Section 1, SRA Basics Risk Score: 0 %

Threats & Vulnerabilities Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Has your practice completed a security risk assessment (SRA) before?	Yes.	Required	Kristian Quino	Tue May 31 15:33:45 EDT 2022
Q2. Do you review and update your SRA?	Yes.	Required	Kristian Quino	Tue May 31 15:42:32 EDT 2022
Q3. How often do you review and update your SRA?	Periodically and in response to operational changes and/or security incidents.	Required	Kristian Quino	Tue May 31 15:52:21 EDT 2022
Q4. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?	Yes.	N/A	Kristian Quino	Tue May 31 15:52:44 EDT 2022
Q6. What do you include in your SRA documentation?	Our SRA documentation includes possible threats and vulnerabilities which we assign impact and likelihood ratings to. This allows us to determine severity. We develop corrective action plans as needed to mitigate identified security deficiencies according to which threats and vulnerabilities are most severe.	Required	Heather Taylor	Thu Jun 09 14:41:51 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q7. Do you respond to the threats and vulnerabilities identified in your SRA?	Yes, we respond. We also maintain supporting documentation of our response.	Required	Kristian Quino	Tue May 31 15:54:54 EDT 2022
Q8. Do you identify specific personnel to respond to and mitigate the threats and vulnerabilities found in your SRA?	Yes.	Required	Kristian Quino	Tue May 31 15:53:44 EDT 2022
Q9. Do you communicate SRA results to personnel involved in responding to threats or vulnerabilities?	Yes.	Required	Kristian Quino	Tue May 31 15:53:48 EDT 2022
Q10. How do you communicate SRA results to personnel involved in responding to identified threats or vulnerabilities?	Written and verbal communication as well as coordinated corrective action planning.	Required	Kristian Quino	Tue May 31 15:54:00 EDT 2022

Section 2, Security Policies Risk Score: 0 %

Threats & Vulnerabilities	Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?	Yes, we have a process by which management develops, implements, reviews, and updates security policies and procedures.	Required	Kristian Quino	Tue May 31 15:55:06 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q2. Do you review and update your security documentation, including policies and procedures?	Yes, we review and update our security documentation periodically and as necessary.	Required	Kristian Quino	Tue May 31 15:55:15 EDT 2022
Q3. How do you update your security program documentation, including policies and procedures?	We have a periodic review of information security policies that formally evaluates their effectiveness. Policies and procedures are updated as needed.	Required	Kristian Quino	Tue May 31 15:55:29 EDT 2022
Q4. Is the security officer involved in all security policy and procedure updates?	Yes.	Required	Kristian Quino	Tue May 31 15:55:32 EDT 2022
Q5. How does documentation for your risk management and security procedures compare to your actual business practices?	Our risk management and security documentation completely and accurately reflects our actual business practices.	Required	Kristian Quino	Tue May 31 15:55:42 EDT 2022
Q6. How long are information security management and risk management documents kept?	We maintain documents for at least six (6) years from the date of their creation or when they were last in effect, whichever is longer. These documents are maintained and backed up.	Required	Kristian Quino	Tue May 31 15:55:54 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q7. Do you make sure that information security and risk management documentation is available to those who need it?	Yes. Documentation is made available to appropriate workforce members in physical and/or electronic formats (for example, our practice's shared drive or intranet).	Required	Kristian Quino	Tue May 31 15:56:18 EDT 2022
Q8. How do you ensure that security and risk management documentation is available to those who need it?	Appropriate workforce members receive instruction on our information security documentation and where to find it as part of their periodic privacy and security training. Documentation is securely made available to workforce members in physical or electronic formats.	Required	Heather Taylor	Thu Jun 09 14:43:23 EDT 2022

