JOHANSON GROUP

HIPAA Report on Compliance

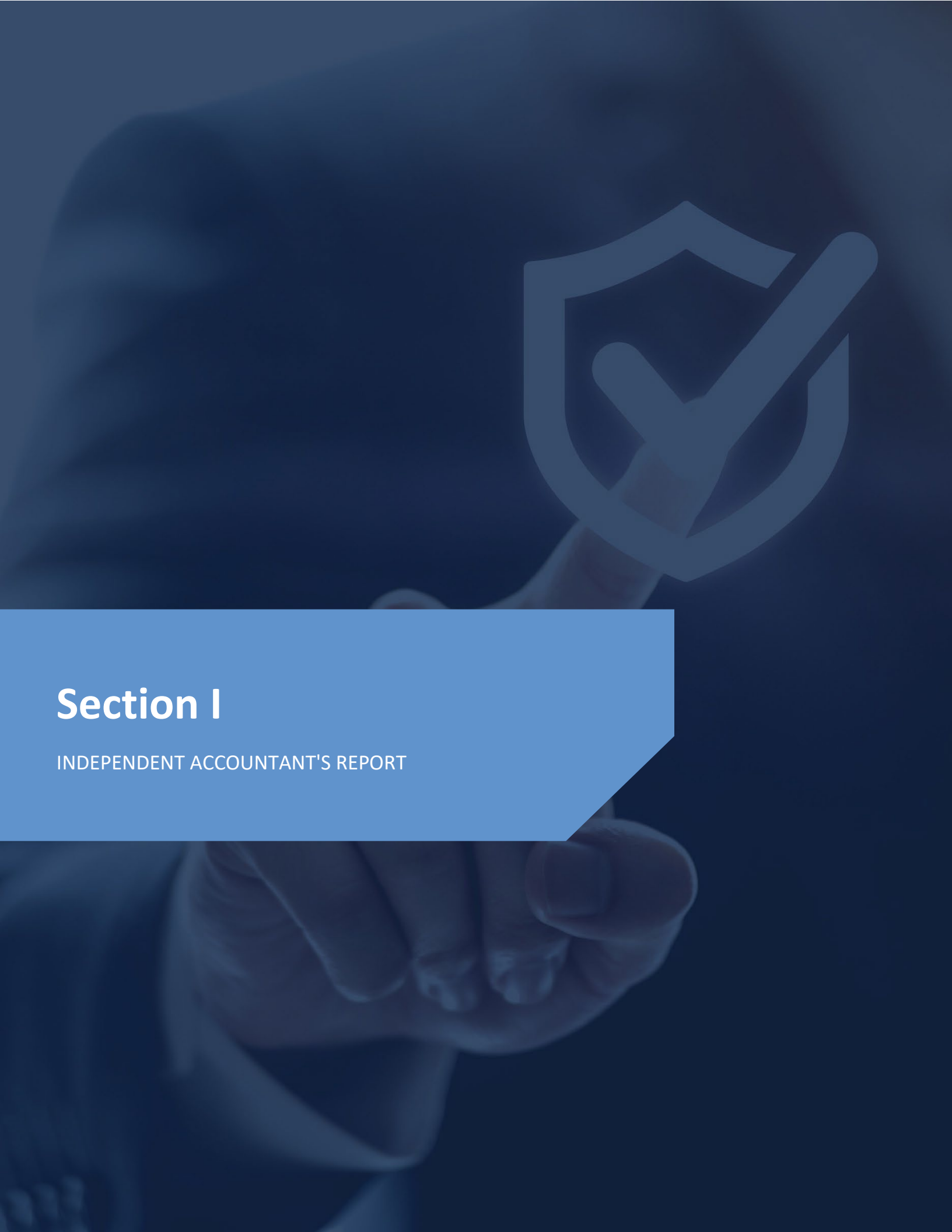
Report on Compliance as defined by the HIPAA Audit Program As published by the U.S. Department of Health and Human Services covering Health Information Privacy related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and to the applicable HIPAA Privacy, Security and Breach Notification Rule Protocols

As of a Point in Time, April 15, 2025

Together with Independent Service Auditor's Report

WPS unlocking potential

TABLE OF CONTENTS



Section I

INDEPENDENT ACCOUNTANT'S REPORT

unlocking potential

Independent Accountant's Report

To the Management of Manson Western, LLC dba Western Psychological Services

We have examined management of Manson Western, LLC dba Western Psychological Services' Western Psychological Services assertion, included in this report, that Manson Western, LLC dba Western Psychological Services complied with the specified requirements as defined by the HIPAA Audit Program - Updated July 2018 as published by the U.S. Department of Health and Human Services covering Health Information Privacy related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and to the applicable HIPAA Privacy, Security and Breach Notification Rule Protocols, collectively known as the "HIPAA Audit Program," as of April 15, 2025.

