Segal

Information Security Program Summary

March 2023

Table of Contents

Content

Program Summary

Segal is committed to protecting the confidentiality, integrity and availability of the PHI, PII and other confidential data entrusted to us by our clients. As part of that commitment, and in accordance with Health and Human Services, New York State Department of Financial Services, Department of Labor Cybersecurity Guidance, and other applicable regulations, Segal has adopted HIPAA Security Rule Policies, and Information Security Policies, which define administrative, technical, and physical safeguards implemented at Segal. These safeguards and controls are summarized in this document.

Administrative safeguards

Segal has well-documented information security policies and procedures to protect the IT infrastructure and clients' data. Every employee must understand and comply with the documented and published company information security policies and procedures. Segal's information security program is based on the requirements and controls of various federal and state privacy and security regulations, as well as industry standard information security frameworks. These requirements and controls are consistent with the HIPAA Security Rule, NIST 800-53 R4, ISO 27001, AICPA Trust Services Criteria and other industry standard information security frameworks and are aligned with the cybersecurity best practices put forth by the DOL. Segal policies are accessible and regularly communicated to all employees and contractors.

Segal employees are required to participate in mandatory information security and compliance training. Training completion is monitored and reported to executive management. Sanctions for violation of security policies and procedures are prescribed and levied by management processes approved by the CEO.

All Segal staff members have a unique user ID and password that allows access to network resources as appropriate for the performance of their job. Periodic password changes are required. Connecting to the Segal network remotely requires additional levels of authentication including multifactor authentication.

Segal has documented and implemented processes and procedures for obtaining authorization for staff member's access to PHI, PII and other confidential data. These processes and procedures are managed by information technology, and requests for, and authorization of access is recorded in an information technology issue tracking and reporting system. Segal will use its "minimum necessary principle," established as part of Segal's information security policies as the basis for the type and extent of authorized access to PHI, PII and other confidential data.

Data security and risk is reviewed and analyzed on an ongoing basis through regular operational and compliance processes. Administrative, technical, and physical security control compliance is audited annually via an IT controls audit performed by an external audit firm. IT systems are monitored daily through automated and operational processes. Annual compliance audits of individual client cases are performed by practice area. These internal audits include a review of physical space, network storage and transmission of data to ensure all security

policies, procedures and standards are adhered to. Client needs and regulatory requirements are constantly evaluated throughout the company using industry standard malware and intrusion protection software, server and workstation security patch management, web filters and internet e-mail filters.

Segal leverages two data center colocations in the United States, as well as network equipment and communications rooms located at Segal facilities. Encrypted tapes are stored offsite at a data archive vendor facility in secured and environmentally controlled environments. Backup integrity checks are performed on a regular basis. Restoration of data from backups are performed periodically on a test basis.

Technical safeguards

Segal workstations are standardized with the latest patched versions of the operating systems and standard applications, and malware and intrusion protection. Additional security enhancements include complex passwords, hard disk encryption, encryption of data on removable devices, regularly scheduled system updates, monthly security updates and a regularly required reboot of all PCs.

Transmission of protected or sensitive data is accomplished through the use of industry standard encryption solutions.

Network vulnerability testing is performed on a regular basis by Segal personnel, and on a periodic basis by external firms specializing in network security.

Segal smartphones are managed by a mobile device management (MDM) system in accordance with corporate policies. Data on these devices is encrypted. Lost or stolen Segal smartphones are wiped remotely and deactivated.

Segal uses an asset disposal company to destroy hardware and media. Personal computers have fully encrypted hard drives and all hard drives are wiped before disposal.

In addition to tape backup systems, all Segal servers are replicated (near real time) to a secondary location for immediate recovery operations.

Segal desktop and laptop hard drives are encrypted. Segal has implemented a security policy stating that all data sent to third parties on removable media or via electronic transmission must be encrypted using company standard encryption methods or other IT or client or vendor secure systems. Technical controls, including e-mail and web data loss prevention monitoring and filtering solutions have been implemented to detect any potential policy violations.

Segal evaluates and implements various outsourced and cloud-based services as appropriate, including but not limited to, supplemental resources, infrastructure as a service, platform as a service and/or software as a service. Any of these services will use equivalent or improved security protocols to those currently employed by Segal. All service providers will be held to strict security and regulatory standards and an assessment of their security protocols will be conducted both before engagement and on a regular basis going forward.

Physical safeguards

A combination of building personnel, access cards, and/or key locks control access to Segal's facilities. In addition, physical access to any of Segal's network equipment or communications rooms is restricted by access card readers or key locks that limit access to the Information Technology department and other authorized personnel.

Contingency operations processes have been implemented to ensure the restoration of data as defined in the Segal business continuity plan. The Segal business continuity plan calls for recovery of operations at an alternate Segal facility that is subject to and is consistent with Segal's standard security measures including security guards, access cards and/or key locks.

Company security policies dictate that laptop computers be locked to their docking stations or secured in locked cabinets when not in use. Segal workstation hard drives are fully encrypted to prevent data loss in the event of lost or stolen computers.

