HIPAA Clinic Assessment – Free Gift
While you are Waiting

- Take 5 minutes to:

  - Helps us know how HIPAA regs apply to your clinic; and
  - You will get a Free ADA Website Compliance Scan

Visit www.patientdataprotection.com

3 HIPAA Mistakes Most Acupuncturists Make

Presented by: David Bibbey, MSOM, Dipl.Ac., L.Ac

Sponsored by: Patient Data Protection

06/14/2023

Areas of Emphasis

- NO HIPAA Privacy & Security Plan
- NO Data Control & Security Plan
- NO Annual Security Risk Assessment and Analysis (SRA)

#1 Mistake Big Mistake Acupuncturists make

No HIPAA Privacy & Security Plan

Visit www.patientdataprotection.com

Why Acupuncturists need a HIPAA Privacy & Security Plan

- Top 2 reasons are because Acupuncturists collect, manage, or transmit patients' Protected Health Information (PHI)
  - Handwritten & Digital (ePHI)
- How is PHI defined?

Patient Name	Medical record number	Any photographic image
Patinet Address	Health plan number	Finger or voice print
Treatment/Birth Dates	ID or license number	Account numbers
Telephone/Fax numbers	Internet (IP) Address	Device identifiers
Email address	Web URL	Any unique identifier
Social Security Number	Vehicle identifiers	

HIPAA Privacy & Security Plan

- SECTION 1: Provider Responsibilities
- SECTION 2: Use and Disclosure of PHI
- SECTION 3- Patient's Individual Rights
- SECTION 4- PHI Breach Reporting
- Why is this important?
  - This is a guiding document for your clinic/business
  - It is a reference tool for training & patients
  - It's required under HIPAA for staff & patients

SECTION 1: Responsibilities of the health care provider – covered entity

- Privacy Officer
- ePHI Manage/Share Policy
- Workforce Training*
- Clinic Data Safeguards (Admin/Phys/Tech)
- Privacy Notices
- Patient/Workforce Complaints
- Sanctions for Violations of Privacy Policy
- Mitigation of Inadvertent PHI Disclosures
- No Intimidating/Retaliatory Acts
- No Waiver of HIPAA Data Privacy
- Plan Document
- Documentation
- Electronic Health Records
- Access Authorization

HIPAA Plan: Identifies the Privacy Officer and describes the workforce training policy

- **Privacy Officer**
- HR/Clinic Director will be the HIPAA Privacy Officer for *Practice Name*. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy, including this Privacy Policy and the Company's use and disclosure procedures. The Privacy Officer will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI. The Privacy Officer can be reached at Phone#.

- **Workforce Training Policy**
- It is the Company's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. All staff members receive HIPAA training. Whenever a privacy incident has occurred, the Privacy Officer in collaboration with management will evaluate the occurrence to determine whether additional staff training is in order. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the Company's privacy policies and procedures.

HIPAA Plan: Details how your office provides patients with privacy notices

- **Privacy Notices**
- The Privacy Officer is responsible for developing and maintaining a notice of the Company's privacy practices that describes:
- • the uses and disclosures of PHI that may be made by the Company;
- • the patient's rights; and
- • the Company's legal duties with respect to the PHI.
- The privacy notice will inform participants that the Company will have access to PHI.
- The privacy notice will also provide a description of the Company's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.
- The notice of privacy practices will be individually delivered to all patients:
- • when a patient is established, at the time of treatment, and on an ongoing basis, as needed the Company must document a patient's written consent; and
- • update within 60 days after a material change to the notice.
- The Company will also provide notice of availability of the privacy notice at least once every three years.