Manson Western, LLC dba Western Psychological Services management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion about Manson Western, LLC dba Western Psychological Services' compliance with the specified requirements, based on our examination.

The detailed procedures and results of testing are enumerated in Appendix A, HIPAA Audit Program Protocol Testing and Results. In instances where safeguards and key activities are not applicable, they are labeled as such in the results of procedures column.

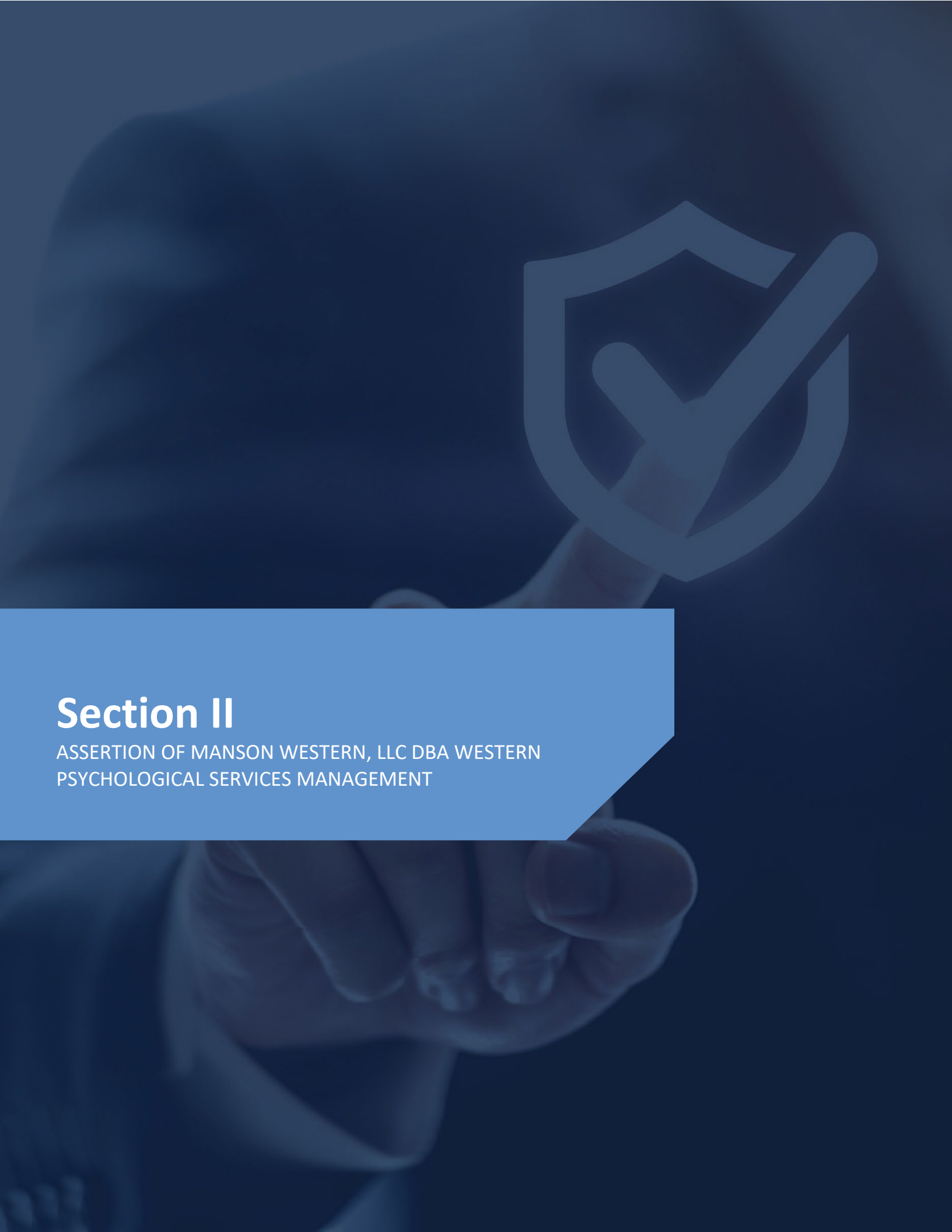
Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion about compliance with the specified requirements is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertions. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination does not provide a legal determination of Manson Western, LLC dba Western Psychological Services' compliance with the specified requirements.