Third party assessments

Segal engaged a leading compliance, security, privacy and technology risk advisor to perform a HIPAA Security Rule compliance assessment. A favorable HIPAA Security Rule compliance report was delivered in August 2022, summarizing the effectiveness of Segal's security policies, procedures, and controls, including Segal's HIPAA Security Rule policies and information security policies and procedures. The requirements contained in the HIPAA Security Rule are comparable to the security controls contained in NIST 800-53 R4 and other industry standard information security frameworks. Segal will provide supplemental information on its information security program upon request and with applicable agreements in place.

Frequently Asked Questions

Access control

What safeguards has Segal put in place to prevent unauthorized use or disclosure of our data?

Segal's employees, contractors, vendors and clients requiring access to any Segal Group systems are assigned a unique user ID and password that controls network and system access and facilitates security audit information. Users are instructed, via policy and training, that they must never share their passwords with anyone, including the IT Help Desk or other IT department staff. All passwords must meet complexity requirements. Multifactor authentication is implemented across all systems.

Segal will use the minimum necessary principle, which has been established as part of the HIPAA privacy policies, and other policies as appropriate, as the basis for the type and extent of authorized access to PHI, PII, other confidential data and system administrative access. The minimum necessary principle ensures that access controls are in place to ensure that access is limited to the minimum necessary required for the user's job role and job function.

Regular entitlement reviews of network resources are performed in order to ensure access is limited to only those who require it to perform their job responsibilities.

In addition, data loss prevention (DLP) systems are utilized to detect accidental and intentional unauthorized disclosure of sensitive information. Segal also takes reasonable and appropriate steps to review audit and system activity logs of its information systems that create, receive, maintain or transmit PHI, PII, C-PI or other confidential data for any potential security breach.

What access control methods does Segal use to limit access to data centers, and network components?

Administrative controls in information technology are provided to only those that require it to perform their job functions. These controls are provided through a separate and distinct privileged account that is only to be used when performing tasks that require privileged access. The activities of these accounts are regularly monitored.

Physical access to any of Segal's data centers, network equipment, or communications rooms is restricted by access card readers or key locks that limit access to the Information Technology Department and other authorized personnel. Visitors to data center facilities must be signed in and escorted by authorized personnel. Visitor logs are maintained for offices and data centers.

Are employees permitted to access data remotely?

Yes, various remote access methods are available to Segal employees. Security controls in place to protect your data include but are not limited to VPN, multifactor authentication, endpoint detection and response (EDR), access management, monitoring and auditing and DLP.

Multifactor authentication is required for all remote access options.

Does Segal enforce password complexity requirements?

Yes, Segal has implemented password complexity requirements which include minimum password length, maximum password age, minimum password age, and password reuse restrictions.

Does Segal limit the amount of invalid password attempts?

Yes, Segal has implemented technical controls to lock accounts after a certain number of invalid password attempts. Users must contact an administrator and verify their identity to regain access to a locked account.

Actuarial software

Can you describe Segal's approach to the development and maintenance of valuation software?

Segal has built and maintained its own actuarial software in-house for many years – this allows us to customize our deliverables based on the unique needs of our clients. Our dedicated Actuarial Technology and Systems department is comprised of a group of systems developers responsible for providing and supporting the company's state-of-the-art actuarial valuation system. This system has been designed internally to maintain control and flexibility to allow for modifications to best meet the unique needs of our clients.

What actuarial software does Segal use to provide services to clients?

Our actuarial valuation system includes:

- **Segal Data Handler.** Interactive processing of the participant data to generate a unified database that becomes the single source for all actuarial processing needs. Segal is capable of handling client data in a number of formats and on most forms of electronic media (electronic transfer, tape, CD, etc.). To exchange data electronically, we use internet-based methods including file transfer protocol (FTP) and secure file transfer (SFT). Data is imported into the Segal Data Handler, a proprietary Segal database system. The Segal Data Handler is fully customizable to accommodate the unique set of data elements particular to each client.
- **STAR.** A multi-decrement actuarial valuation program that produces a comprehensive set of liability calculations associated with a wide range of benefit plans. The modular structure of

the program allows for improvements to be implemented with a high degree of ease, speed and accuracy.

- **Costs and report generator.** The set of demographic and liability calculations produced by STAR are automatically imported into an integrated costs and report generator program. This program produces actuarial calculations associated with the liabilities to meet regulatory, legislative and client requirements. The results of these calculations are electronically linked to a report generator that creates the valuation report including tables and graphs.
- **Experience study software.** This software aggregates experience over survey period and compiles summary tables and charts comparing expected to actual to recommended data.
- **Actuarial utility programs.** These user-friendly tools are readily available to our actuaries for use in performing various actuarial calculations such as Section 415 limitations, Social Security calculations and generation of annuity values.
- **Asset liability modeling.** Segal's capabilities include our proprietary Forecast dynamic real-time modeling tool that accommodates deterministic projections to increase understanding and facilitate decision-making by allowing plan sponsors to view and assess emerging retirement plan finances. Segal's asset liability modeling (ALM) tool is used for stochastic asset/liability modeling studies to make sound decisions regarding plan assets and liabilities while measuring actuarial funding risks. Segal Pulse is Segal's new, web- based version of our popular Forecast modeling tool that dynamically generates financial and actuarial deterministic projections. For clients who want to explore alternative scenarios hands-on, Segal Pulse is an enhanced, client-driven version of our Forecast tool.