HIPAA Plan: Details staff management and sanctions for policy violations

- Sanctions for Violations of Privacy Policy*
- Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Plan will be imposed in accordance up to and including termination.
- Write up a plan for providing staff a warning, retraining and termination and have each staff person read, sign and return a copy of the plan.
- No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy
- No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.
- No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

SECTION 2: Use and Disclosure of PHI

- Use and Disclosure Defined*
- Access to PHI is Limited to Certain Employees
- Disclosures of PHI Pursuant to an Authorization*
- Permissive Disclosures of PHI
- Complying with the “Minimum-Necessary” Standard*
- Disclosures of PHI to Business Associates
- Disclosures of De-Identified Information
- Disclosures to Family, Friends or Others-Patient Location
- Removing PHI from Company Premises
- Faxing PHI

HIPAA Plan: Defines policies and terms related to “use” and “disclosure”

- **Use and Disclosure Defined***
- The Company will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure“ are defined as follows:
- •**Use:** The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Company, or by a Business Associate of the Company.
- •**Disclosure:** For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the practice with a business need to know PHI.

- **Disclosures of PHI Pursuant to an Authorization***
- PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the Patient. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

HIPAA Plan: Defines “Minimum Necessity” and PHI disclosing standards

- **Complying with the “Minimum-Necessary” Standard***
- HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.
- The "minimum-necessary" standard does not apply to any of the following:
- • uses or disclosures made to the individual;
- • uses or disclosures made pursuant to a valid authorization;
- • disclosures made to the Department of Labor;
- • uses or disclosures required by law; and
- • uses or disclosures required to comply with HIPAA.

- **Minimum Necessary When Disclosing PHI.**
- For making disclosures of PHI to any business associate or providers, or auditing purposes, only the minimum necessary amount of information will be disclosed.
- All other disclosures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Visit www.patientdataprotection.com

HIPAA Plan: 2 Sections Down – 2 more !!!

SECTION 3–Patient INDIVIDUAL RIGHTS.

- Access to PHI and Requests for Amendment*
- Accounting
- Requests for Alternative Communication
- Requests for Restrictions on Uses and Disclosures of PHI
- When a Patient Requests a Copy of their Record*
- Patient's Request for Copy of Clinic Notes or Labs
- Acceptable Methods of Verification of Identification*
- When the Requestor is the Patient's Legally Authorized Representative
- Other Methods*

HIPAA Plan: Describes a patient's individual rights

- **Access to PHI and Requests for Amendment**
- HIPAA gives participants the right to access and obtain copies of their PHI that the Company or its business associates maintains.
- HIPAA also provides that participants may request to have their PHI amended.
- The Company will provide access to PHI, and it will consider requests for amendment that are submitted in writing by participants.

- **Patient Requests a Copy of their Record**
- A patient can request a copy of their medical record by completing a Request for Accessing / Inspecting / Copying Health Information Form and submitting it to Company. The office must process and respond to the request within 30 days.
- Patients can receive this form from the office staff or clinic director.

HIPAA Plan: Defines ID verification for records requests

- **Acceptable Methods of Verification of Identification***
- If the request is made in person, verification of identity asking for photo identification. A copy of the I.D. must be attached to the request and placed in the Participants record.
- If the request is made over the telephone, verification will be accomplished by identifying information such as social security number and birth date, or callback process.
- If the request is made in writing, verification will be accomplished by requesting a photocopy of photo identification, or the signature on the written request must be compared with the signature in the Patient record. In addition, the practice will need to verify the validity of the written request by contacting the Patient by telephone.

- **Other Methods**
- The Company may use any other method of verification that, in the Company's discretion, is reasonably calculated to verify the identity of the person making the request. Some acceptable means of verification include, but are not limited to:
- Requesting to see a photo ID
- Requesting a copy of a power of attorney
- Confirming personal information with the requestor such as date of birth, policy number or social security number
- Questioning a child's caretaker to establish the relationship with the child
- Calling the requestor back through a main organization switchboard rather than a direct number

SECTION 4–PHI BREACH REPORTING

- Breach Notification Requirements
- Complaint/Concerns Reporting
- Non-Retaliation