In our opinion, management's assertion that Manson Western, LLC dba Western Psychological Services complied with the HIPAA Audit Program requirements listed in Appendix A, as of April 15, 2025 is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
May 29, 2025



Section II

ASSERTION OF MANSON WESTERN, LLC DBA WESTERN PSYCHOLOGICAL SERVICES MANAGEMENT

Manson Western, LLC dba Western Psychological Services Management Assertion

We have evaluated the specific requirements as defined by the HIPAA Audit Program - Updated in July 2018 as published by the U.S. Department of Health and Human Services covering Health Information Privacy related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and to the applicable HIPAA Privacy, Security and Breach Notification Rule Protocols, collectively known as the "HIPAA Audit Program," as implemented by Manson Western, LLC dba Western Psychological Services (WPS or the "Company").

1. We are responsible for selecting the HIPAA Audit Program criteria and how Manson Western, LLC dba Western Psychological Services complies with the requirements applicable to its activities. That responsibility encompasses the following:
    a. Identifying applicable compliance requirements relevant to Manson Western, LLC dba Western Psychological Services activities.
    b. Determining the types of services provided by Manson Western, LLC dba Western Psychological Services including, as appropriate, the classes of transactions and data processed that are impacted by the requirements.
    c. Determining how Manson Western, LLC dba Western Psychological Services systems capture and address significant events and conditions, other than transactions.
    d. Implementing processes and procedures to address the requirements of the HIPAA Audit Program.
    e. Identifying other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions.
    f. Establishing and maintaining internal controls to provide reasonable assurance that Manson Western, LLC dba Western Psychological Services complies with those requirements.
    g. Evaluating and monitoring Manson Western, LLC dba Western Psychological Services compliance with the HIPAA Audit Program.
    h. Determining legal, regulatory, or contractual requirements and Manson Western, LLC dba Western Psychological Services compliance with those requirements.

2. We confirm, to the best of our knowledge and belief that we have complied with the HIPAA Audit Program as of a point in time, April 15, 2025. The criteria we used in making this assertion were that:
    a. The risks that threaten compliance with the HIPAA Audit Program by Manson Western, LLC dba Western Psychological Services have been identified by management.
    b. The controls identified by management as responses to the requirements of the HIPAA Audit Program, if operating would provide reasonable assurance of the achievement of such compliance.

Manson Western, LLC dba Western Psychological Services Management
May 29, 2025

Appendix A

HIPAA Audit Program Testing and Results

Appendix A – HIPAA Audit Program Testing and Results

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
Security		
§164.308(a)(1)(i)	The organization has established security and privacy policies and procedures for protecting PHI, which are communicated to all employees and contractors. These policies and procedures are reviewed and approved by management on an annual basis or in case of significant changes.	Control is determined to be suitably designed.
§164.308(a)(1)(ii)(A), §164.308(a)(1)(ii)(B)	Management performs a formal risk assessment to identify potential risks and vulnerabilities related to confidentiality, integrity, and availability of PHI (including electronic) on an annual basis or in the event of significant changes. Identified risks, along with mitigation strategies, are documented and implemented by the organization's management.	Control is determined to be suitably designed.
§164.308(a)(1)(ii)(C)	The organization has established a formal disciplinary process describing actions to be taken against employees and contractors who fail to comply with the organization's security and privacy policies and procedures. The formalized disciplinary process is communicated to and acknowledged by employees and contractors.	Control is determined to be suitably designed.
§164.308(a)(1)(ii)(D)	Logging is enabled to record administrative activities, access login attempts, and security events, and is monitored on a regular basis. Automated alerts are configured, notifying IT management of any security issues, followed up and resolved in a timely manner through the incident management process.	Control is determined to be suitably designed.
§164.308(a)(1)(ii)(D)	On a periodic basis, management reviews the effectiveness and efficiency of processes and safeguards implemented for PHI's security and privacy. Identified issues are followed up on, and appropriate actions are taken in a timely manner.	Control is determined to be suitably designed.
§164.308(a)(2)	Management has designated a security and privacy official to oversee the development and implementation of security and privacy policies and procedures.	Control is determined to be suitably designed.
§164.308(a)(3)(i)	The organization has established and implemented an access control policy and procedure that governs access rules for granting access to ePHI and is reviewed by management annually.	Control is determined to be suitably designed.
§164.308(a)(3)(ii)(A)	Access to ePHI requires a documented access request and approval from designated management personnel prior to access provisioning.	Control is determined to be suitably designed.
§164.308(a)(3)(ii)(B)	User access to information systems containing ePHI is reviewed by management annually to assess appropriateness. Corrective actions are documented and resolved in a timely manner.	Control is determined to be suitably designed.
§164.308(a)(3)(ii)(C)	User access to information systems containing ePHI is revoked in a timely manner upon employment or contract termination.	Control is determined to be suitably designed.
§164.308(a)(4)(i),	The organization has established and implemented an access control policy and procedure that governs access	Control is determined to be suitably designed.