Audit logging and monitoring

Does Segal have policies and procedures in place for collecting and reviewing audit logs?

Segal is committed to taking reasonable and appropriate steps to review audit and system activity logs of its information systems that create, receive, maintain or transmit PHI, PII, C-PI or other confidential data for any potential security breach. Audit and accountability methods include the following:

- Managed security service that has been implemented to complement Segal's auditing, monitoring, analysis and security event correlation capabilities
- Information technology tracking tool and reporting system that record reported security events potentially involving electronic protected health information
- Access management and audit process, which include but are not limited to:
  - Data governance and entitlement management software
  - Access entitlement reviews conducted on at least an annual basis
  - Elevated access privilege reviews that occur on at least a quarterly basis

Awareness and training

What kind of training do the employees who will be working with our data receive?

All Segal employees, contractors and vendors requiring access to PHI, PII, C-PI or other confidential data are required to participate in Information security and compliance training; participation is mandatory. Mandatory training completion is monitored and reported to company management. Segal information security and compliance training also includes phishing and spear phishing simulation campaigns that are conducted on at least a quarterly basis.

In addition to annual information security and compliance training, periodic security awareness and training communications are distributed by the Information Security Department. Ad hoc educational opportunities are also provided through webinars and lunch & learns. New hires, contractors and vendors requiring access to PHI, PII, C-PI or other confidential data must complete information security and compliance training within two weeks of hire.

How often are employees required to receive information security training?

Participation in Segal's information security and compliance training is required within two weeks of hire, and on an annual basis thereafter.

Information security and compliance training content is reviewed and updated on an annual basis.

Business continuity

Does Segal have a business continuity plan?

Yes. Segal has developed a business continuity plan (BCP) which defines roles and responsibilities as well as processes for the recovery and restoration of services in the event of an incident impacting our facilities or systems. Segal conducts an annual review of its BCP to assess effectiveness and make revisions as necessary. The BCP is reviewed annually by National Facilities and Offices Services, the IT Department and appropriate representatives of the business to confirm that all processes are accurate and up to date based on changing business, regulatory, technical and security requirements.

In the event that a Segal office experiences a disaster, power failure or other facility or systems incident, recovery and restoration of services are performed. The IT infrastructure provides for rapid recovery, utilizing replicated systems and remote access capabilities. Once an incident is declared, following the Segal BCP, systems are failed over to the alternate site, making them available immediately, beginning with communication and remote access services followed by the recovery of all business systems.

Does Segal's BCP have a defined recovery time objective (RTO)?

Segal's does have a defined RTO, which prioritizes the restoration of systems critical to providing services to our clients. Segal's BCP is broken into four phases that include the following:

- Phase I – Appraisal
- Phase II – Activation
- Phase III – Recovery
- Phase IV – Restoration

Does your board of directors or senior management provide oversight of the BCP?

Yes. Segal's BCP is reviewed annually by National Facilities and Offices Services, the IT Department and appropriate representatives of the business to confirm that all processes are accurate and up to date based on changing business, regulatory, technical and security requirements.

When was the most recent BCP test performed?

In response to COVID-19, Segal activated its BCP on March 16, 2020, which consisted of transferring the entire organization to 100 percent remote work. This proved the effectiveness and flexibility of our plan to respond to a fluid situation in a rapid fashion. In addition, Segal was able to implement enhancements for application performance, security/protection of critical and confidential data, technology training and dispersal of hardware and equipment to ensure staff were able to meet client deliverables. Segal was able to support all client services as well as internal operations. The activation, testing, and ability for staff to function remotely has been seamless since March 2020.

Cloud storage and services

Does Segal leverage cloud storage or services?

Segal evaluates and implements various outsourced and cloud-based services as appropriate, including but not limited to supplemental resources, infrastructure as a service, platform as a service and/or software as a service. Any of these services will use equivalent or improved security protocols to those currently employed by Segal. All service providers will be held to strict security and regulatory standards and an assessment of their security protocols will be conducted before engagement and on a regular basis going forward.

Will any of our data be stored on the cloud?

Segal does use cloud services and storage, and the technical controls described here are also applicable to data being stored on the cloud.

Cyber liability insurance

Does Segal have cyber liability insurance?

Yes, Segal has a cyber liability insurance p[program. The program contains various sublimits and is designed to respond in the event of a data breach, including covering notification expenses, conduit injury, extortion, electronic vandalism and liability coverage. The policy contains standard exclusions found in many cyber policies, including a retroactive/prior acts date, prior notice, bodily injury and upgrade/improvement costs. However, the coverages and exclusions summarized above should not be considered a binding interpretation of coverage, which is subject to other terms within the policy and specific fact pattern of a given event.

Data retention

What are Segal's data retention policies?

Segal is subject to numerous federal and state laws and contractual obligations that require Segal to retain certain records and documents. Segal has developed a records retention and destruction policy that includes appropriate retention periods for the types of records created, received and maintained by Segal. This policy is consistent and compliant with legal, regulatory and client requirements.

Does Segal have a process to delete our data at the completion of our engagement?