Section 3, Security & Workforce Risk Score: 0 %

Threats & Vulnerabilities	Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Who within your practice is responsible for developing and implementing information security policies and procedures?	The security officer is a member of the workforce identified by name in policy documents.	Required	Kristian Quino	Tue May 31 15:57:01 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q2. Do you identify and document the role and responsibilities of the security officer?	Yes. The security officer is identified by role and this is documented in our practice's information security policies, which describes the role's responsibilities.	Required	Kristian Quino	Tue May 31 15:57:06 EDT 2022
Q3. Is your security officer qualified for the position?	Yes. The security officer is an assigned member of the workforce familiar with security and has the ability to design, implement, and enforce security policies and procedures.	Required	Kristian Quino	Tue May 31 15:57:18 EDT 2022
Q4. Do workforce members know who the security officer is?	Yes. Workforce members are aware of who our security officer is.	Required	Kristian Quino	Tue May 31 15:57:21 EDT 2022
Q5. Do workforce members know how and when to contact the security officer?	Workforce members are made aware of the identity of the security officer and reasons for contacting the security officer as part of their orientation to the practice (upon hire) as well as periodic reminders of our internal policies and procedures (e.g. periodic review).	Required	Kristian Quino	Tue May 31 15:57:37 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q7. How are roles and job duties defined as pertained to accessing ePHI?	We have written job descriptions, roles, and required qualifications documented for all workforce members with access to ePHI.	Required	Kristian Quino	Tue May 31 15:57:53 EDT 2022
Q8. Do you screen your workforce members to verify trustworthiness?	Yes.	Addressable	Kristian Quino	Tue May 31 15:57:57 EDT 2022
Q9. How are your workforce members screened to verify trustworthiness?	Professional references are collected and verified. Criminal background checks are performed in addition to verifying licenses, credentials, and certifications .	Addressable	Kristian Quino	Tue May 31 15:58:02 EDT 2022
Q10. Do you ensure that all workforce members (including management) are given security training?	Yes, we ensure all workforce members complete security training on a periodic basis.	Required	Heather Taylor	Thu Jun 09 14:44:45 EDT 2022
Q11. How do you ensure that all workforce members are given security training?	We keep a list of workforce members who have completed security training. Trainings are provided upon hire and periodically thereafter. The list is reviewed and verified by the security officer.	Required	Kristian Quino	Tue May 31 15:58:18 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q12. How long are records of workforce member security training kept?	Records documenting the completion of required security trainings are kept for all workforce members (including management) and retained for at least six (6) years after completion of the training.	Required	Heather Taylor	Thu Jun 09 14:49:07 EDT 2022
Q13. Are procedures in place for monitoring log-in attempts and reporting discrepancies?	Yes, these procedures workforce members' roles and responsibilities, log-in monitoring procedure, how to identify a log-in discrepancy and how to respond to an identified discrepancy.	Addressable	Kristian Quino	Wed Jun 08 12:18:50 EDT 2022
Q14. Is protection from malicious software (including timely antivirus/ security updates and malware protection) covered in your procedures?	Yes. Software protection is included in our procedures. This includes a review of our procedures for guarding against malware, and the mechanisms in place for protection, and how procedures for workforce members to follow can to detect and report malicious software.	Addressable	Kristian Quino	Wed Jun 08 12:18:58 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q15. What password security elements are covered in your security training?	Our security procedures include what our workforce roles/ responsibilities are in password security, how to safeguard passwords, how to respond to a compromised password, and how to properly change a password using various password characteristics (e.g. many characters long, easy to remember, avoiding easy to guess phrases).	Addressable	Heather Taylor	Thu Jun 09 14:49:35 EDT 2022
Q16. Do you ensure workforce members maintain ongoing awareness of security requirements?	Yes.	Addressable	Heather Taylor	Thu Jun 09 14:49:43 EDT 2022
Q17. How does your practice ensure workforce members maintain ongoing awareness of security requirements?	Formal trainings and periodic security reminders	Addressable	Heather Taylor	Thu Jun 09 14:50:02 EDT 2022
Q18. Do you have a sanction policy to enforce security procedures?	Yes.	Required	Heather Taylor	Thu Jun 09 14:50:12 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q19. What is included in your sanction policy to hold personnel accountable if they do not follow your security policies and procedures?	All of the above.	Required	Heather Taylor	Thu Jun 09 14:50:29 EDT 2022