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
§164.308(a)(4)(ii)(B), §164.308(a)(4)(ii)(C)	rules for granting access to ePHI and is reviewed by management annually.	
§164.308(a)(5)(i)	Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.	Control is determined to be suitably designed.
§164.308(a)(5)(ii)(A)	Periodic security updates are published on the organization's website, which is accessible to all employees.	Control is determined to be suitably designed.
§164.308(a)(5)(ii)(B)	Antivirus software is installed on systems containing ePHI to prevent or detect the introduction of unauthorized or malicious software, and it is configured to force updates when available.	Control is determined to be suitably designed.
§164.308(a)(5)(ii)(C)	The organization has established and implemented a formal log management procedure for monitoring log-in attempts and reporting discrepancies. Access to change log configurations or to modify logs is restricted.	Control is determined to be suitably designed.
§164.308(a)(5)(ii)(C)	Logging is enabled to record administrative activities, access login attempts, and security events, and is monitored on a regular basis. Automated alerts are configured, notifying IT management of any security issues, followed up and resolved in a timely manner through the incident management process.	Control is determined to be suitably designed.
§164.308(a)(5)(ii)(D)	Password management procedures have been established and implemented to create, change, and safeguard passwords, and communicated to all employees.	Control is determined to be suitably designed.
§164.308(a)(6)(i)	A formal incident management process has been established, which requires incidents (breaches) to be tracked, documented, and resolved in a timely manner in accordance with the breach notification rule. The process document is reviewed and updated by management on an annual basis.	Control is determined to be suitably designed.
§164.308(a)(6)(ii)	Incidents related to security and privacy are logged, tracked, and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process.	Control is determined to be suitably designed.
§164.308(a)(7)(i)	A business continuity plan (BCP) and Disaster Recovery Plan (DRP) have been developed and tested annually (including procedures on the protection of ePHI while operating in emergency mode). Test results are reviewed, and plans are updated, if required, based on the outcome of the test performed.	Control is determined to be suitably designed.
§164.308(a)(7)(ii)(A)	Data backups are performed regularly in accordance with an approved backup policy. Backups are monitored for failure using an automated system, and appropriate corrective actions are taken.	Control is determined to be suitably designed.
§164.308(a)(7)(ii)(A)	Formal procedures that outline the data backup and restoration process are documented. The procedures are reviewed by IT management annually or in case of significant changes.	Control is determined to be suitably designed.
§164.308(a)(7)(ii)(B)	Backup restoration testing is performed on a quarterly basis to test the integrity and completeness of backup data. The Incident Management Process is invoked for anomalies.	Control is determined to be suitably designed.
§164.308(a)(7)(ii)(C), §164.308(a)(7)(ii)(D)	A business continuity plan (BCP) and Disaster Recovery Plan (DRP) have been developed and tested annually (including procedures on the protection of ePHI while operating in emergency mode). Test results are reviewed, and plans are updated, if required, based on the outcome of the test performed.	Control is determined to be suitably designed.
§164.308(a)(8)	Penetration testing is performed on an annual basis on networks and applications. Issues identified are classified according to risk, analyzed, and remediated in a timely manner.	Control is determined to be suitably designed.

