CP State – The Arc NY
HIPAA/SAMHSA
2024

Brian L Tuttle, CPHIT, CHA, CHP, CBRA, CISSP, CCNA, Net +

www.hipaa-consulting.com

1

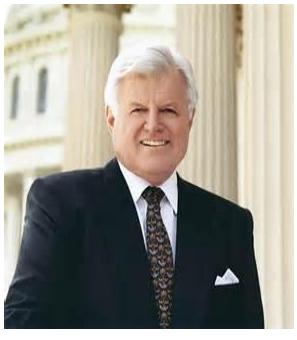
HIPAA

HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996

2

- The Health Insurance Portability Act of 1996 (HIPAA)
- Enacted by the United States Congress and signed by President Clinton in 1996.

3



Bi-partisan bill also known as the Kennedy-Kassebaum Act named after two of its major sponsors:

- Senator Ted Kennedy (D) Massachusetts
- Senator Nancy Kassebaum (R) Kansas

4

MASSIVE LAW WITH MANY TENTACLES

5

“Privacy” and “Security” are not even in the name “HIPAA” but they present our biggest challenge

6

2024

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

YES!!

7

2024

Can Practice/Business be fined for HIPAA violations even if a breach **doesn't** occur?

YES!!

8

TELEMEDICINE

9

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.

10

Telecommuting

11

Risks of Telemedicine (Telecommuting)

Telecommuting Policy Should be in Place

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

12

Telecommuting

Telecommuting Policy Should be in Place

13

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.

14

Telecommuting

Telecommuting Policy Should be in Place

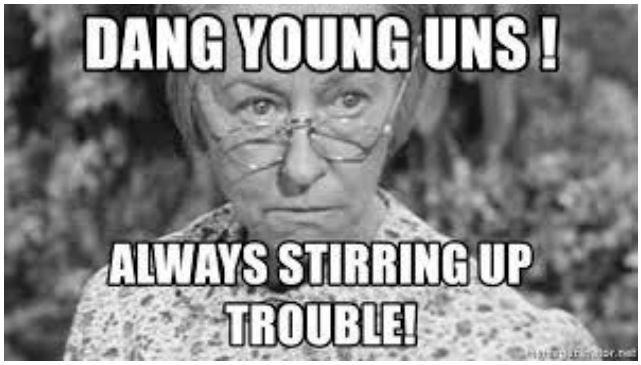
15

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.

16



17

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)

18

HIPAA SPECIFIC CHANGES

19

HIPAA PRIVACY RULE CHANGES FOR 2024

1. Changes to Right of Access
2. Changes relating to Care Coordination and Information Sharing
3. Necessity to update the Notice of Privacy Practices

Compliance Required by February 2026

20

Right of Access

- Allows patients right to take notes and use “personal resources” such as a smartphone to take pics of their PHI
- Changes in Response Time for Requests – timeframe for requests change from 30 days with optional 30 day extension to 15 days with an optional 15 day extension
- Rights to PHI in Form and Format Requested by Patient – “readily producible” copies of PHI (to include EPHI) must be provided through secure application program interfaces (API’s) via applications chosen by the individual
- Requirement to deliver copies of PHI in any form and format required by applicable state or other laws

21

Right of Access (cont)

- Eased Identity Verification – prohibits covered entities from imposing unreasonable verification measures such as notarized signatures or proof of identification in person (when other credible, more convenient methods are available)

22

Right of Access (cont)

- Changes to Fees for Obtaining PHI – must post fee schedules on website, offer estimates, and provide itemized bills (when requested)
- Specifies when PHI must be provided free of charge (e.g., during in-person viewing) and amends fees related to responding to requests to send PHI to third parties.

- Providers required to:
  - Post estimated fee schedules on their websites;
  - Offer individualized fee estimates; and
  - Provide itemized bills for completed requests.

23

Information Sharing and Care Coordination

For Individuals: Patients allowed to request that a provider or health plan submit an access request for PHI in an Electronic Health Record (EHR) to another healthcare provider, albeit with some provisions:

- Requests to send direct electronic copies of PHI to a third party are limited to only electronic copies of PHI in an EHR.
- Requests need to be "clear, conspicuous, and specific" and may be made orally, in writing, or via electronic means.

24

Information Sharing and Care Coordination (cont)

For Providers and Health Plans:

- Must create a requirement for these organizations to facilitate an individual's request for a copy of PHI in an EHR and receive the information on behalf of the individual.
- Must modify the rules related to "minimum necessary standard:"
- The Privacy Rule generally requires that covered entities use, disclose, or request only the minimum PHI necessary to accomplish the task at hand (outside of treatment purposes).
- Makes an exception to the minimum necessary standard for use by, disclosure to, or requests from a covered entity for care coordination and case management.