Section 4, Security & Data Risk Score: 14 %

Threats & Vulnerabilities	Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Do you manage and control personnel access to ePHI, systems, and facilities?	Yes.	Required	Kristian Quino	Wed Jun 08 12:19:24 EDT 2022
Q2. How do you manage and control personnel access to ePHI, systems, and facilities?	Log of personnel names and access levels.	Required	Kristian Quino	Wed Jun 08 12:19:43 EDT 2022
Q3. What is your process for authorizing, establishing, and modifying access to ePHI?	Our security procedures designate personnel authorized to grant, review, modify, and terminate access. Access levels are reviewed and modified as needed.	Addressable	Heather Taylor	Thu Jun 09 14:51:40 EDT 2022
Q4. How much access to ePHI is granted to users or other entities?	Minimum access necessary based on the user's formal role.	Required	Heather Taylor	Thu Jun 09 14:53:02 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q5. How are individual users identified when accessing ePHI ?	Unique IDs and individual passwords are created for authorized workforce members and contractors in order access ePHI.	Required	Kristian Quino	Wed Jun 08 12:19:57 EDT 2022
Q6. Do you ensure all of your workforce members have appropriate access to ePHI?	Yes. We have written procedures to ensure workforce members' access privileges are minimum necessary (i.e. "need to know") based on their roles. These access privileges are approved by the security officer.	Required	Heather Taylor	Thu Jun 09 14:53:28 EDT 2022
Q7. How do you make sure that your workforce's designated access to ePHI is logical, consistent, and appropriate ?	Workforce members are granted access based on the minimum amount necessary for their role. This is consistently applied across the practice and any changes must be formally approved and documented.	Required	Heather Taylor	Thu Jun 09 14:53:59 EDT 2022
Q8. Do you use encryption to control access to ePHI?	Yes.	Addressable	Kristian Quino	Wed Jun 08 12:20:14 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q9. What procedures do you have in place to encrypt ePHI when deemed reasonable and appropriate?	Encryption is evaluated as part of our risk management process. We have procedures in place to encrypt data at rest (for example, USB drives or tapes) and in transit (for example, email or cloud EHR) whenever reasonable and appropriate, and find an alternative safeguard when not reasonable and appropriate.	Addressable	Kristian Quino	Wed Jun 08 12:20:47 EDT 2022
Q10. Do you use alternative safeguards in place of encryption?	Yes. When encryption is not reasonable or appropriate, we implement an alternative safeguard.	Addressable	Kristian Quino	Wed Jun 08 12:21:10 EDT 2022
Q11. When encryption is deemed unreasonable or inappropriate to implement, do you document the use of an alternative safeguard?	Yes. We have policies and procedures to identify encryption capabilities of our devices and information systems. When encryption is not reasonable or appropriate, we implement an alternative safeguard and document it.	Addressable	Kristian Quino	Wed Jun 08 12:21:16 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q12. Have you evaluated implementing any of the following encryption solutions in your local environment? (Full disk encryption, file/ folder encryption, encryption of thumb drives or other external media)	All of the above.	Addressable	Kristian Quino	Wed Jun 08 12:21:25 EDT 2022
Q13. Have you evaluated implementing encryption solutions for any of the following cloud services? (Email service, file storage, web applications, remote system backups)	All of the above.	Addressable	Kristian Quino	Wed Jun 08 12:21:34 EDT 2022
Q14. Have you evaluated implementing any of the following encryption solutions for data in transit? (Encryption of internet traffic by means of a VPN, web traffic over HTTP encrypted email, or secure file transfer)	All of the above.	Addressable	Kristian Quino	Wed Jun 08 12:21:42 EDT 2022
Q15. Do you periodically review your information systems for how security settings can be implemented to safeguard ePHI?	Yes.	Required	Kristian Quino	Wed Jun 08 12:21:48 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q16. How are you aware of the security settings for information systems which process, store, or transmit ePHI?	All systems which create, receive, maintain, or transmit ePHI (including any firewalls, databases, servers, and networked devices) have been examined to determine how security settings can be implemented to most appropriately protect ePHI.	Required	Kristian Quino	Wed Jun 08 12:21:57 EDT 2022
Q17. Do you use security settings and mechanisms to record and examine system activity?	Yes.	Required	Kristian Quino	Wed Jun 08 12:22:03 EDT 2022
Q18. What mechanisms are in place to monitor or log system activity?	Monitoring of system users, access attempts, and modifications. This includes a date/time stamp.	Required	Kristian Quino	Wed Jun 08 12:22:07 EDT 2022
Q19. How do you monitor or track ePHI system activity?	System activity records are reviewed as needed but not on a regular basis. Documentation of activity reviews are not maintained.	Required	Kristian Quino	Mon Jun 13 09:15:53 EDT 2022
Q20. Do you have automatic logoff enabled on devices and platforms accessing ePHI?	Yes, automatic logoff is enabled on all devices and platforms to terminate access to ePHI after a set time of inactivity.	Addressable	Kristian Quino	Wed Jun 08 12:22:18 EDT 2022
Q21. Do you ensure users accessing ePHI are who they claim to be?	Yes.	Required	Kristian Quino	Wed Jun 08 12:22:24 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q22. How do you ensure users accessing ePHI are who they claim to be?	Users authenticate themselves to access ePHI using the method authorized by our practice's policy and procedure (for example, user name and password, physical token, or biometric feature).	Required	Kristian Quino	Wed Jun 08 12:22:32 EDT 2022
Q23. How do you determine the means by which ePHI is accessed?	All systems, devices, and applications which access ePHI are identified, evaluated, approved, and inventoried. Users can only access ePHI through these approved systems, devices, and applications.	Required	Kristian Quino	Wed Jun 08 12:22:42 EDT 2022
Q24. Do you protect ePHI from unauthorized modification or destruction?	Yes. We have some procedures to protect the integrity of our ePHI but these may not be totally comprehensive.	Required	Kristian Quino	Wed Jun 08 12:23:01 EDT 2022
Q25. How do you confirm that ePHI has not been modified or destroyed without authorization?	We manually monitor changes made to ePHI in systems with audit log functionality, but do not have automated systems.	Addressable	Kristian Quino	Mon Jun 13 09:16:13 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q26. Do you protect against unauthorized access to or modification of ePHI when it is being transmitted electronically?	Yes. We have implemented technical security measures and procedures to prevent unauthorized access to and detect modification of transmitted ePHI.	Required	Heather Taylor	Mon Jun 13 10:30:21 EDT 2022
Q27. Have you implemented mechanisms to record activity on information systems which create or use ePHI ?	Yes. Activity on systems which create or use ePHI is recorded and examined through hardware, software or procedural mechanisms. However, this process is not formally documented in our procedures.	Required	Kristian Quino	Wed Jun 08 12:23:35 EDT 2022