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
§164.308(a)(8)	A vulnerability scan (external and internal) is performed on a quarterly basis to identify system vulnerabilities containing PHI. Issues identified are analyzed and remediated in a timely manner.	Control is determined to be suitably designed.
§164.308(a)(8)	Management performs a formal risk assessment to identify potential risks and vulnerabilities related to confidentiality, integrity, and availability of PHI (including electronic) on an annual basis or in the event of significant changes. Identified risks, along with mitigation strategies, are documented and implemented by the organization's management.	Control is determined to be suitably designed.
§164.308(b)(1)	On an annual basis, the organization performs a review of business associates or vendors with access to ePHI to assess their compliance with agreed-upon security, confidentiality, and privacy requirements.	Control is determined to be suitably designed.
§164.308(b)(1), §164.308(b)(2), §164.308(b)(3)	Business associates or vendors working on behalf of the organization and with access to PHI are required to sign an agreement outlining the security and privacy requirements for protecting PHI.	Control is determined to be suitably designed.
§164.310(a)(1)	Facilities housing systems containing PHI are protected by appropriate physical entry controls to prevent unauthorized access.	Control is determined to be suitably designed.
§164.310(a)(1), §164.310(a)(2)(ii)	Physical security policy and procedure have been established and implemented to secure the organization's facilities from unauthorized access.	Control is determined to be suitably designed.
§164.310(a)(2)(iii)	Physical access to facilities housing systems with ePHI requires formal authorization from designated management personnel prior to granting access to facilities.	Control is determined to be suitably designed.
§164.310(a)(2)(iii)	Physical access to facilities housing systems with ePHI is reviewed by an authorized management representative on a quarterly basis.	Control is determined to be suitably designed.
§164.310(a)(2)(iii)	Physical access to facilities housing systems with ePHI is revoked in a timely manner for terminated employees/contractors.	Control is determined to be suitably designed.
§164.310(a)(2)(iv)	The organization maintains documentation of repairs and modifications (i.e., maintenance records) to the facility's physical components related to security.	Control is determined to be suitably designed.
§164.310(b)	Workstation security policy and procedure have been established that specify security measures to be implemented on workstations that store or access ePHI.	Control is determined to be suitably designed.
§164.310(c)	Access to workstations that store or access ePHI is restricted to authorized users and provisioned based on the formal authorization process.	Control is determined to be suitably designed.
§164.310(d)(1)	A media handling policy and procedure have been established and implemented that govern any media movement containing ePHI into or out of the facility.	Control is determined to be suitably designed.
§164.310(d)(2)(i), §164.310(d)(2)(ii)	Data disposal policy is in place to guide secure disposal of ePHI or media containing ePHI, including guidelines on media sanitization before re-use.	Control is determined to be suitably designed.
§164.310(d)(2)(iii)	Any movement of media containing ePHI is recorded and approved by designated management personnel.	Control is determined to be suitably designed.
§164.312(a)(1)	The organization has established and implemented an access control policy and procedure that governs access rules for granting access to ePHI and is reviewed by management annually.	Control is determined to be suitably designed.

