**Pennsylvania**

**CYBERSECURITY POLICY**

**FOR [insert Agency Name]**

LAST UPDATED [insert Date]

**NOTES**

* This cybersecurity policy is mandated for all agencies holding a resident or non-resident license in Pennsylvania and having **at least** **10** **employees,** $5 million in gross revenue AND $10 million in year-end assets; *Individual* *licensees* (producers) are exempt from the Information Security Program (ISP) requirement if they are covered by their agency’s (employer’s) ISP.
* Agencies with fewer than 10 employees, less than $5 million in gross revenue OR less than $10 million in year-end assets are not required to develop, implement and maintain the Information Security Program described here (§4513 of the Pennsylvania Data Security Law). However, these agencies should have one in order to comply with other federal and state requirements, including the Gramm-Leach-Bliley Act and corresponding state regulation, and as a best practice.[[1]](#footnote-1)
* Agencies subject to the Health Insurance Portability and Accountability Act (HIPAA) and that have developed an Information Security Program compliant with HIPAA are deemed compliant IF they treat nonpublic information the same way they treat Protected Health Information (PHI). If that is the case, they are not required to develop, implement and maintain a *separate* Information Security Program as described here (§4513)**1**.
* Other sections of the law, including investigation and notification of a cybersecurity event do apply to ALL AGENCIES, regardless of staff size,­ under §4517 and §4518 of the [Pennsylvania Insurance Data Security Act](https://www.legis.state.pa.us/cfdocs/Legis/LI/uconsCheck.cfm?txtType=HTM&yr=2023&sessInd=0&smthLwInd=0&act=2).
* Upon completion, and prior to official implementation, the agency’s Cybersecurity Policy should be reviewed with agency personnel.
* If an ISP is required, it must designate a Chief Information Security Officer or Information Security Manager for the agency, in accordance with Section 15 of this Cybersecurity Policy.
* Upon completion of the agency’s Cybersecurity Policy, protocols should be established for purposes of appropriately conducting all reviews and/or inventories as provided for in Sections 1, 3, and 4, and Section 15, if applicable.
* After initial adoption and review, any and all substantive modifications to the Cybersecurity Policy which affect and/or are applicable to agency personnel should be reviewed with agency personnel prior to implementation.
* Language in RED in subsequent pages should be deleted and not included as part of your final Cybersecurity Policy.
* Green highlights herein refer to a secondary document or record that should be developed to address the referenced requirement.

**INTRODUCTION**

This Cybersecurity policy was developed to comply with the Pennsylvania Insurance Data Security Law set forth at Title 40 of the Pennsylvania Consolidated Statutes, Chapter 45, specifically §4513 (see Appendix), and incorporates the different components required by the law.

**Employee applicability -** It is the intent of this policy to cover all employees of the agency, and **all employees are required to comply with all aspects of this information security Policy**. Employees have been instructed that failure to comply with this information security Policy could:

* lead them to be found in violation of the agency’s procedures and subject to disciplinary action,
* expose them to their own liability under the Law, including the obligation to file an individual Information Security Policy (see 40 Pa. C.S. §4532(c)).
1. **Information Security**

Our Information Security policy was developed after conducting a risk assessment to:

* identify reasonably foreseeable internal and external threats to the security, confidentiality and/or integrity of the agency’s records containing private information,
* assess these threats and our existing procedures, taking into account the type and nature of the information,
* implement physical, administrative, and technical safeguards to minimize risks,
* implement a monitoring program to regularly assess the effectiveness of our policy and safeguards.

In developing this policy, the agency has focused on our customers’ Non-Public Information (NPI) as defined in the law, including:

* access,
* collection,
* storage,
* use,
* transmission,
* destruction, and
* overall protection,

when the information is used by the agency staff and when it is accessed by third parties who have been authorized to do so by the agency in order to provide services to the agency. Such access will be granted in compliance with the requirements of the law.

This Information Security Policy shall be reviewed periodically and reevaluated [insert timetable, e.g. annually], or sooner, to address changes in the agency’s information systems, NPI or business operations &/or changes to applicable laws or regulations. The agency may also amend this policy at any time.