HIPAA Plan: Describes breach notice and complaint reporting

- **Breach Notification Requirements**
- Following a breach of unsecured PHI covered must provide notification of the breach to affected individuals and if needed to the media. In addition, business associates must notify covered entities that a breach has occurred.
- •Individual Notice
- •Media Notice: more than 500 records
- •Notice to the Secretary: < 60 days
- •Notification by a Business Associate

- **Complaint/Concerns Reporting**
- Concerns about the Company's privacy practices may arise in a variety of contexts and may be received by many different persons. It is important that the Company responds to concerns and complaints in a timely manner.
- When a staff member hears or receives a complaint/concern, they should ask the complainant if they wish to file a formal complaint and offer to assist with the form. Even if the person does not wish to file a complaint or provide identifying information, the staff member should proceed with the procedures prescribed by the Compnay.

HIPAA Plan: Describes "Non-Retaliation" office policy

- **Non-Retaliation**
- The Company shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident.

#2 Big Mistake Acupuncturists Make

No Data Control and Security Plan

Visit www.patientdataprotection.com

HIPAA Encryption Requirements

- **HIPAA Data at Rest Encryption Requirements**
- The HIPAA data at rest encryption requirements (access controls) refer to any ePHI maintained on a server, in a desktop file, on a USB, or in a mobile device.
- However, it is a good idea to apply the HIPAA data at rest encryption requirements to as much data as possible to prevent hackers getting into a network at its weakest point and navigating laterally through the network.
- Applying the HIPAA data at rest encryption requirements to as much data as possible (including login credentials) can create sufficient obstacles for hackers to give up and move onto an easier target.
- While this may slow down some processes (because encrypted access takes longer to perform), any loss in productivity is compensated for with a higher level of security.

HIPAA Plan: HIPAA Compliant Email Encryption Software

- HIPAA compliant email encryption software is the most effective way to protect ePHI contained within emails as it not only encrypts the text content of emails, but also any file or image attachments.
- However, it is important to note that, if using an email service alongside HIPAA compliant email encryption software, it will be necessary to enter into a Business Associate Agreement with the service provider.
- To ensure the integrity/availability of ePHI emailed, implement a HIPAA compliant email archiving solution that takes a copy of each email as it passes through the mail server and stores it in read-only format on a secure server.
- This not only guarantees there is a copy of each email but can also help Covered Entities more easily comply with retention requirements for HIPAA documentation and patients' medical records. Minimum 6 years

Is Office 365 email encryption HIPAA compliant?

- Office 365 email encryption is HIPAA compliant provided a Business Associate Agreement is signed with Microsoft.
- This is because, although Microsoft cannot access the data (because the Covered Entity or Business Associate maintains the decryption key), the Department for Health and Human Services considers cloud service providers to have persistent access to data.

Visit www.patientdataprotection.com

HIPAA Plan: Must Document Data Control & Security Policies and Procedures

- The Company will protect the confidentiality, integrity and availability of PHI and ePHI by implementing sound data management and backup practices.
- The Company establishes and implements procedures to create and maintain retrievable exact backup copies of electronic protected health information (ePHI) as required by 45 CFR § 164.308(a)(7)(ii)(A)
- (HIPAA Security Rule – Contingency Plan – Data Backup Plan).
- The procedures will assure that complete, accurate, retrievable and tested back-ups are available for all ePHI on all information systems used by the Company, with the following exceptions:
- 1. Additional copies of ePHI created for convenience do not need to be backed up.
- 2. Duplicate records and data do not need to be backed up provided that the original ePHI data is properly backed up and available in a timely manner

HIPAA Plan: Must Document Data Control & Security Policies and Procedures

- The Company creates a retrievable exact backup copy of ePHI before movement of equipment as required by 45 CFR § 164.310(d)(2)(iv) (HIPAA Security Rule – Device and Media Controls – Data Backup and Storage).
- The Company maintains a record of location and movement of hardware and electronic media containing ePHI and any person responsible therefore as required by 45 CFR § 164.310(d)(2)(iii)
- (HIPAA Security Rule – Device and Media Controls – Accountability).
- The Company creates and stores backup copies according to its Continuity Plan and HIPAA Security Risk Management Plan.
- The Company creates and stores backup copies for a sufficient length of time to accomplish the following:
- 1. To restore ePHI lost or corrupted.
- 2. To support the Company's Disaster Recovery Plan
- 3. To support authentication of ePHI
- 4. Data backups will be tested according to HIPAA requirements