25

Information Sharing and Care Coordination (cont)

Third Parties: Permits covered entities to disclose PHI to third-party organizations that provide health-related services for individual-level care coordination and case management (for treatment or healthcare operations).

Covered entities expressly permitted to disclose PHI to:

- Social services agencies;
- Community-based organizations;
- Home and Community-Based Services providers and
- Other third parties that provide health-related services to specific individuals for individual-level care coordination and case management, either as a treatment activity of a covered healthcare provider or as a healthcare operations activity

26

Notice of Privacy Practices

Eliminates the requirement for direct healthcare providers to obtain — or to document their good faith efforts to obtain — patients' written acknowledgment of receipt of the provider's Notice of Privacy Practices (NPP).

Modifies the header of the NPP to specify that the notice provides individuals with information about:

- How to access their information,
- How to file a HIPAA complaint, and
- Their right to receive a copy of the notice.

(These new NPP headers also would need to include a phone number and email address for the designated contact person.)

27

Hot Topics
HIPAA and Email

28

http://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html

Directly from www.HHS.gov

Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?

29

YES

Directly from www.HHS.gov

The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so.

30

Continued

Directly from www.HHS.gov

While the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail.

31

I get this question often:

What if a patient initiates the conversation via email?

If this situation occurs, one can assume (unless the patient has explicitly stated otherwise) that e-mail/text communications are acceptable to the individual. If the CE or BA feels the patient may not be aware of the possible risks of using unencrypted e-mail/texting, or has concerns about potential liability, the CE or BA can alert the patient of those risks, and let the patient decide whether to continue e-mail communications. – recommended.

The above should also apply when communicating with other CE's or BA's

32

Let's review:

If you think the individual may not be aware of the possible risks of using unencrypted e-mail/texting, or has concerns about potential liability, you should ABSOLUTELY alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

Remember – risks are higher now that patients can sue

33

2024 PATEINT'S RIGHT TO NON-ENCRYPTED PHI

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?

34

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**.

35

https://www.hhs.gov/hipaa/for-professionals/faq/568/does-hipaa-permit-a-covered-health-care-to-email-information-with-another-provider/index.html

Does the HIPAA Privacy Rule permit a covered health care provider to e-mail or otherwise electronically exchange protected health information (PHI) with another provider for treatment purposes?

36

YES

Yes. The Privacy Rule allows covered health care providers to share PHI electronically (or in any other form) for treatment purposes, as long as they apply reasonable safeguards when doing so. Thus, for example, a physician may consult with another physician by e-mail about a patient's condition, or health care providers may electronically exchange PHI to and through a health information organization (HIO) for patient care.

37

Personal Device Use Increasing

38

DO NOT

- Allow PHI to be written to the mobile device
- Permit integration with insecure file sharing or hosting services
- Set it and forget it (always include BYOD in risk assessments)

39

DO

- Require business grade security suites
- Require business grade operating systems
- Require hardware encryption

40

TEXTING and HIPAA

41

TEXTING Positives in Healthcare

- Texting CAN provide great advantages in health care
  - Appointment Reminders (**2024 - MUST OPT IN FOR MENTAL HEALTH AND SUBSTANCE ABUSE**)
  - Fast
  - Easy
  - Loud background noise problems are mitigated
  - Bad signal issues mitigated
  - Device neutral

42

TEXTING Negatives in Healthcare

- Reside on device and not deleted
- Very easily accessed
- Not typically centrally monitored by IT
- Can be compromised in transmission relatively easy
- HIPAA Privacy Rule requires disclosure of PHI to patient (i.e. text message is used to make a judgement in patient care)
- **CANNOT TEXT PATIENT ORDERS UNLESS ENCRYPTED**

43

Include Texting in Policies

- Administrative policy on workforce training (i.e. minimum necessary)
- Appropriate use of texting
- Password protections and encryption
- Mobile device inventory
- Retention period (require immediate deletion of PHI texts)
- Use of secure texting applications

44

2024 Mobile Devices

45

2024 Mobile Devices

- HHS issued guidance addressing the extent to which PHI is protected on mobile devices. Although the HIPAA Privacy Rule and Security Rule (protecting PHI when maintained or transmitted electronically) provide protections for the use and disclosure of PHI held or maintained by covered entities and their business associates, they do not address PHI accessed through or stored on personal devices owned by individual patients.