1. **Risk assessment**
* An employee has been designated to manage and oversee this Information Security Program (see Section 3)
* A risk assessment to identify foreseeable internal and external threats was conducted to develop this Cybersecurity Policy.
* The risk assessment is reevaluated periodically, and whenever changes occur to the agency’s information systems, business operations or nature of the nonpublic information held.
* The effectiveness and sufficiency of the existing safeguards are reassessed annually, including employee training and management.
* This Cybersecurity Policy is and will be updated following reevaluation of the risk assessment, when necessary.
1. **Chief Information Security Officer/ Information Security Manager**

*[When establishing an Information Security Program, agencies must designate one or more employees, an affiliate or outside vendor (IT or cybersecurity provider) to be responsible for managing and overseeing the Information Security Program. Agencies with a Board of Directors need to exercise oversight of the Third Party Service Provider, and remain responsible for compliance, and a senior staff member of the agency should be designated to direct and oversee the Third Party Service Provider.]*

* The agency does not have a Board of Directors - [Insert name] will act in the capacity of Information Security Manager for the agency, and coordinate and supervise implementation of the Information Security Program and cybersecurity policy.
* The agency has a Board of Directors - [Insert name] has been designated as the agency’s Chief Information Security Officer (CISO)/Information Security Manager. In this capacity, he [she] will be responsible for developing, implementing and maintaining the agency’s Information Security Program, including providing an annual report to the Board as required under 40 Pa C.S.A. §4514. If any functions are outsourced and deal with risk assessment, the ISP itself or oversight of third-party providers, the outsourced entity will provide a written report to the executive management.
1. **Data Governance & Classification**

Non-Public Information (NPI) will be treated as confidential information by the agency and its staff, and will only be shared as necessary to process the transactions in the ordinary course of business and within the safeguards built to protect that information.

NPI includes, but is not limited to, first name or initial and last name, in combination with any of the following:

1. Social Security number
2. Driver's license number, or non-driver identification card number
3. Financial account number, or credit or debit card number
4. A security code, access code, or password that would permit access to the consumer’s financial account
5. Biometric records
6. Personal or protected health information, or information relative to the provision of healthcare to the individual, including payment

NPI also includes the agency’s or another licensed entity’s sensitive business-related information.

Even if not connected with a first name/initial and last name, other data may be handled as confidential as stated above, in compliance with the agency’s policies & procedures.

Any doubt as to whether information should be shared will be referred to the Chief Information Security Officer or the Information Security Manager, as applicable, for determination.

1. **Asset inventory and device management**

An inventory of all devices and equipment containing, or which have the capacity to contain NPI has been completed, and will be updated regularly, and no less than annually. This inventory includes all data processing equipment such as desktops and laptops, but also equipment that may “passively” retain data on their hard drives such as printers, copiers and faxes, and mobile devices used for business.

1. Employees have been instructed:
	1. to keep their mobile devices secured at all times,
	2. only to use their mobile devices (including PDAs, smart phones, etc.) with access to NPI in secured locations and on secured networks; in other words, employees may not access public networks and wi-fi when using their mobile devices that either contain or have access to NPI.
2. Mobile electronic devices must be password-protected. Employees have been instructed not to share passwords or other access information with others.
3. Employees are prohibited from loading agency/customer data on thumb drives, laptops or other portable media, drives and devices unless authorized to do so by the agency. If the employee is authorized, the data files transferred to the device must be password-protected and encrypted, and the mobile devices/laptops must be password-protected and encrypted.
4. All terminated employees must:
	1. return to the agency all agency proprietary information, including all NPI, however and wherever that information is kept (hard copy or electronic copy) before leaving employment;
	2. return any and all keys, access codes, fobs and/or IDs and badges; and
	3. not access any NPI (including, but not limited to, any private information).
5. The terminated employee’s email and voice mail accounts will be immediately disabled and transferred to another agency staff member until a replacement for the terminated employee has been hired, as applicable.
6. The terminated employee’s access codes to all agency systems as well as all carrier and vendor systems will be immediately disabled, and carriers and vendors will be notified that the employee has been terminated.
7. All employees are required to report all actual or potential unauthorized access to, use of or disclosure of NPI to the Chief Information Security Officer or the Information Security Manager, as applicable. All employees are instructed and trained to remain alert to suspicious activity.
8. **Access controls and identity management**