HIPAA Plan: Website Security Compliance

- HIPAA compliant websites are necessary if it is used to collect, store, process, display, or transmit ePHI.
- Any webpage that allows patients to submit information can be considered a contact form.
- Even the simplest contact form must be secure; a person contacting a doctor will not want anyone to have easy access to their inquiries regarding particular health problems.

- HIPAA Compliant Web Servers
- PHI must be protected at every step.
- HIPAA compliant servers must include the most secure protection available while PHI is in the Cloud, but it also must be secure during any sort of internet transfer.
- That includes end to end encryption for any information that is sent back to the or between healthcare providers.

HIPAA Plan: Website Security Compliance

- Collecting PHI – If your website collects any individually identifiable medical information, such as symptoms, conditions, or requested healthcare services, you are collecting PHI. That information must be ferried securely to the web server.
- Storing PHI – Whether you store the PHI on your own server or on a third-party server, you must ensure that the security of the information is HIPAA compliant, and that regular maintenance is done to keep it so.
- Transmitting PHI – PHI must also be secure and encrypted when it is transferred in any way. This includes direct transfer between servers, via email, or any other digital transference.
- Health care providers and their business associates are not permitted to use tracking technologies in a manner that would result in impermissible disclosures8 of PHI to tracking technology vendors or any other violations of the HIPAA Rules.
- Most Google Analytics and Meta Pixel software tools are not HIPAA compliant, because patient data is shared unauthorized ways.
- OCR's Bulletin presumes that when a healthcare provider collects individually identifiable health information (IIHI) through a website or mobile app, the individual is automatically connected to that provider, and that connection "is indicative that the individual has received or will receive health care services or benefits from the covered entity."