Yes. Segal has established procedures for deleting online copies of the client's ePHI, PII and other confidential data. Segal may retain an archival copy of the client's information in accordance with the contingency plan standard of the Segal HIPAA security rule policy.

Data storage

Where will our data be stored?

Segal leverages colocations in the United States for data center services. The SOC2 compliant industry leading colocation service provides reliability, redundancy, and physical access control and environmental protection systems. Segal also leverages network equipment and communications rooms located at Segal facilities.

How does Segal manage physical assets that store sensitive data?

Segal has implemented formal IT asset management processes related to protecting Segal IT systems and data by managing the IT assets used by the company in a planned, organized and secure fashion. Maintenance and repairs are conducted in accordance with these policies and procedures. These processes include data removal from IT hardware assets and are documented.

Does Segal permit data to be stored on removable media?

Yes. Segal provides employees with encrypted USB drives in the event that they have a business need to transport data via removable media. The use of personal removable media devices is prohibited by policy and enforced through technical controls.

Does Segal have policies and procedures outlining how data is secured on devices that are reused or destroyed?

Yes. Segal has a documented asset destruction policy that details procedures for the secure destruction of all assets, including those that house confidential data.

Disaster recovery

Can you describe Segal's disaster recovery plan?

In the event that a Segal office experiences a disaster, power failure or other facility or systems incident, recovery and restoration of services are performed. The IT infrastructure provides for rapid recovery, utilizing replicated systems and remote access capabilities. Once an incident is declared, following the Segal BCP, systems are failed over to the alternate site, making systems available immediately, beginning with communication systems and remote access services followed by the recovery of all business systems.

Segal replicates and backs up data to alternate storage sites in order to ensure the availability of data in the event of a disaster or incident that impacts the primary data center.

Segal performs nightly backups of server data to guard against data loss due to hardware failure or data corruption. Encrypted tapes are stored offsite at a data archive vendor facility in secured and environmentally controlled environments. Backup integrity checks are performed on a regular basis. Restoration of file servers from backups are performed periodically on a test basis.

Encryption

Will our data be encrypted in transit?

Yes. Segal has implemented processes to ensure that electronically transmitted PHI, PII, C-PI or other confidential data is encrypted using company standard encryption methods that include:

- Secure File Transfer (SFT)
- Transport Layer Security (TLS)

Will our data be encrypted at rest?

Yes. Segal workstation computer hard drives are fully encrypted to prevent data loss in the event of lost or stolen computers.

Segal has migrated critical systems containing PHI, PII, C-PI or other confidential data housed in primary data centers to encrypted SAN. Segal utilizes AES-256 to encrypt your data at rest. All servers and storage devices are housed in secure data centers, equipment or communications rooms protected by physical access controls as an additional safeguard for protecting data at rest. Physical access to any of Segal's network equipment or communications rooms is restricted by access card readers or key locks that limit access to the Information Technology department and other authorized personnel. In addition, physical access to Segal's facilities are protected by a combination of building personnel, access cards and/or key locks.

Segal also evaluates and implements as appropriate, various outsourced and cloud-based services, including infrastructure as a service. All service providers will be held to strict security and regulatory standards, and an assessment of their security protocols will be conducted before engagement, and on a regular basis going forward.

What steps are taken by your staff to ensure the privacy and security of confidential data? What does your organization do to ensure that your staff?

Segal is committed to protecting the confidentiality, integrity and availability of the PHI, PII and other confidential data entrusted to us by our clients. As part of that commitment, and in accordance with Health and Human Services, New York State Department of Financial Services, and other applicable regulations, Segal has adopted HIPAA Security Rule policies, and information security policies, which define administrative, technical, and physical safeguards implemented at Segal. These safeguards and controls are summarized in the attached Segal Information Security Program Summary document.

Security controls in place to protect confidential data include but are not limited to VPN, multifactor authentication, identity management, access management, device trust, monitoring and auditing, web filtering and data loss prevention (DLP), and endpoint detection and response (EDR).

Segal workstation computer hard drives are fully encrypted to prevent data loss in the event of lost or stolen computers. Workstations are standardized with the latest patched versions of the operating systems and standard applications, and malware and intrusion protection. Standardized applications include a hybrid proxy agent which provides additional web filtering capabilities while off-premise. Additional security enhancements include complex passwords, hard disk encryption, encryption of data on removable devices, regularly scheduled system updates, monthly security updates, and a regularly required reboot of all PCs.

Segal has documented and implemented processes and procedures for obtaining authorization for staff member's access to PHI, PII and other confidential data. These processes and procedures are managed by Information Technology, and requests for, and authorization of access is recorded in an Information Technology issue tracking and reporting system. Segal will use its "Minimum Necessary Principle", which has been established as part of Segal's HIPAA and information security policies, and other policies as appropriate, as the basis for the type and extent of authorized access to PHI, PII and other confidential data. Regular entitlement reviews of network resources are performed in order to ensure access is limited to only those who require it to perform their job responsibilities.

Lastly, data loss prevention (DLP) systems are utilized to detect accidental and intentional unauthorized disclosure of sensitive information. Segal also takes reasonable and appropriate steps to review audit and system activity logs of its information systems that create, receive, maintain or transmit PHI, PII, C-PI or other confidential data for any potential security breach.