The following controls have been adopted for the agency:

1. Access to the agency’s information systems is limited to agency authorized individuals only. The list of authorized individuals will be reassessed and confirmed periodically, and no less than annually.
2. Access to the agency’s systems will require login information in the form of a user ID and a password. The agency protocol is to establish strong passwords combining upper-case and lower-case letters, numbers and special characters. It may include other multi-factor authentication methods, as appropriate.
3. Employees must never share passwords or access codes with others.
4. Systems are designed to generate password changes/updates periodically.
5. Visitors’ wireless access, if any, will be separated (with a firewall) from the agency’s network.
6. Employees must lock their computer screens and mobile devices when not in use (such as when headed out to a meeting or lunch). In addition, the device should be set to automatically lock after 10 minutes of inactivity.
7. Employees may not download any software or applications without first clearing the download with the IT Manager, Chief Information Security Officer, Information Security Manager or agency principal.
8. Employees should not open any email attachment, link, or application if the employee does not reasonably believe the information originated from a trustworthy source.
9. Due to the increasing number of phishing and other fraudulent practices, employees are expected to be prudent in their handling of emails. Any unusual instructions, including the wiring of funds, should be questioned with a supervisor, the Chief Information Security Officer or Information Security Manager (as applicable), or the agency principal directly.
10. *[If the agency uses credit card payments]* The agency will retain only the last four digits of credit card numbers and will not retain bank routing numbers, personal bank account numbers and checks. All credit- and banking-related information that is not kept by the agency will be destroyed in accordance with applicable law and agency business practices.
11. Any servers and equipment housing NPI and located on the agency’s premises will be held securely.
12. Terminated employees’ access codes will be immediately disabled, as described in Section (3) above regarding device management.
13. **Business continuity and disaster recovery planning and resources**

**Definitions**:

A Cybersecurity Event is defined as “an event resulting in unauthorized access to, disruption of or misuse of an Information System or nonpublic information stored on the Information System.”

Information System means “(1) a discrete set of information resources that is stored in an electronic system and is organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic nonpublic information, (2) any specialized system such as an industrial or process control system, telephone switching and private branch exchange system or an environmental control system.” For purposes of this Cybersecurity Policy, Information System includes the agency management system, software, and electronic processes used by the agency.

**In case of a cybersecurity event:**

If an employee discovers **or suspects** that a Cybersecurity Event has occurred or is occurring, that employee must immediately report the incident to the Chief Information Security Officer or the Information Security Manager, as applicable. This reporting should be treated with the highest level of priority. If the Chief Information Security Officer is not present, the agency principal &/or agency manager must be notified, as well as any other designated person, as applicable.

The following steps will be followed by the agency:

1. Report the Cybersecurity Event to the Chief Information Security Officer or the Information Security Manager immediately
2. Contact the IT provider in charge of Cybersecurity to immediately contain the exposure and mitigate the breach, as applicable
3. Assess the nature and scope of the Cybersecurity Event
4. Consult with Counsel/ Contact the agency’s Cyber insurance policy carrier (as applicable)
5. Depending on the assistance provided by 4. above (Cyber/data breach insurer or Legal Counsel), the federal and state legal and regulatory requirements regarding proper data breach notification**[[2]](#footnote-2)** will be reviewed, and the agency will do the following, as applicable:
	1. Notify legal and regulatory authorities within the time frame allotted (5 business days to notify the PA Insurance Commissioner),
	2. Notify each affected carrier in accordance with the law and the provisions set forth in that carrier’s agency contract,
	3. Notify affected policyholders/consumers affected by the Cybersecurity Event, unless the authorities request you to delay notification during the investigation,
	4. Notify the media (if and as required),
	5. For all notifications above, the agency will consider the state where the individual whose information may have been accessed is located and comply with that state’s statute.
6. Continue the investigation, and correct any issue identified.
7. Upon closure of the Event, assess procedures with staff and review any changes implemented as a result.
8. Update this Cybersecurity Policy, as applicable, and advise all employees regarding applicable updates/revisions.

Step 1 above is applicable to all employees.

Steps 2 to 8 above are the responsibility of the Chief Information Security Officer or the Information Security Manager, as applicable.