Section 5, Security and the Practice Risk Score: 16 %

Threats & Vulnerabilities	Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Do you manage access to and use of your facility or facilities [i.e. that house information systems and ePHI]?	Yes. We have written procedures in place restricting access to and use of our facilities.	Required	Kristian Quino	Wed Jun 08 12:23:54 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q2. What physical protections do you have in place to manage facility security risks?	We have methods for controlling and managing physical access to our facility such as, keypads, locks, security cameras, etc. We also have an inventory of our practice's facilities that house equipment that create, maintain, receive, and transmit ePHI.Our policies and procedures outline managements' involvement in facility access control and how authorization credentials for facility access are issued and removed for our workforce members and/or visitors. Workforce members' roles and responsibilities in facility access control procedures are documented and communicated.	Addressable	Kristian Quino	Wed Jun 08 12:24:01 EDT 2022
Q3. Do you restrict physical access to and use of your equipment [i.e. equipment that house ePHI]?	Yes. We have written policies and implemented procedures restricting access to equipment that house ePHI to authorized users only.	Required	Kristian Quino	Wed Jun 08 12:24:09 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q4. Do you manage workforce member, visitor, and third party access to electronic devices?	Yes. We have written procedures for classifying electronic devices, based on their capabilities, connection, and allowable activities; access to electronic devices by workforce members, visitors, and/ or third parties is determined based on their classification.	Required	Heather Taylor	Thu Jun 09 15:00:15 EDT 2022
Q5. Do you have physical protections in place, such as cable locks for portable laptops, screen filters for screen visible in high traffic areas, to manage electronic device security risks?	Yes. We have physical protections in place for all electronic devices and this is documented in policy and procedure.	Required	Kristian Quino	Wed Jun 08 12:24:36 EDT 2022
Q6. What physical protections do you have in place for electronic devices with access to ePHI?	We have limited procedures for electronic device access control including some but not all of those listed above.	Required	Kristian Quino	Wed Jun 08 12:25:02 EDT 2022
Q7. Do you keep an inventory and a location record of all of its electronic devices?	Yes. Our inventory list of all electronic devices and their functions is currently documented and updated on a periodic basis.	Required	Kristian Quino	Wed Jun 08 12:25:07 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q8. Do you have an authorized user who approves access levels within information systems and locations that use ePHI?	Yes. We have written procedures outlining who has the authorization to approve access to information systems, location, and ePHI; how access requests are submitted; and how access is granted.	Addressable	Heather Taylor	Thu Jun 09 15:01:21 EDT 2022
Q9. Do you validate a person's access to facilities (including workforce members and visitors) based on their role or function?	Yes. We have procedures for validating access to our facility. Access levels are based on role or function. We also have strict requirements for validating workforce members or visitors who seek access to our critical systems and software programs.	Addressable	Heather Taylor	Thu Jun 09 15:02:36 EDT 2022
Q10. How do you validate a person's access to your facility?	We maintain lists of authorized persons and have controls in place to identify persons attempting to access the practice, grant access to authorized persons, and prevent access by unauthorized persons.	Addressable	Heather Taylor	Thu Jun 09 15:03:42 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q11. Do you have access validation requirements for personnel and visitors seeking access to your critical systems (such as IT, software developers, or network admins)?	Yes.	Addressable	Heather Taylor	Thu Jun 09 15:03:56 EDT 2022
Q12. Does this include controlling access to your software programs for testing and revisions?	Yes.	Addressable	Heather Taylor	Thu Jun 09 15:04:14 EDT 2022