- **Example:** although PHI maintained on electronic devices owned by a covered entity would be protected from disclosure by HIPAA, once a patient downloads that information to a personal device, HIPAA would no longer protect it.

46

2024 Mobile Devices

- **The guidance does provide tips to help individuals protect their own PHI, such as:**

- Avoiding downloads of unnecessary or random apps to personal devices; and
- Avoiding (or turning off) permissions for apps to access an individual's location data. (This reduces information about a person's activities that can be used by the app or sold to third parties, such as the name and address of health care providers a person visits.)
- LOCATIONS CAN BE AND ARE SOLD TO 3rd PARTIES

47

Substance Abuse and Mental Health Services Administration
SAMHSA

48

Patient Record Confidentiality (CFR Title 42: Part 2)

Federal regulations which specify restrictions concerning the disclosure and use of patient records pertaining to substance abuse treatment that federal programs maintain

Confidentiality of Alcohol and Drug Abuse Patient Records (CFR Title 42: Part 2)

49

DOES 42 CFR Part 2 APPLY TO MY PRACTICE?

50

DOES 42 CFR Part 2 APPLY TO MY PRACTICE?

MUST BE FEDERALLY ASSISTED AND PROVIDE SUD TREATMENT OR REFERRAL FOR TREATMENT

Part 2 Programs are prohibited from disclosing any information that would identify a person as having or having had a SUD unless that person provides written consent.

Part 2 specifies a set of requirements for consent forms, including but not limited to the name of the patient, the names of individuals/entities that are permitted to disclose or receive patient identifying information, the amount and kind of the information being disclosed, and the purpose of the disclosure.

51

FEDERAL ASSISTANCE CHECKLIST:

Is your Organization Currently: (**YES or NO**)

1. Authorized, certified, licensed, or registered by the Federal Government?
2. Receiving federal funds in any form, including funds that do not directly pay for SUD services? Granted tax-exempt status by the IRS?
3. Allowed tax deductions for contributions by the IRS?
4. Authorized to conduct business by the federal government, including programs?
5. Certified as a Medicare provider?
6. Authorized to conduct methadone maintenance treatment?
7. Registered with the DEA, and use such license to the extent of treating SUD
8. Conducting business directly with the federal government?

52

Substance Abuse and Mental Health Services Administration
SAMHSA

MEDICAL RECORDS ARE NOT CREATED EQUAL

53

Substance Abuse and Mental Health Services Administration
SAMHSA

SEPARATING SUD RECRODS FROM NORMAL MEDICAL RECORDS

- **Higher risks potential legal consequences for not properly securing SUD records**
- **In general, SUD records are only to be accessed by the provider of care (with limited exceptions as discussed later)**
- **Almost like attorney/client privilege**
- **If possible, within the EMR system, lock SUD portion of medical record to specific provider**
- **Ensure all EMR audit capabilities are enabled and audit trails are reviewed periodically**

54

Substance Abuse and Mental Health Services Administration SAMHSA

WHAT HAS CHANGED?

55

Substance Abuse and Mental Health Services Administration SAMHSA

WHAT HAS CHANGED?

Part 2 regulations serve to protect patient records created by federally assisted programs for the treatment of substance use disorders (SUD).

These revisions further facilitate better coordination of care in response to the opioid epidemic while maintaining confidentiality protections against unauthorized disclosure

Compliance date: Persons subject to this regulation must comply with the applicable requirements of this final rule by February 16, 2026

56

WHAT HAS CHANGED?

Applicability and Re-Disclosure

Treatment records created by non-Part 2 providers based on their own patient encounter(s) are explicitly not covered by Part 2, unless any SUD records previously received from a Part 2 program are incorporated.

Segmentation or holding a part of any Part 2 patient record previously received can be used to ensure that new records created by non-Part 2 providers will not become subject to Part 2.

57

WHAT HAS CHANGED?

Disposition of Records

When an SUD patient sends an incidental message to the personal device of an employee of a Part 2 program, the employee will be able to fulfill the Part 2 requirement for "sanitizing" the device by deleting that message

58

WHAT HAS CHANGED?

Consent Requirements

An SUD patient may consent to disclosure of the patient's Part 2 treatment records to an entity (e.g., the Social Security Administration), without naming a specific person as the recipient for the disclosure

59

WHAT HAS CHANGED?