#3 Big Mistake Acupuncturists Make

No Security Risk Assessment & Analysis (SRA) – Web-Based App

Visit www.patientdataprotection.com

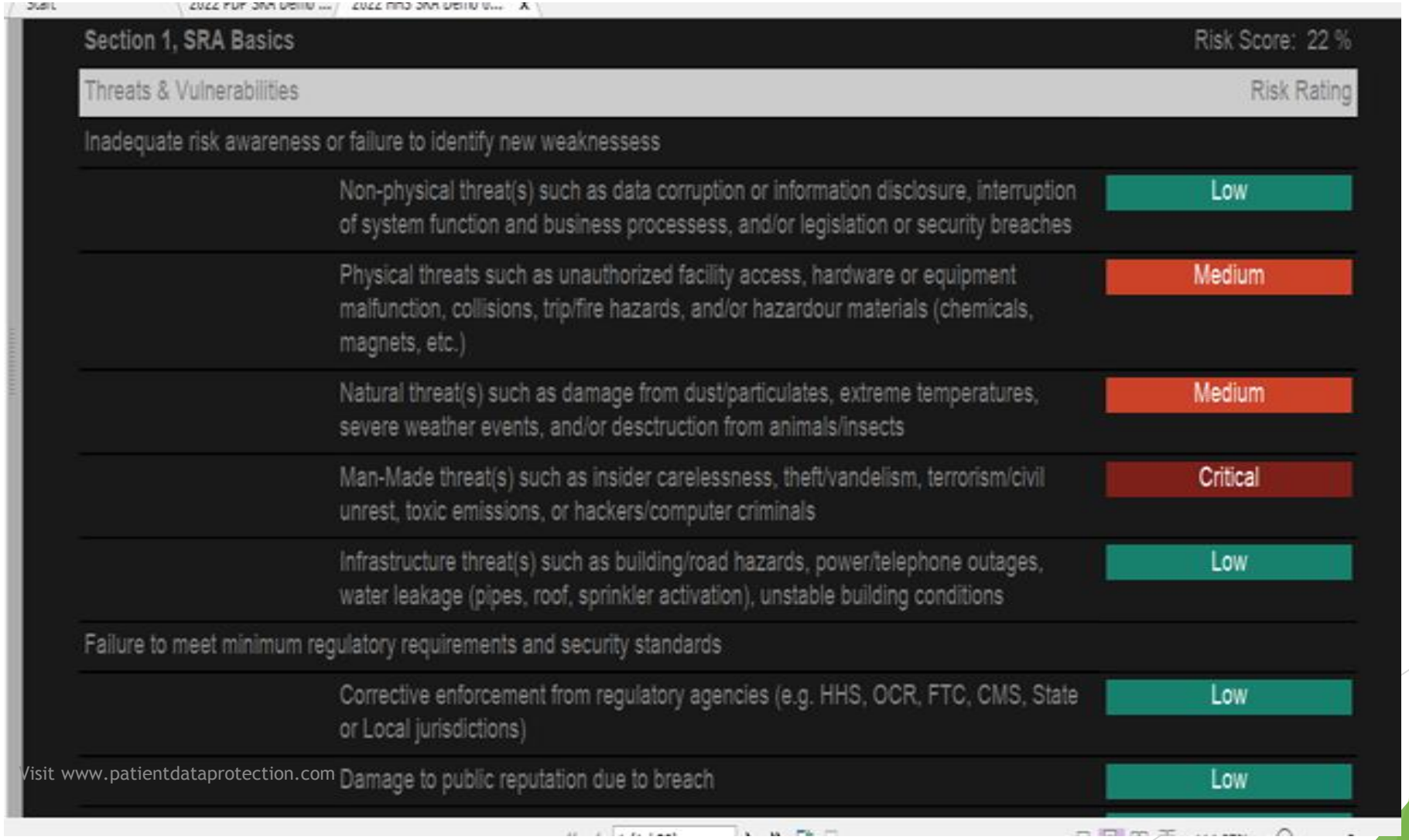
SRA tool survey tool allows providers to assess 7 critical areas of HIPAA compliance online

- Section 1: SRA Basics
  - Clinic Details, Digital Inventory, and Staff
- Clinic Policies, Procedures & Docs
  - HIPPA Administrative Standards
- Clinic Staff Training
- Patient Data Access Management
  - HIPAA Physical/Technical Standards
- Business Associates Agreements
- Contingency/Disaster Planning

HIPAA SRA – Tool Results

Visit www.patientdataprotection.com

SRA Tool - Analysis



Section 1, SRA Basics — Risk Score: 22 %

Threats & Vulnerabilities	Risk Rating
Inadequate risk awareness or failure to identify new weaknessess	
Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processess, and/or legislation or security breaches	Low
Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardour materials (chemicals, magnets, etc.)	Medium
Natural threat(s) such as damage from dust/particulates, extreme temperatures, severe weather events, and/or desctruction from animals/insects	Medium
Man-Made threat(s) such as insider carelessness, theft/vandelism, terrorism/civil unrest, toxic emissions, or hackers/computer criminals	Critical
Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof, sprinkler activation), unstable building conditions	Low
Failure to meet minimum regulatory requirements and security standards	
Corrective enforcement from regulatory agencies (e.g. HHS, OCR, FTC, CMS, State or Local jurisdictions)	Low
Damage to public reputation due to breach	Low

SRA Tool – Compliance/Audit time-stamp

Q2. Do you review and update your SRA?			
Answer	Yes.		
Education	This is the most effective option to protect the confidentiality, integrity, and availability of ePHI.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI	Required	David III	Thu Sep 29 12:28:00 EDT 2022