Q13. Do you have procedures for validating a third party person's access to the facility based on their role or function?	Yes.	Addressable	Heather Taylor	Thu Jun 09 15:05:06 EDT 2022
Q14. Do you have hardware, software, or other mechanisms that record and examine activity on information systems with access to ePHI?	Yes.	Required	Kristian Quino	Wed Jun 08 12:25:33 EDT 2022
Q15. What requirements are in place for retention of audit reports?	Our practice retains records of audit report review for a minimum of six (6) years, consistent with retention requirements for all information security documentation.	Required	Heather Taylor	Thu Jun 09 15:05:51 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q16. Do you maintain records of physical changes upgrades, and modifications to your facility?	Yes. We have written procedures to document modifications to our facility. This includes documenting when physical security component repairs, modifications, or updates are needed and our workforce members' roles and responsibilities in that process. Any changes to our facility's security components go through an authorization process.	Addressable	Heather Taylor	Thu Jun 09 15:07:24 EDT 2022
Q17. How do you maintain awareness of the movement of electronic devices and media?	We keep a basic list of devices but do not formally track their movement.	Addressable	Kristian Quino	Wed Jun 08 12:26:13 EDT 2022
Q18. Are electronic devices secured?	Yes. We have procedures for safeguarding all electronic devices (such as screen guards, cable locks, locking storage rooms, cameras, and other physical features).	Required	Heather Taylor	Thu Jun 09 15:08:06 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q19. Do you back up ePHI to ensure availability when devices are moved?	Yes. Our critical data and ePHI is centrally stored (such as in a cloud or active directory server) that can be accessed from any authorized device.	Addressable	Kristian Quino	Wed Jun 08 12:26:35 EDT 2022
Q20. Do you ensure devices which created, maintained, received, or transmitted ePHI are effectively sanitized when they are disposed of?	Devices are given to a third-party, which wipes the data and disposes of the devices appropriately. We are not provided a certificate of destruction to confirm appropriate disposal.	Required	Kristian Quino	Wed Jun 08 12:27:05 EDT 2022
Q21. How do you determine what is considered appropriate use of electronic devices and connected network devices?	We have documented policies and procedures in place outlining proper functions to be performed on electronic devices and devices (e.g. whether or not they should access ePHI), how those functions will be performed, who is authorized to use the devices, and the physical surroundings of the devices.	Required	Heather Taylor	Thu Jun 09 15:09:01 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q22. Do you ensure access to ePHI is terminated when employment or other arrangements with the workforce member ends?	Yes. We have written procedures documenting termination or change of access to ePHI upon termination or change of employment, including recovery of access control devices (including organization-owned devices, media, and equipment), deactivation of information system access, appropriate changes in access levels and/or privileges pursuant to job description changes that necessitate more or less access to ePHI, time frames to terminate access to ePHI, and exit interviews that include a discussion of privacy and security topics regarding ePHI.	Addressable	Heather Taylor	Thu Jun 09 15:11:14 EDT 2022
Q23. Do you have procedures for terminating or changing third-party access when the contract, business associate agreement, or other arrangement with the third party ends or is changed?	Yes	Addressable	Heather Taylor	Thu Jun 09 15:11:38 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q24. How do you ensure media is sanitized prior to re-use?	We have a third party business associate sanitize devices for the practice prior to their re-use. The business associate does not provide a certificate of proper disposal identifying the sanitized devices individually (e.g. with serial numbers).	Required	Kristian Quino	Mon Jun 13 09:19:51 EDT 2022