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
§164.312(a)(2)(i)	Unique user IDs and strong passwords are required in order to gain access to systems containing ePHI.	Control is determined to be suitably designed.
§164.312(a)(2)(ii)	The Emergency Access procedure has been established to obtain electronic protected health information during an emergency.	Control is determined to be suitably designed.
§164.312(a)(2)(iii)	Policies are enforced to automatically terminate workstation sessions after a predefined period of inactivity.	Control is determined to be suitably designed.
§164.312(a)(2)(iv)	A policy on the use of cryptographic controls and key management for the protection of electronic information is developed and implemented.	Control is determined to be suitably designed.
§164.312(a)(2)(iv)	Encryption technologies are used to protect the communication and transmission of ePHI over public networks and between systems.	Control is determined to be suitably designed.
§164.312(a)(2)(iv)	Electronic Protected Health Information (ePHI) is encrypted at rest (stored and backed up) using strong encryption technologies.	Control is determined to be suitably designed.
§164.312(b)	The organization has established and implemented a formal log management procedure for monitoring log-in attempts and reporting discrepancies. Access to change log configurations or to modify logs is restricted.	Control is determined to be suitably designed.
§164.312(b)	Logging is enabled to record administrative activities, access login attempts, and security events, and is monitored on a regular basis. Automated alerts are configured, notifying IT management of any security issues, followed up and resolved in a timely manner through the incident management process.	Control is determined to be suitably designed.
§164.312(c)(1)	Data integrity policy and procedure have been established that provide guidelines to protect ePHI from improper alteration or destruction.	Control is determined to be suitably designed.
§164.312(c)(2)	The organization has established and implemented an access control policy and procedure that governs access rules for granting access to ePHI and is reviewed by management annually.	Control is determined to be suitably designed.
§164.312(d)	The organization has implemented processes to verify the identity of individuals or entities before granting them access to ePHI.	Control is determined to be suitably designed.
§164.312(e)(1)	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols, and services. Firewall rules are reviewed on an annual basis by IT management.	Control is determined to be suitably designed.
§164.312(e)(1)	A formal network diagram outlining boundary protection mechanisms (e.g., firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.	Control is determined to be suitably designed.
§164.312(e)(1)	Encryption technologies are used to protect the communication and transmission of ePHI over public networks and between systems.	Control is determined to be suitably designed.
§164.312(e)(2)(i)	Data integrity policy and procedure have been established that provide guidelines to protect ePHI from improper alteration or destruction.	Control is determined to be suitably designed.
§164.312(e)(2)(i)	Logging is enabled to record administrative activities, access login attempts, and security events, and is monitored on a regular basis. Automated alerts are configured, notifying IT management of any security issues, followed up and resolved in a timely manner through the incident management process.	Control is determined to be suitably designed.

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
§164.312(e)(2)(i)	Encryption technologies are used to protect the communication and transmission of ePHI over public networks and between systems.	Control is determined to be suitably designed.
§164.312(e)(2)(ii)	Electronic Protected Health Information (ePHI) is encrypted at rest (stored and backed up) using strong encryption technologies.	Control is determined to be suitably designed.
§164.312(e)(2)(ii)	Encryption technologies are used to protect the communication and transmission of ePHI over public networks and between systems.	Control is determined to be suitably designed.
§164.314(a)(1), §164.314(a)(2)(i)(A), §164.314(a)(2)(ii)	Business associates or vendors working on behalf of the organization and with access to PHI are required to sign an agreement outlining the security and privacy requirements for protecting PHI.	Control is determined to be suitably designed.
§164.316(a), §164.316(b)(1)	The organization has established security and privacy policies and procedures for protecting PHI, which are communicated to all employees and contractors. These policies and procedures are reviewed and approved by management on an annual basis or in case of significant changes.	Control is determined to be suitably designed.
§164.316(b)(1)	Records of assessments and activities required to be performed as per defined policies and procedures are maintained and retained for six years from the date of their creation or when it was last in effect, whichever is later.	Control is determined to be suitably designed.
§164.316(b)(2)(ii), §164.316(b)(2)(iii)	The organization has established security and privacy policies and procedures for protecting PHI, which are communicated to all employees and contractors. These policies and procedures are reviewed and approved by management on an annual basis or in case of significant changes.	Control is determined to be suitably designed.
Breach		
§164.402	Risk Assessment is performed on the identified incidents following the discovery of a breach to determine the probability that PHI has been compromised and whether notifications are required.	Control is determined to be suitably designed.
§164.404(a)(1), §164.404(b), §164.404(c)(1)	Notifications regarding breach of protected health information are provided to individuals impacted by the breach without unreasonable delay and no later than 60 days after discovering a breach.	Control is determined to be suitably designed.
§164.404(d)	The organization has established a formal procedure for breach notification methods for notifying an individual, an individual's next of kin, or a personal representative.	Control is determined to be suitably designed.
§164.408	Procedures are in place to notify data breaches to appropriate authorities and media outlets. Such notifications are provided within 60 calendar days after discovery of a breach (if a breach affects 500 or more individuals) and no later than 60 days after the end of the calendar year (if a breach affects fewer than 500 individuals), except in cases stated by law enforcement official to delay the notification.	Control is determined to be suitably designed.
§164.410(b), §164.410(c)	Roles and responsibilities of business associates with respect to breach notification are communicated as part of contractual obligations requiring them to notify data breaches, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except in cases stated by law enforcement officials to delay the notification.	Control is determined to be suitably designed.
§164.412	Roles and responsibilities of business associates with respect to breach notification are communicated as part of	Control is determined to be suitably designed.