Q3. How often do you review and update your SRA?			
Answer	Periodically but not in response to operational changes and/or security incidents.		
Education	An accurate and thorough security risk assessment should be reviewed and updated periodically, or in response to operational changes, or security incidents.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(a)(1)(ii)(A) NIST CSF: ID.RA, ID.AM, ID.BE, PR.DS, PR. IP, RS.MI	Required	David III	Thu Sep 29 12:28:07 EDT 2022

Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?			
Answer	I don't know.		
Education	Include all information systems that contain, process, or transmit ePHI in your security risk assessment. In addition, document your systems in a complete inventory.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: N/A NIST CSF: ID.RA, PR.	N/A	David III	Thu Sep 29 12:28:14 EDT 2022

SRA Tool – Section 3 – Security & workforce: Threats and Vulnerabilities

Section 3, Security & Workforce		Risk Score: 42 %
Threats & Vulnerabilities		Risk Rating
Unqualified, uninformed, or lack of Security Officer		
	Unqualified workforce or untrained personnel on security standards and procedures	Critical
	Security policies not followed when not enforced	High
	Misuse of audit tools, information systems, and/or hardware	Medium
	Proliferation of unknown threats	Critical
	Insider carelessness exposing ePHI	Medium
	Unauthorized information disclosure (ePHI, proprietary, intellectual, or confidential)	High
	Disruption of business processes, information system function, and/or prolonged adversarial presence within information systems	Medium
Section Questions		

SRA Tool – Section 6 – Business Associates

Q13. Do you obtain Business Associate Agreements (BAAs) from business associates who access another covered entity's ePHI on your behalf?			
Answer	Yes. We make sure to have BAAs in place with covered entities for which we are Business Associates as well as subcontractors to those covered entities who contract with us.		
Education	This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI.		
References	**Compliance**	**Username**	**Audit Date**
HIPAA: §164.308(b)(2) NIST CSF: N/A	Required	David III	Thu Sep 29 12:37:07 EDT 2022

SRA Analysis is required to provide Risk Management & Action Plan

- When done correctly the SRA Assessment gives providers data that identifies their level of HIPAA compliance.
- No area can be ignored, but compliance is always viewed as work in progress
- The SRA tool will assess 7 areas of HIPAA compliance and generate a Report/Analysis.
- The Analysis report will help you identify specific areas that require improvement.
- Identifying those area of improvement will help clinics prioritize compliance tasks.
- Then plan and budget time and resources to move to better compliance under HIPAA.

The SRA Analysis – Roadmap for developing Risk Management Plan

- Priorities
  - Identify/Eliminate
  - Vulnerabilities / Risks
    - CRITICAL
    - HIGH
    - MEDIUM

- Create 2023 Risk Management Plan
- Identify 3-5 top priorities
  - Solve those issues
- You avoided any "Willful Neglect" claim…
  - You have developed P & P's
  - You are assessing your clinic
  - You are working to correct known deficiencies…this is ALWAYS a work in progress

Areas of Emphasis

- NO HIPAA Privacy & Security Plan
- NO Data Control & Security Plan
- NO Annual Security Risk Assessment and Analysis (SRA)

Patient Data Protection: < $20 week

- **Compliance Kits include:**
- Customized Clinic Privacy & Security Plans (4 sections-45 pages)
  - This includes customized HIPAA required patient forms
- Secure Website Server Platform
  - Website PHI Encryption
  - HIPAA Compliant Email
  - HIPAA Compliant Backup (6 years)
- SRA Tool – Auto Survey for Clinic

- **Other services:**
- ADA Website Compliance tools
- Website Editing/Monitor/Develop
- Good Faith Estimate Compliance
  - Website
  - Office
- Website Privacy Notices
- Website Trouble-shooting
- HIPAA /ADA Compliance Support

Visit www.patientdataprotection.com

HIPAA Clinic Assessment – Free Gift

Thank you for joining us…

- Time for Questions…
- Take 5 minutes to:

  - Helps us know how HIPAA regs apply to your clinic
  - FREE HIPAA Clinic Eval & ADA Website Compliance Scan

Visit www.patientdataprotection.com