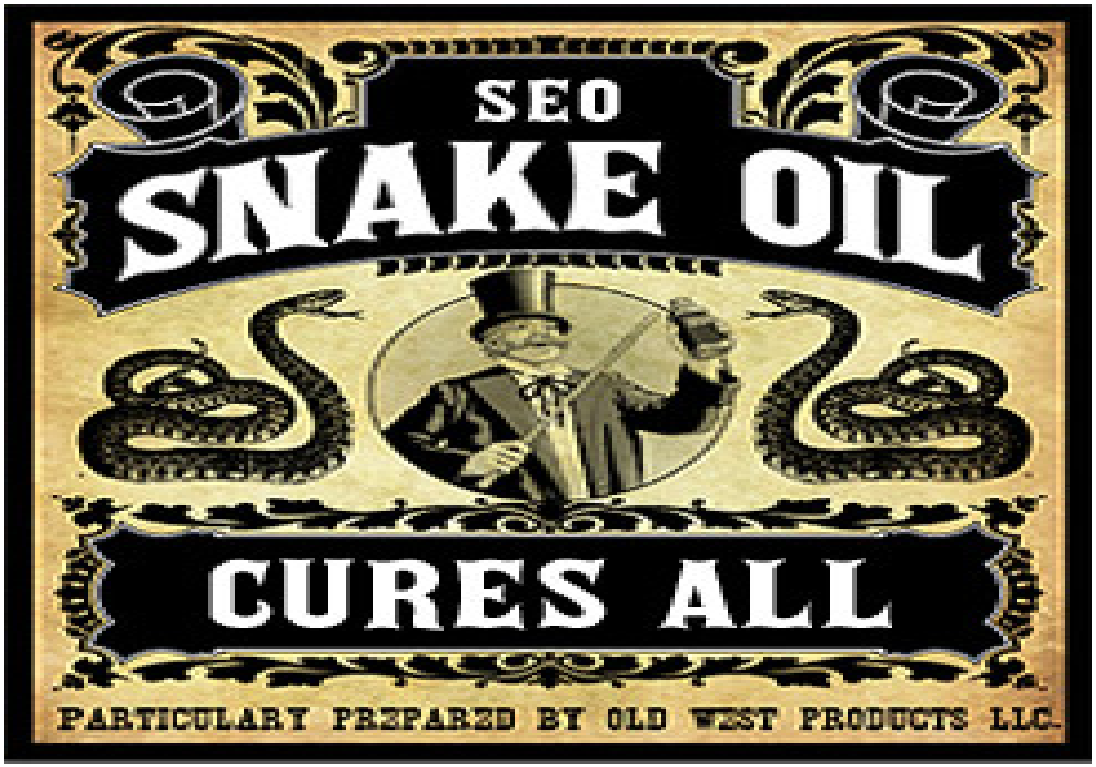


http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

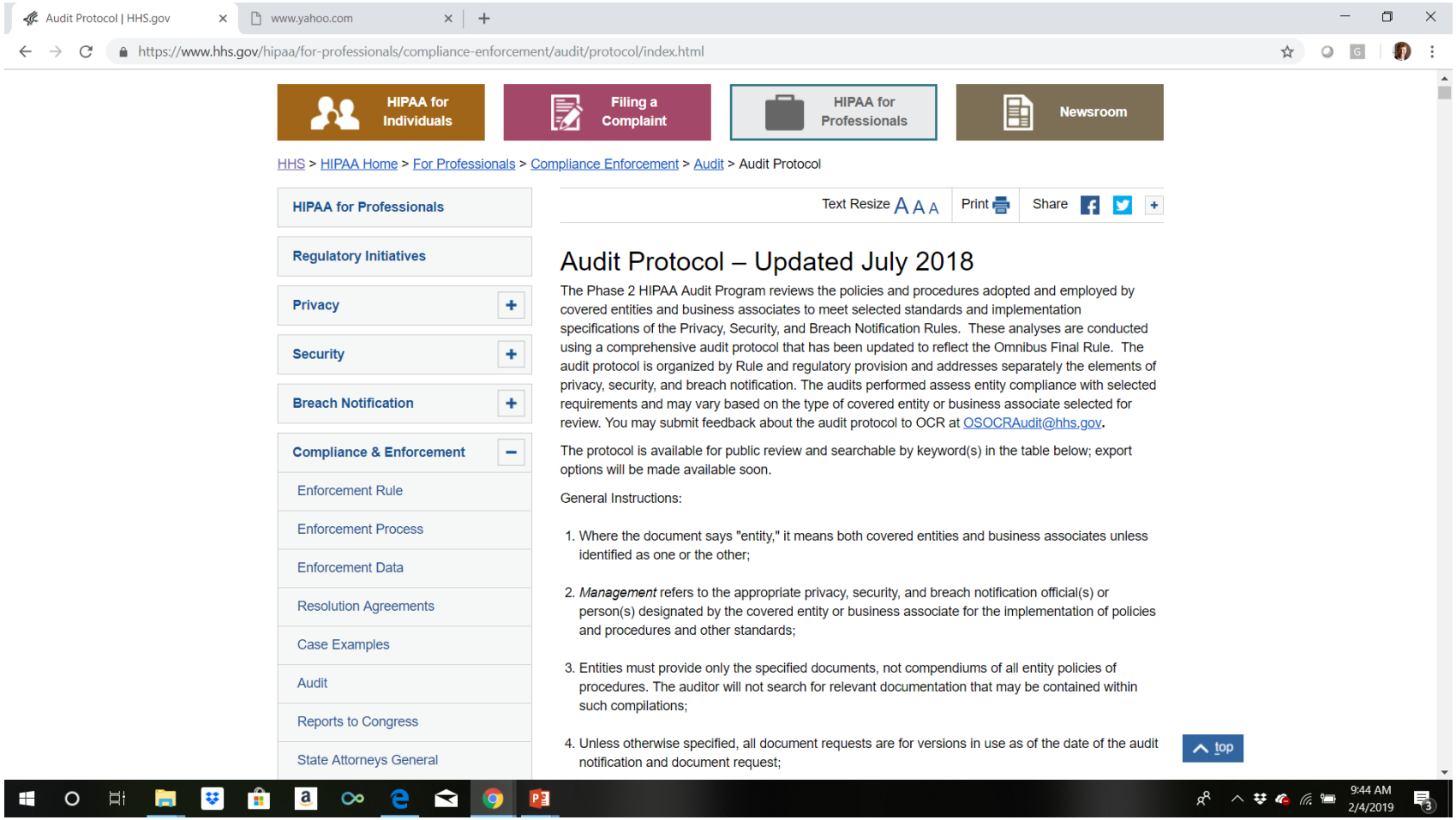


ALWAYS FACT CHECK WITH WWW.HHS.GOV

DON’T FALL FOR SNAKE OIL!!



https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html



No Such Thing as 100% Security

Covered Entities and business associates are just expected to follow the Security and Privacy Rule standards; implement the proper policies, procedures, and technologies; and **reasonably show the organization is making an effort to protect against common threats and vulnerabilities.**

Best Course of Action

BE PROACTIVE!!

RESOURCES

AMERICAN OSTEOPATHIC ASSOCIATION

AOiA
AMERICAN OSTEOPATHIC INFORMATION ASSOCIATION

AOA Resources

www.osteopathic.org/covid-19

AOIA Webinars

https://aoaonlinelearning.osteopathic.org/course/index.php?categoryid=40

Telemedicine Platforms

Remote Monitoring of COVID-19 Patients
Ceras Health – https://cerashealth.com/aoa.html - 877-723-7277

Patients download the Ceras app and enter vitals three times a day. Readings are monitored by a Ceras RN. If the readings raise an alert, Ceras will notify the patient and provider for follow up. Consult with Ceras on your state reimbursement. No implementation fee for AOA members

Free COVID video consultations
Bluestream Health is offering AOA members free access to HIPAA-compliant video sessions with patients during the COVID-19 crisis. Bluestream will create a platform for the provider to send a secure invite to your patient via text or email. The patient clicks on the link to begin a HIPAA-compliant video session with provider. Email membervalue@osteopathic.org to receive the link.

Find links at osteopathic.org/membervalue
Questions? membervalue@osteopathic.org

Questions & Answers

AOA
Physician Services Department
1-312-202-8194
physicianservices@osteopathic.org

Brian Tuttle
www.hipaa-consulting.com

Lee Hamil Little
www.ksllawfirm.com

THANK YOU

AMERICAN OSTEOPATHIC ASSOCIATION

AOiA
AMERICAN OSTEOPATHIC INFORMATION ASSOCIATION