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
	contractual obligations requiring them to notify data breaches, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except in cases stated by law enforcement officials to delay the notification.	
§164.412	Communication from law enforcement officials regarding delay of breach notification is retained and documented by the organization (in case of oral communication), including the identity of the official making the statement. Breach notifications are delayed for the period as specified by the official.	Control is determined to be suitably designed.
§164.414(b)	Notifications regarding breach of protected health information are provided to individuals impacted by the breach without unreasonable delay and no later than 60 days after discovering a breach.	Control is determined to be suitably designed.
Privacy		
§164.502(a)(3)	Permitted and required uses or disclosures of protected health information by a business associate are defined in the business associate agreement/contract and implemented accordingly.	Control is determined to be suitably designed.
§164.502(a)(5)(i)	The organization has established formal policies and procedures on permitted and prohibited collection, use, and disclosure of PHI. These policies and procedures are approved by management and communicated to employees and contractors.	Control is determined to be suitably designed.
§164.502(c)	Restriction on uses or disclosures of PHI requested by individuals is recorded, monitored, and adhered to except when emergency treatment is required for the individual.	Control is determined to be suitably designed.
§164.502(d)	The organization has established a procedure to define the appropriate PHI methods for de-identification and guidance on implementing such methods. The procedure is communicated to and acknowledged by employees and contractors.	Control is determined to be suitably designed.
§164.502(e)	Business associates or vendors working on behalf of the organization and with access to PHI are required to sign an agreement outlining the security and privacy requirements for protecting PHI.	Control is determined to be suitably designed.
§164.502(a), §164.502(b), §164.502(i)	Notice of the organization's privacy practices on uses and disclosures of PHI and individuals' rights is provided to individuals whenever significant changes are made and at least once every three years.	Control is determined to be suitably designed.
164.502(j)(1)	The organization has established and communicated the communication channels that allow employees and contractors to report any misconduct anonymously with respect to the security or privacy of protected health information.	Control is determined to be suitably designed.
§164.504(e)(1),	A formal incident management process has been established, which requires incidents (breaches) to be tracked, documented, and resolved in a timely manner in accordance with the breach notification rule. The process document is reviewed and updated by management on an annual basis.	Control is determined to be suitably designed.
§164.504(e)(2)(4)	Business associates or vendors working on behalf of the organization and with access to PHI are required to sign an agreement outlining the security and privacy requirements for protecting PHI.	Control is determined to be suitably designed.
§164.506(a)	Authorization is obtained from an individual regarding the use and disclosure of their PHI except for the purposes permitted under the HIPAA privacy rule. Any uses and disclosures of PHI are documented and are consistent with	Control is determined to be suitably designed.

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
	such authorizations or exceptions.	
§164.506(b)	Explicit consent is obtained from individuals regarding the use and disclosure of their protected health information prior to collection.	Control is determined to be suitably designed.
§164.508(a)(1-3), §164.508(b)(1-3)	Authorization is obtained from an individual regarding the use and disclosure of their PHI except for the purposes permitted under the HIPAA privacy rule. Any uses and disclosures of PHI are documented and are consistent with such authorizations or exceptions.	Control is determined to be suitably designed.
§164.508(b)(5)	Revocation requests received from individuals regarding authorizations on uses or disclosures of PHI are recorded, monitored, and adhered to except when authorization was obtained as a condition of obtaining insurance coverage, which is handled in accordance with the insurance policy.	Control is determined to be suitably designed.
§164.508(b)(6)	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of PHI. Documentation, as required by HIPAA regulation, is maintained and retained for at least six years from the date of its creation or the date when it was last in effect, whichever is later.	Control is determined to be suitably designed.
§164.508(c)	Authorization is obtained from an individual regarding the use and disclosure of their PHI except for the purposes permitted under the HIPAA privacy rule. Any uses and disclosures of PHI are documented and are consistent with such authorizations or exceptions.	Control is determined to be suitably designed.
§164.512	Authorization is obtained from an individual regarding the use and disclosure of their PHI except for the purposes permitted under the HIPAA privacy rule. Any uses and disclosures of PHI are documented and are consistent with such authorizations or exceptions.	Control is determined to be suitably designed.
§164.512(i)(2)(iv)	Privacy board meetings are held on a periodic basis to review the proposed research and approve alteration or waiver of authorization by the majority of the privacy board members unless the privacy board elects to use an expedited review procedure.	Control is determined to be suitably designed.
§164.514(b)	Periodic assessments of the systems, tools and processes using de-identified PHI are performed to assess compliance with the organization's de-identification procedure. Deficiencies are tracked and resolved in a timely manner.	Control is determined to be suitably designed.
§164.514(f)	Authorization is obtained from an individual regarding the use and disclosure of their PHI except for the purposes permitted under the HIPAA privacy rule. Any uses and disclosures of PHI are documented and are consistent with such authorizations or exceptions.	Control is determined to be suitably designed.
§164.514(h)	The organization has defined processes to verify the identity and authority of a person requesting access to PHI. Request for access to PHI is facilitated based on verification of documentation, statements, or representations, and the identity of the person requesting such access.	Control is determined to be suitably designed.
§164.520(c)	Notice of the organization's privacy practices on uses and disclosures of PHI and individuals' rights is provided to individuals whenever significant changes are made and at least once every three years.	Control is determined to be suitably designed.
§164.522(a)(1) §164.522(a)(2)	Restriction requests received from individuals on uses and disclosure of their PHI are adhered to by the	Control is determined to be suitably designed.