Section 6, Security and Business Associates Risk Score: 15 %

Threats & Vulnerabilities	Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Do you contract with business associates or other third-party vendors?	Yes.	Required	Kristian Quino	Wed Jun 08 12:28:23 EDT 2022
Q2. Do you allow third-party vendors to access your information systems and/or ePHI?	Yes.	Required	Kristian Quino	Wed Jun 08 12:28:35 EDT 2022
Q3. How do you identify which business associates need access to create, receive, maintain, or transmit ePHI?	We review business associate contracts to determine which vendors or contractors require access to ePHI and we include a Business Associate Agreement (BAA) in our contract with them.	Required	Heather Taylor	Thu Jun 09 15:14:06 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q4. How does your practice enforce or monitor access for each of these business associates?	We determine degree of access based on the amount of ePHI accessed, the types of devices or mechanisms used for access, and our ability to control and monitor third-party access.	Required	Heather Taylor	Thu Jun 09 15:14:23 EDT 2022
Q5. How do business associates communicate important changes in security practices, personnel, etc. to you?	Our BAAs include language describing how security-relevant changes should be communicated to our organization.	Required	Heather Taylor	Thu Jun 09 15:14:58 EDT 2022
Q6. Have you executed business associate agreements with all business associates who create, receive, maintain, or transmit ePHI on your behalf?	Yes. We ensure all business associates have a fully executed BAA with us before creating, receiving, maintaining, or transmitting ePHI on our behalf.	Required	Heather Taylor	Thu Jun 09 15:15:10 EDT 2022
Q7. How do you maintain awareness of business associate security practices? (e.g. in addition to Business Associate Agreements)	We rely on the language of our BAAs to ensure that business associates are securing ePHI.	Required	Heather Taylor	Thu Jun 09 15:15:31 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q8. Do you include satisfactory assurances within your Business Associate Agreements pertaining to how your business associates safeguard ePHI?	Yes. Our Business Associate Agreements include specifications on authorized use and disclosure of ePHI as well as other requirements as required by the Omnibus Rule updates to HIPAA.	Required	Heather Taylor	Thu Jun 09 15:16:03 EDT 2022
Q9. What terms are in your BAA's to outline how your business associates ensure subcontractors access ePHI securely?	Our BAAs include language requiring the business associate to obtain satisfactory assurances from subcontractors as to how they protect ePHI.	Required	Heather Taylor	Thu Jun 09 15:16:29 EDT 2022
Q10. Do your BAA's require your third-party vendors to report security incidents to your practice in a timely manner?	Yes. Our BAAs describe requirements to provide satisfactory assurances for the protection of ePHI, obtain the same assurances from its subcontractors, and report security incidents (experienced by the Business Associate or its subcontractors) to our practice in a timely manner.	Required	Heather Taylor	Thu Jun 09 15:16:43 EDT 2022
Q11. Have you updated all your BAA's to reflect the requirements in the 2013 Omnibus Rule updates to HIPAA?	We have reviewed all BAAs and have confirmed their compliance with the Omnibus Rule updates to HIPAA.	Required	Heather Taylor	Thu Jun 09 15:17:03 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q12. How does your practice document all of its business associates requiring access to ePHI?	We maintain a current listing of all business associates with access to ePHI in addition to having Business Associate Agreements (BAAs) on file with any business associates with access to ePHI.	Required	Heather Taylor	Thu Jun 09 15:17:26 EDT 2022
Q13. Do you obtain Business Associate Agreements (BAAs) from business associates who access another covered entity's ePHI on your behalf?	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.	Required	Heather Taylor	Thu Jun 09 15:17:50 EDT 2022