Will any backups of our data be encrypted?

Yes. Segal replicates and backs up data to alternate storage sites in order to ensure the availability of data in the event of a disaster or incident that impacts the primary data center. Encrypted tapes are stored offsite at a data archive vendor facility in secured and environmentally controlled environments.

Incident response

Does Segal have an incident response plan?

Yes. Segal has implemented electronic and procedural mechanisms to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security violations and other security events. These mechanisms include a formal security event response plan. This plan is tested annually and identifies the roles and responsibilities of all security event response team members, as well as the responsibilities of management and coordination between participating departments. It outlines the appropriate event response procedures that will be undertaken as appropriate in the event of a suspected incident.

The Segal incident response plan includes steps to:

- Respond to detected or reported security and/or privacy events or suspected events
- Identify affected critical systems, policies or practices
- Assess damage and scope of the event
- Control and contain the breach or intrusion
- Collect and document all evidence relating to the event according to established forensic procedures
- Engage additional personnel as necessary for investigation of a given event
- Confer with legal counsel to determine appropriate course of action regarding notification, if appropriate, of clients, law enforcement, etc.
- Provide liaison to proper criminal and legal authorities under the direction of Segal or designee
- Initiate breach notification, if appropriate, by reporting the event to the Office of the Privacy Official
- Implement new, or enhance existing privacy and security controls to prevent a future event
- Document the investigation, mitigation and future prevention activities

The event response policies and procedures are reviewed by a third-party risk assessment team on an annual basis and are updated based on its findings and recommendations.

How soon will Segal notify me in the event of a security incident or breach?

Segal will notify you of any confirmed security incident or data breach as soon as reasonably practicable under the circumstances.

Has Segal ever experienced a data breach?

No. Segal has never experienced a data breach.

Please provide a description as to how your company mitigates phishing attempts.

All Segal employees are required to participate in information security and compliance training; participation is mandatory. Mandatory training completion is monitored and reported to company management. Segal information security and compliance training also includes phishing simulation campaigns, that are conducted on at least a quarterly basis.

In addition to annual information security and compliance, periodic security awareness and training communications are distributed by the Information Security department. New hires, contractors and vendors requiring access to PHI, PII, C-PI or other confidential data must complete information security and compliance training within two weeks of hire.

Segal's Information Security team has created "Segal Tips Toolkit on Phishing" that provides detailed advice for how to avoid fall victim to a phishing campaign. Segal's toolkit on phishing is communicated on a regular basis and provides the following details to mitigate phishing attacks:

- Provide examples of specific phishing attacks
- Red flags to look for in phishing emails
- Steps to take to report a suspicious email
- What to do if you have questions about the legitimacy of an email

Lastly, Segal has implemented electronic and procedural mechanisms to identify and respond to suspected or known phishing campaigns. These mechanisms include but are not limited to the following:

- Identifying a phishing campaign
- Reporting the phishing campaign to the Computer Security Incident Response team (CSIRT)
- Determine the scope of impact
- Notifying impacted users of potential phishing campaign
- Removing phishing emails from inboxes to reduce attack surface
- Escalating users with potential relevant risk for further investigation.

Information Technology & Security Staff

Does Segal have in-house IT staff to support the services you provide?

Yes, Our IT staff is an in-house department of approximately 60 technology and information security professionals, headquartered in New York and on-site in offices across the country. The IT department includes infrastructure, applications, and information security departments. The applications area is organized into development groups responsible for specific business unit applications. Enterprise standards are maintained across all development groups. The infrastructure area is comprised of engineering, operations, help desk and procurement. The Information Security department consists of dedicated information security professionals responsible for the development, implementation, and oversight of companywide information security policies, procedures and programs.

Does Segal have dedicated information security staff?

Yes. Segal has established the role of Chief Information Security Officer, who is responsible for the development, implementation and oversight of company wide information security policies, procedures and programs. Segal also has a team of information security analysts who are responsible for contributing to the previously mentioned responsibilities, including but not limited to DLP event management, information security training for employees handling PHI, PII, C-PI or other confidential data, access management and vendor risk management.

Does Segal have staff dedicated to data governance?

Yes. Segal has established an information security governance structure to uphold information security standards and practices that protect the confidentiality, integrity and availability of data belonging to Segal and its clients and ensure compliance with all applicable regulations and industry standards and obligations.

This structure is made up of members of the Office of the Privacy Official and the Data Security committee. These groups consist of senior members of the company representing Risk Management, Legal, Health Practice, Compliance, Human Resources, IT and the CEO. These groups are responsible for the planning and implementation of security policies, procedures and controls.

Maintenance

Does Segal have a process for applying security patches?

Yes. Security patches are applied to all Segal desktops, laptops, servers, and other infrastructure on a regular basis. Windows security updates as well as application security updates are tested, packaged and deployed to all workstations and Windows servers on a monthly basis. Emergency updates are tested and deployed within days when there are critical

vulnerabilities. Reports are reviewed after the deployment. Unsuccessful installations are remediated based on these reports.

Does Segal have a defined change control process?

Yes. All changes to Segal's production systems require appropriate management approval and are recorded in the Information Technology tracking tool and reporting system consistent with the change management policy.