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
	organization except when PHI is needed to provide emergency treatment to individuals. Restrictions are terminated only based on formal acknowledgement from individuals. The organization maintains documentation of such requests on restrictions or terminations.	
§164.524(c)(4)	Access request from individuals to obtain and review their PHI is documented, retained, and acted upon within 30 days from the receipt of the request. Any denial of access is communicated to individuals and handled in accordance with the requirement 45 CFR §164.524.	Control is determined to be suitably designed.
§164.526	Amendment requests received from individuals to amend their PHI are documented, retained, and carried out in accordance with the organization's policies and procedures. Any denial of the amendment, whole or in part, is communicated to individuals in a timely manner in accordance with the requirement 45 CFR §164.526.	N/A
§164.528	Individuals' requests for access to their accounting disclosures for PHI are retained and addressed within 60 days of receiving such requests. Exceptions are handled in accordance with the requirement 45 CFR §164.528.	Control is determined to be suitably designed.
§164.530(b)	Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.	Control is determined to be suitably designed.
§164.530(c)	On a periodic basis, management reviews the effectiveness and efficiency of processes and safeguards implemented for PHI's security and privacy. Identified issues are followed up on, and appropriate actions are taken in a timely manner.	Control is determined to be suitably designed.
§164.530(d)	A formal incident management process has been established, which requires incidents (breaches) to be tracked, documented, and resolved in a timely manner in accordance with the breach notification rule. The process document is reviewed and updated by management on an annual basis.	Control is determined to be suitably designed.
§164.530(e)	The organization has established a formal disciplinary process describing actions to be taken against employees and contractors who fail to comply with the organization's security and privacy policies and procedures. The formalized disciplinary process is communicated to and acknowledged by employees and contractors.	Control is determined to be suitably designed.
§164.530(e)	The organization has established a formal disciplinary process describing actions to be taken against employees and contractors who fail to comply with the organization's security and privacy policies and procedures. The formalized disciplinary process is communicated to and acknowledged by employees and contractors.	Control is determined to be suitably designed.
§164.530(f)	A formal incident management process has been established, which requires incidents (breaches) to be tracked, documented, and resolved in a timely manner in accordance with the breach notification rule. The process document is reviewed and updated by management on an annual basis.	Control is determined to be suitably designed.
§164.530(g)	The organization has established a formal disciplinary process describing actions to be taken against employees and contractors who fail to comply with the organization's security and privacy policies and procedures. The formalized disciplinary process is communicated to and acknowledged by employees and contractors.	Control is determined to be suitably designed.
§164.530(g), §164.530(h), §164.530(i)	A formal incident management process has been established, which requires incidents (breaches) to be tracked,	Control is determined to be suitably designed.

HIPAA Security, Breach & Privacy Notification Protocols		
Section	**Established Performance Criteria**	**Results of Procedure**
	documented, and resolved in a timely manner in accordance with the breach notification rule. The process document is reviewed and updated by management on an annual basis.	
§164.530(i)	The organization has established security and privacy policies and procedures for protecting PHI, which are communicated to all employees and contractors. These policies and procedures are reviewed and approved by management on an annual basis or in case of significant changes.	Control is determined to be suitably designed.