Disclosures Permitted w/ Written Consent

Disclosures for the purpose of "payment and health care operations" are permitted with written consent, in connection with an illustrative list of 18 activities that constitute payment and health care operations now specified under the regulatory provision.

60

WHAT HAS CHANGED?

Disclosures to Central Registries and PDMPs

Non-OTP (opioid treatment program) and non-central registry treating providers are now eligible to query a central registry to determine whether their patients are already receiving opioid treatment through a member program.

OTPs are permitted to enroll in a state prescription drug monitoring program (PDMP), and permitted to report data into the PDMP when prescribing or dispensing medications on Schedules II to V, consistent with applicable state law.

61

WHAT HAS CHANGED?

Medical Emergencies

Declared emergencies resulting from natural disasters (e.g., hurricanes) that disrupt treatment facilities and services are considered a “bona fide medical emergency,” for the purpose of disclosing SUD records without patient consent under Part 2.

62

WHAT HAS CHANGED?

Audit and Evaluation

Clarifies specific situations that fall within the scope of permissible disclosures for audits and/or program evaluation purposes.

63

WHAT HAS CHANGED?

Undercover Agents and Informants

Court-ordered placement of an undercover agent or informant within a Part 2 program is extended to a period of 12 months, and courts are authorized to further extend the period of placement through a new court order.

64

Substance Abuse and Mental Health Services Administration
SAMHSA

Here are some of the other changes that <u>ARE</u> implemented:

- The ability to disclose Part 2 information to contractors, subcontractors and legal representatives ("contractors") for payment and health care operations activities without additional patient consent, if certain conditions are met; and
- The ability of lawful holders to disclose Part 2 information for Medicaid, Medicare or Children's Health Insurance Program ("CHIP") audit or evaluation activities if certain conditions are met.

65

New York Shield Act

66

New York Shield Act and HIPAA

On July 25, 2019 New York adopted the Stop Hacks and Improve Electronic Security Act, colloquially referred to as the "SHIELD Act."

The SHIELD Act and HIPAA work in concert to ensure that data breaches are reported, and that patient information is kept secure.

67

New York Shield Act and HIPAA

The SHIELD Act amends existing New York data breach notification and cybersecurity laws.

New York HIPAA-covered entities and business associates must now comply with the revised New York law as well as existing HIPAA law.

68

New York Shield Act and HIPAA

While HIPAA requires notification of a breach to HHS and to affected individuals, the breaching entity, under the SHIELD law, must also notify the New York State Attorney General of the breach – within 5 business days of notifying HHS. In other words, in this circumstance, the New York SHIELD Act AND HIPAA both require HHS be notified.

However, in this situation, the SHIELD law does not require that affected individuals be notified.

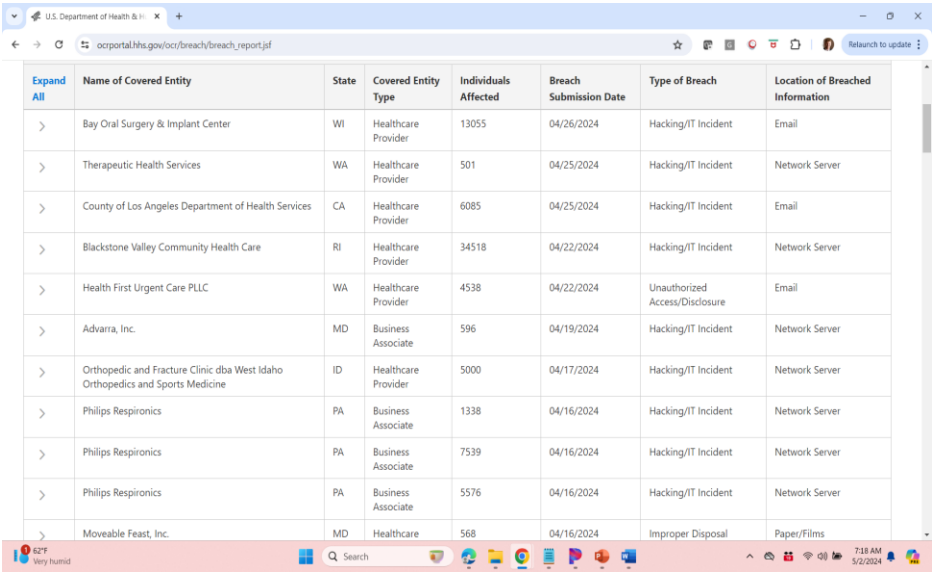
This is because HIPAA already imposes that requirement