Changes to the Segal production environment, as well as system maintenance and repair, are recorded in the Information Technology tracking tool and reporting system. Changes to Segal's production systems require appropriate management approval and are recorded in the Information Technology tracking tool and reporting system consistent with our change management policy. Functionality tests are conducted for all key system components, including security controls, after maintenance or repairs are completed.

Does your company run regular malware scans? What is the frequency? How often are malware tools updated?

Yes. Segal runs malware scans in real time.

Additionally, anti-virus signature files are updated at least daily.

Personnel security

Does Segal perform background checks?

Yes. All employees and contractors are subject to a background check before starting employment in the firm. Background checks may include, but are not limited to:

- Confirmation of claimed academic degree(s)
- Confirmation of professional experience and qualifications through employment reference checks
- Validation of claimed professional license(s) (as relevant to the position)
- Criminal background check

Does Segal require employees and contractors to sign confidentiality agreements?

Yes. All employees and contractors are required to read and sign confidentiality and other employment terms.

Does Segal have processes in place to disable access to our data in the event that an employee is terminated?

Yes, Segal has implemented formal termination processes and procedures to revoke access to Segal's network, systems and confidential data. These processes include the following:

- Termination requests are initiated by Human Resources or staff member's manager and executed by the IT help desk.
- Network and system user access is removed upon termination and in certain instances, upon notification of resignation.
- Terminated staff members must return company-issued laptops, smartphones, card keys and other devices.
- BYOD (Bring Your Own Device) and company-issued devices are wiped of all corporate data, remotely wiped when necessary.

Termination requests are managed by the IT help desk and recorded and tracked through completion in the Information Technology issue tracking and reporting system.

Physical and environmental protection

What physical security controls are in place at Segal locations where data is stored and processed?

A combination of building personnel, access cards and/or key locks are required to access Segal's facilities. In addition, physical access to any of Segal's network equipment or communications rooms is restricted by access card readers or key locks that limit access to the Information technology department and other authorized personnel.

Visitors to Segal facilities are required to check in with security or an authorized Segal representative. Visitors to data center facilities must be signed in and escorted by authorized personnel. Visitor logs are maintained for offices and data centers.

Segal security policy instructs all staff to maintain the physical security of data within the office by adhering to best practices which include, but are not limited to:

- Locking workstations when not in use
- Utilizing secure printing functions when printing confidential data
- Securing printed copies of confidential data
- Preventing tailgating into secure office space

Does Segal have environmental controls in place in its data centers?

Yes. Segal data centers, network equipment, and communications rooms are equipped with environmental controls which include but are not limited to fire detection and suppression, water detection and mechanisms to monitor and maintain temperature and humidity level.

Risk assessment

Does Segal perform risk assessments of its critical systems and infrastructure?

Yes. Segal continuously assesses potential risks to PHI, PII, C-PI or other confidential data, and evaluates the effectiveness of implemented mitigating controls. Segal's HIPAA Security Rule policies document outlines the policies and procedures for periodic risk assessments and analysis.

In addition, third parties are engaged periodically to conduct risk assessments, risk analysis, and vulnerability and penetration testing to identify and evaluate security risks and vulnerabilities and effectiveness of existing mitigating controls.

Results of periodic internal practice-level audits, general controls audits and penetration testing are evaluated and incorporated into the risk assessment process where applicable. Items identified for remediation are tracked in the information technology tracking tool and reporting system and are prioritized appropriately.

Results and findings of risk assessments, risk analysis, vulnerability and penetration tests are reviewed by Segal's information security governance bodies and other personnel as appropriate.

How often do application security tests occur?

Segal performs vulnerability scans on at least a bi-annual basis. However, there is an effort to do a web application based-scan every month for externally facing applications.

Security assessment

Can Segal provide a SOC report, SSAE audit, or other third-party audit report?

Segal does not have requirements for a SOC or SSAE audit. Segal does, however, have an information security program, including information security policies and procedures, which are independently audited by third parties. A leading compliance, security, privacy and technology risk advisor delivered a favorable HIPAA Security Rule compliance report in August 2022, summarizing the effectiveness of Segal’s security policies, procedures and controls, including Segal’s HIPAA Security Rule policies and information security policies and procedures. The requirements contained in HIPAA’s Security Rule are comparable to the security controls contained in NIST 800-53 R4 and other industry standard information security frameworks.

Technical architecture

Can you briefly describe the Segal systems environment?

Segal operates a software-defined wide area network (SD-WAN) comprised of redundant links that are a combination of both MPLS and internet-based circuits. Our hub offices host critical data for our organization. Such data is protected behind virtual firewalls, physical firewalls and in some cases access lists for true segmentation. Depending on the type of data, we enforce more than one form of authentication and log all pertinent traffic. Ports and access points are controlled and secured by a Network Access Control solution. The traffic traversing through them is encrypted which allows all office's local area networks (LAN) to connect to one another in a secured manner. File server standards and storage area networks (SAN) ensure fault tolerance to minimize downtime. All application software processing occurs on Microsoft Windows computers using the most current Windows operating system.