Section 7, Contingency Planning Risk Score: 25 %

Threats & Vulnerabilities	Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Does your practice have a contingency plan in the event of an emergency?	Yes.	Required	Kristian Quino	Wed Jun 08 12:30:54 EDT 2022
Q2. Is your contingency plan documented?	Yes.	Required	Kristian Quino	Wed Jun 08 12:30:57 EDT 2022
Q3. Do you periodically update your contingency plan?	Yes.	Required	Kristian Quino	Wed Jun 08 12:31:04 EDT 2022
Q4. How do you ensure that your contingency plan is effective and updated appropriately?	We periodically review the plan's contents but do not perform any tests or exercises of the plan's effectiveness.	Required	Heather Taylor	Fri Jun 10 10:13:39 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q5. Have you considered what kind of emergencies could damage critical information systems or prevent access to ePHI within your practice?	Yes.	Required	Kristian Quino	Wed Jun 08 12:31:15 EDT 2022
Q6. What types of emergencies have you considered?	All of the above.	Required	Kristian Quino	Wed Jun 08 12:31:22 EDT 2022
Q7. Have you documented in your policies and procedures various emergency types and how you would respond to them?	Yes.	Required	Kristian Quino	Wed Jun 08 12:31:28 EDT 2022
Q8. Does your practice have policies and procedures in place to prevent, detect, and respond to security incidents?	Yes.	Required	Kristian Quino	Wed Jun 08 12:31:31 EDT 2022
Q9. How does your practice prevent, detect, and respond to security incidents?	We have a security incident response plan documented in our policies and procedures.	Required	Kristian Quino	Wed Jun 08 12:32:58 EDT 2022
Q10. Has your practice identified specific personnel as your incident response team?	Yes.	Required	Heather Taylor	Thu Jun 09 15:21:35 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q11. How are members of your incident response team identified and trained?	Workforce members are trained on their role and responsibilities as part of the incident response team (upon hire) as well as periodic reminders of our internal policies and procedures and testing exercises.	Required	Heather Taylor	Thu Jun 09 15:22:02 EDT 2022
Q12. Has your practice evaluated and determined which systems and ePHI are necessary for maintaining business-as-usual in the event of an emergency?	Yes, we have a process of evaluating all hardware and software systems, including those of business associates, to determine criticality of the systems and ePHI that would be accessed by executing our contingency plan. This is documented along with our asset inventory.	Required	Kristian Quino	Wed Jun 08 12:35:54 EDT 2022
Q13. How would your practice maintain access to ePHI in the event of an emergency, system failure, or physical disaster?	We have established procedures and mechanisms for obtaining necessary electronic protected health information during an emergency.	Required	Kristian Quino	Wed Jun 08 12:38:03 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q14. How would your practice maintain security of ePHI and crucial business processes before, during, and after an emergency?	We have contingency plans which will be used to maintain continuity of security processes during an emergency setting.	Required	Kristian Quino	Wed Jun 08 12:38:11 EDT 2022
Q15. Do you have a plan for backing up and restoring critical data?	Yes, we have a plan for creating retrievable, exact copies of critical data and how to restore that data. We do not have a process for testing and revising this plan.	Required & Addressable	Kristian Quino	Wed Jun 08 12:38:26 EDT 2022
Q16. How is your practice's emergency procedure activated?	Upon identification or initiation of an emergency situation, emergency procedures are activated according to documented procedure, such as by formal communication from the security officer or other designated personnel.	Required	Kristian Quino	Wed Jun 08 12:38:33 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q17. How is access to your facility coordinated in the event of disasters or emergency situations?	We have written policies and procedures outlining facility access for the restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency. Members of the workforce who need access to the facility in an emergency have been identified. Roles and responsibilities have been defined. A backup plan for accessing the facility and critical data is in place.	Addressable	Kristian Quino	Wed Jun 08 12:38:42 EDT 2022
Q18. How is your emergency procedure terminated after the emergency circumstance is over?	Upon the conclusion of the emergency situation, normal operations are resumed according to documented procedure, such as by formal communication from the security officer or other designated personnel.	Required	Kristian Quino	Wed Jun 08 12:38:48 EDT 2022
Q19. Do you formally evaluate the effectiveness of your security safeguards, including physical safeguards?	Yes.	Required	Heather Taylor	Thu Jun 09 15:24:20 EDT 2022

Question	Answer	Compliance	Username	Date/Time
Q20. How do you evaluate the effectiveness of your security safeguards, including physical safeguards?	We have procedures in place to evaluate the effectiveness of our security policies and procedures, physical safeguards, and technical safeguards but we do not update them with any set frequency.	Required	Heather Taylor	Thu Jun 09 15:25:35 EDT 2022

Practice Information (1 location)

Practice Name	BIM Group
Address	1151 Red Mile Rd
City, State, Zip	Lexington, KY, 40504
Phone, Fax	(859) 255-9455
Point of Contact	Heather Taylor
Title/Role	Sr. Director of Operations
Phone	(859)255-9455
Email	htaylor@bimgroup.us

Asset Information (0 total)

Risk	ID#	Type	Status	ePHI	Encryption	Assignment	Location

Business Associates and Vendors (0 total)

Vendor Name	Vendor Type	Satistfactory Assurances	Risk Assessed