69

ALL TIME HIGH

70

OCR Breach Portal



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

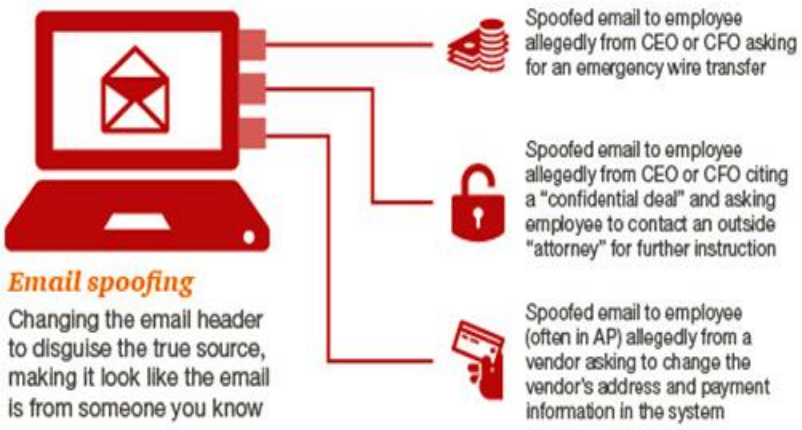
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
›	Bay Oral Surgery & Implant Center	WI	Healthcare Provider	13055	04/26/2024	Hacking/IT Incident	Email
›	Therapeutic Health Services	WA	Healthcare Provider	501	04/25/2024	Hacking/IT Incident	Network Server
›	County of Los Angeles Department of Health Services	CA	Healthcare Provider	6085	04/25/2024	Hacking/IT Incident	Email
›	Blackstone Valley Community Health Care	RI	Healthcare Provider	34518	04/22/2024	Hacking/IT Incident	Network Server
›	Health First Urgent Care PLLC	WA	Healthcare Provider	4538	04/22/2024	Unauthorized Access/Disclosure	Email
›	Advarra, Inc.	MD	Business Associate	596	04/19/2024	Hacking/IT Incident	Network Server
›	Orthopedic and Fracture Clinic dba West Idaho Orthopedics and Sports Medicine	ID	Healthcare Provider	5000	04/17/2024	Hacking/IT Incident	Network Server
›	Philips Respironics	PA	Business Associate	1338	04/16/2024	Hacking/IT Incident	Network Server
›	Philips Respironics	PA	Business Associate	7539	04/16/2024	Hacking/IT Incident	Network Server
›	Philips Respironics	PA	Business Associate	5576	04/16/2024	Hacking/IT Incident	Network Server
›	Moveable Feast, Inc.	MD	Healthcare	568	04/16/2024	Improper Disposal	Paper/Films

71

Train Staff on Email Hacking Tricks

72

Email Hacking Tricks



73

Ransomware
Major Concern for 2024 and Beyond

74

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

75

What does OCR say?

Office for
Civil Rights

76

What does OCR say?

OCR Makes It Official:

Ransomware Attacks ARE HIPAA Breaches!!

77

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 (or data) was encrypted prior to the attack it, Safe Harbor may apply**

78

Trial Attorneys – a dangerous aspect to HIPAA/SAMHSA moving forward

79

CANNOT SUE <u>UNDER</u> 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.

80

Private Legal Remedies

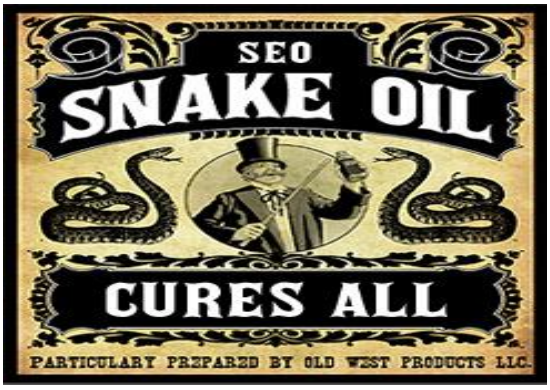
- If the violation resulted in damages, meaning you suffered some kind of verifiable financial loss, slander or defamation you may have a civil claim against the individual who violated your HIPAA rights.