As technology and services evolve, Segal will evaluate and implement as appropriate various cloud-based services, including but not limited to, infrastructure as a service, platform as a service and/or software as a service. Any cloud service implementations will utilize equivalent or improved security protocols to those currently employed by Segal. All cloud service providers will be held to strict security and regulatory standards and an assessment of their security protocols will be conducted before engagement, as well as on a regular basis going forward.

Can you briefly describe the hardware that employees will use to perform services?

All computers feature the latest version of Segal standard software. The hardware and processors provide optimal performance and enhanced security features including anti-malware and intrusion prevention. Additional security enhancements include complex passwords, hard disk encryption, encryption of data on removable devices, regularly scheduled PC updates, monthly security updates and required reboots of all PCs.

Do you support Bring Your Own Device (BYOD)?

Yes. Segal supports BYOD in accordance with our BYOD policy, which defines approved devices and requirements for the installation of mobile device management (MDM) software on the device.

Third party and vendor risk management

Does Segal have a process to ensure that any vendors or other third parties who will have access to our data have been appropriately vetted?

Yes. When entering into an agreement with vendors or subcontractors, Segal will perform due diligence in selecting third party service providers in support of services provided to Segal and/or clients. Due diligence includes but is not limited to a background check of the service

provider and personnel, evaluating length of time in business and financial standing, and requiring completion of a security questionnaire, as well as a contractual agreement to comply with related Segal policies and procedures.

All vendors, contractors and other members of Segal's extended workforce that require greater than incidental access to confidential information are required to enter into any applicable and appropriate agreements including but not limited to business associate agreements (BAA), confidentiality agreements, non-disclosure agreements (NDA), data use agreements (DUA), etc.

Is a risk management program/policy in place, maintained, and approved by senior management?

Yes. Segal's risk management policy is reviewed, updated and approved by senior management at least annually, as well as periodically throughout the year.

Additional questions

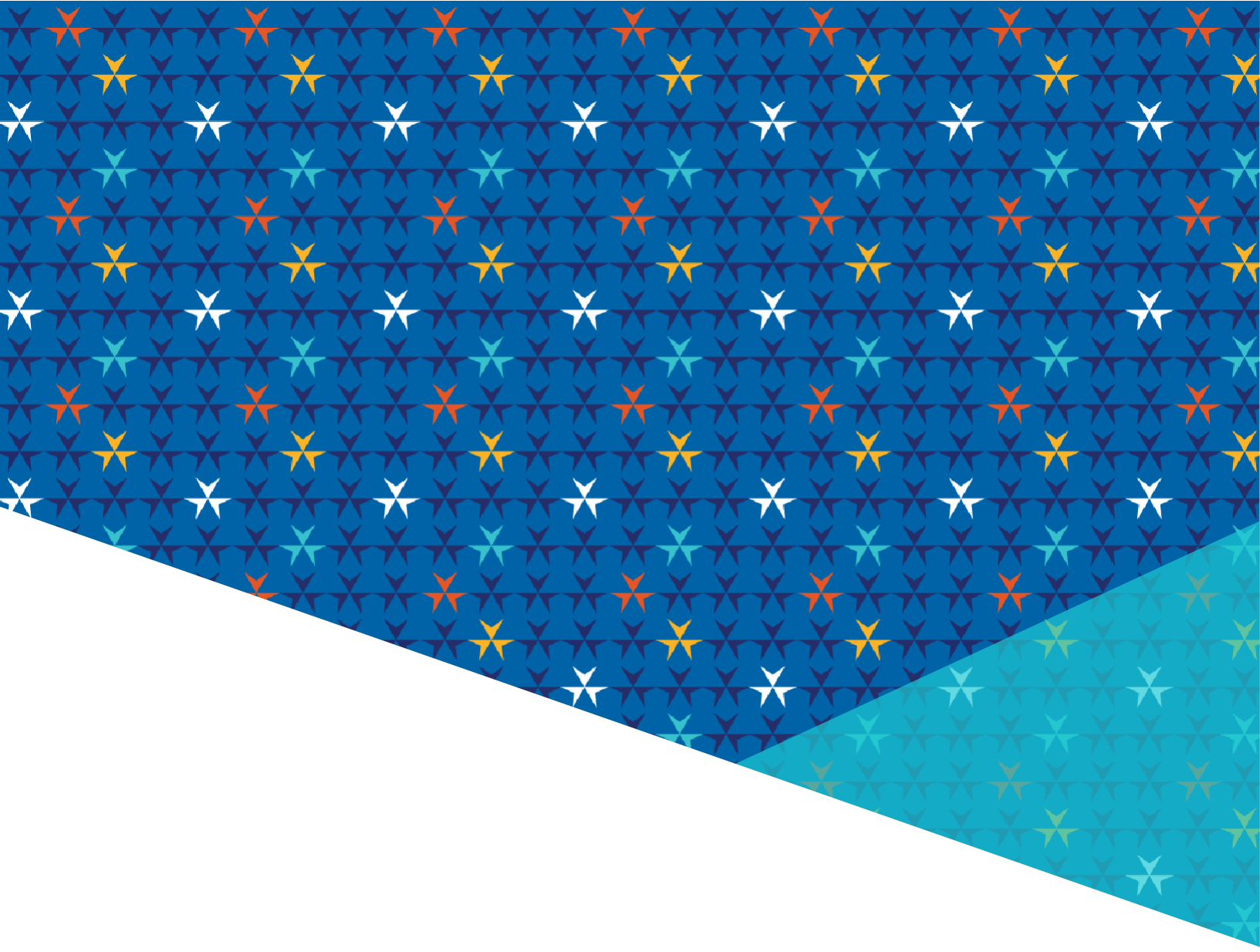
We have a question that was not answered here; who can we speak to?

If you have additional questions that have not been answered in this document, or would like to request additional information, please reach out to your CRM, who can connect you with Segal's Chief Information Security Officer.

Appendix – Policy Excerpts

Please find below excerpts of the following policies, procedures, and audit reports:

- Segal Information Security Policies and Procedures
- Segal HIPAA Security Rule Policies
- Segal HIPAA Security Assessment Summary Report
- Segal Business Continuity Plan
- Segal Data Access Management Policy
- Segal Data Classification and Handling Guidelines
- Segal Data Security and Sanctions Policy
- Segal Marketing Materials — How will Segal Secure your Data?



Segal

Information Security Policies and Procedures

2022

Table of Contents

Information Security Policies and Procedures - 2022

Segal

HIPAA Security Rule Policies

2022

Table of Contents

levelUP CONSULTING GROUP

HIPAA Security Alignment Memo

LevelUP Consulting Partners

Created for Segal

August 2022

Introduction

Segal is a benefits and human resources, consulting firm for multiemployer funds, public sector organizations and the private sector. Other services that Segal offers include investment advisory, commercial insurance and brokerage services, and HR and Benefits Technology consulting. These services involve the collection, processing, and storage of data including electronic Protected Health Information (ePHI) which can classify Segal as an organization acting in the capacity of a Business Associate and as such, subject to the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

As part of its ongoing compliance efforts, Segal engaged a third party, LevelUP Consulting Partners ("LevelUP"), to review their alignment with the HIPAA Security Rule requirements. LevelUP brings years of experiences with deep expertise across a broad spectrum of services focused on assisting organizations evaluate, enhance, build, and maintain HIPAA compliance programs. These experiences have led to the development of a robust set of methodologies and standards that are used throughout the delivery of our services. To ensure continued alignment with changing regulatory and industry standards, LevelUP continually enhances its methodologies including evaluating and implementing guidance issued by the Office for Civil Rights ("OCR").

Scope

LevelUP performed an independent assessment of Segal's alignment to the HIPAA Security and Breach Rule requirements. The assessment included an in-depth analysis of Segal's physical, technical, and administrative controls, the related documented policies, procedures, and operational practices required by the HIPAA Security and Breach Rules. To ensure accuracy and completeness, the assessment techniques included: (1) a detailed review of documentation including, policies, procedures, system documentation, and (2) discovery and interview sessions with Segal subject matter experts in information security, human resources, and other business lines relevant to the requirements of the HIPAA Security Rule. LevelUP's comprehensive assessment and risk analysis of Segal's environment was performed in May, June, and July of 2022.

In alignment with the detailed guidance provided by OCR, LevelUP performed an extensive evaluation of the technical controls and administrative safeguards for the systems that collect, process, and store ePHI. This included but was not limited to the Segal Health Analysis of Plan Experience (SHAPE) application (formerly known as the Health Data Warehouse application), which had technical safeguards operating consistent with HIPAA Security Rule requirements.

Conclusion

LevelUP determined that Segal's administrative, technical, and physical controls and safeguards are aligned to the HIPAA Security and Breach Rule requirements for protecting ePHI. LevelUP also noted Segal's commitment to evolve the information security program which has been maintained and further strengthened for alignment to the Security and Breach Rule standards. Segal has demonstrated their commitment to establishing and maintaining compliance with the HIPAA Security and Breach Rule standards and as such, have a high level of maturity in its information security program relevant to the disciplines represented across the Security and Breach Rules. While the focus of the assessment activities was on systems containing ePHI, Segal has asserted and demonstrated that it has extended its information security program beyond ePHI to include all individually identifiable information, and other confidential data. As such, Segal noted the same policies, procedures, and safeguards that are implemented for systems containing ePHI, are also implemented for other confidential data collected, processed, or stored by Segal. In addition, many of the requirements contained in the HIPAA Security Rule are comparable to the security controls reviewed as part of a SOC 2 audit, those contained in NIST 800-53 R4, and other industry standard information security frameworks and regulations including but not limited to NYS DFS Cybersecurity Regulation (23 NYCRR 500). Segal was responsive and helpful throughout the assessment. LevelUP completed the assessment successfully including presenting final results to the Segal leadership team.

By: Eric Dieterich

Name: Eric Dieterich

Title: Managing Partner

Date: August 15, 2022

Segal

Data Access Management Policy

July 2022

Table of Contents

Segal

Data Security and Sanctions Policy

July 2022

Table of Contents

Segal

Data Classification and Handling Guidelines

2022

Table of Contents

Still Have Questions?

If you have additional questions that have not been answered in this document, or would like to request additional information, please reach out to your CRM, who can connect you with Segal's Chief Information Security Officer.