81

HIPAA RESOURCES

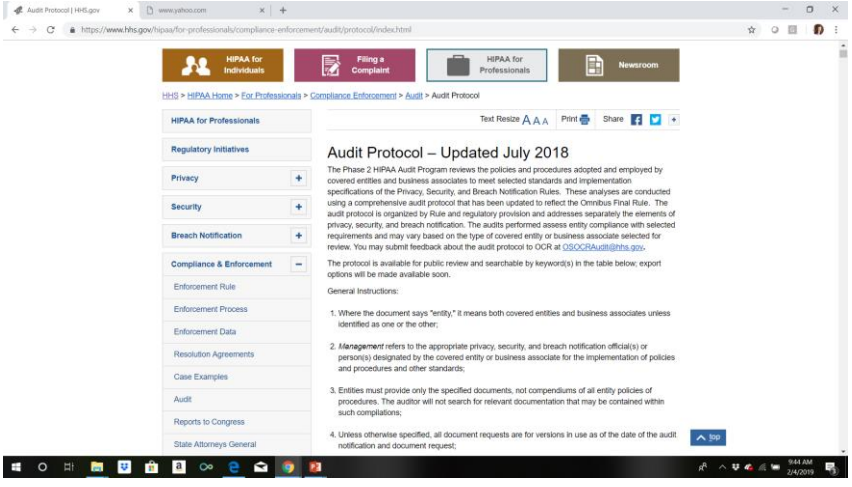
82

ALWAYS FACT CHECK WITH WWW.HHS.GOV
DON'T FALL FOR SNAKE OIL!



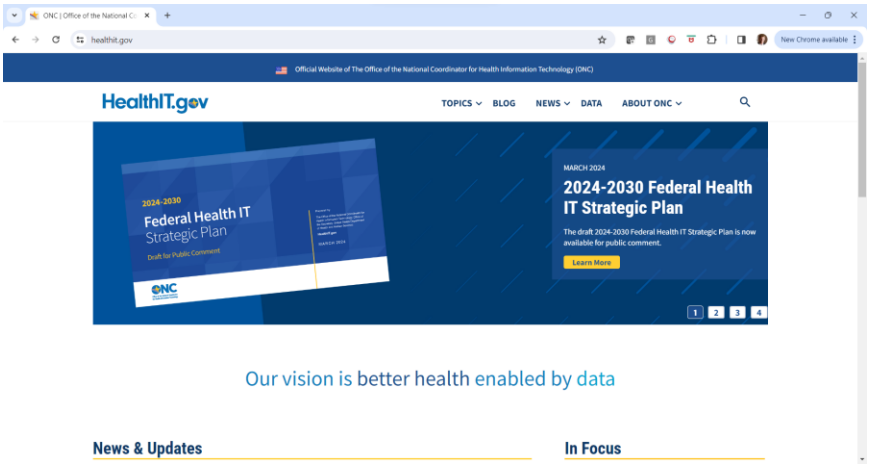
83

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



84

http://www.healthit.gov/

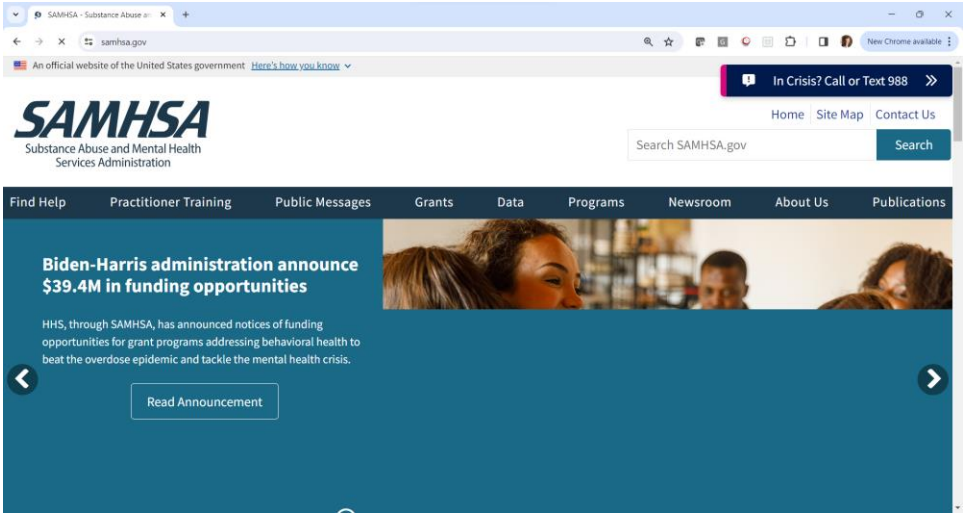


85

SAMHSA RESOURCES

86

www.samhsa.gov



87

Best Course of Action

BE PROACTIVE!!

88

THE END

Q&A

www.hipaa-consulting.com

89