1. **Systems operations and availability concerns**
* Our internal policy requires utilization of passwords that are difficult to guess. Employees' passwords must be between six and eight characters and include at least one lower-case letter, one upper-case letter, and one number. Employees are required to change passwords regularly every [insert number, preferably no less than every 90 days] days.
* Employees are instructed not to leave their passwords in a visible location and never to share their passwords.
* Individuals no longer employed by the agency shall be removed from having system access immediately upon termination.
* Employees have been trained and are instructed to exercise caution if they receive suspicious emails.
* Employees are instructed to limit the transmission of NPI via email to necessary transmissions only, and to do so using secure email procedures established for the agency [such as Transport Layer Security (TLS) or other dedicated encryption software]
* Employees are instructed not to disseminate, communicate or store NPI on/through any social media platform or unsecured web services.
* Any employees accessing agency systems remotely will do so using a secure connection (such as via a Virtual Private Network)
* Employees should not access agency systems or NPI using non-agency equipment (e.g., a home computer) unless the agency has established such access will meet the security requirements of the agency and has authorized the employee to proceed.
* Employees are prohibited from retaining any NPI on non-agency equipment.
* The agency has a record retention schedule that governs the destruction of records. When the schedule calls for the destruction of records, any paper or electronic records containing NPI must be destroyed so that these records cannot be read or reconstructed (following the recommendations spelled out in the Disposal Rule[[3]](#footnote-3)). This means:
* shredding, burning or pulverizing papers
	+ destroying or erasing electronic files (wiping, not just deleting, in order to avoid risks of recapture of the information). This method will be used before discarding office computer equipment but also all replication devices such as copiers, printers, scanners and faxes that contain a hard drive that must be fully wiped/erased
	+ conducting due diligence and hiring a document destruction contractor to dispose of consumer report information in a manner consistent with the Disposal Rule [ [access more information on proper due diligence in hiring a commercial shredding contractor](https://issuu.com/primary_agent/docs/july-2023/s/27142629) ]
1. **Systems and network security**
* The agency uses various hardware and software solutions to protect agency systems from penetration and malware. These solutions have been developed and are regularly reassessed with the agency’s Chief Information Security Officer or Information Security Manager (as applicable), Information Technology (IT) staff and/or outside IT provider.
* These software solutions are kept up-to-date (with set automatic updates), and patches are applied following system recommendations or recommendations made by our IT provider, and include:
	+ An email filter, and virus, spyware and malware protection on its systems and servers, and on its desktop and laptop computers, PDAs and mobile devices as applicable.
	+ Network and firewall protection
* Information processed is backed up at least daily, and backups kept off-site in a secure location. Backups are password-protected and encrypted.
* If/when the agency’s website collects customer information, such information is collected on a secured web page using Secure Sockets Layer (SSL) technology. Such SSL technology will be activated before the consumer enters his or her password and/or any NPI.
1. **Systems and network monitoring**
* The agency monitors its systems and equipment to promptly identify any attempt at malicious intrusion or unauthorized access to the agency’s system, &/or misuse of information stored on the agency’s system.
* Such monitoring includes activity-log reports.
* If a cybersecurity event is detected, Section (5) above on Business Continuity and Disaster Recovery will be triggered, and will include notifying affected parties as required by law
* The agency exercises due diligence in selecting Third-Party Service Providers that must be provided access to NPI to provide their services to the agency. Such service providers must provide the agency with appropriate assurances and confirmation that requisite security controls are in place and agree in writing **[[4]](#footnote-4)** to safeguard and store NPI with at least the same level of security controls as the agency maintains (as outlined in this policy). The service provider must also agree to notify **[[5]](#footnote-5)** the agency following discovery of any real or suspected breach of NPI while being held by the service provider, and follow any other requirements set in applicable federal &/or state law.

If these provisions are not currently included in the contract with the TPSP, an agreement should be executed separately.

1. **Systems and application development and quality assurance**
* The agency does not currently develop its own system applications [as applicable]
* Any purchase of systems software or applications is subject to a review of the product characteristics and information security features (through our IT Department or third-party IT provider).
1. **Physical security and environmental controls**

General premises security

* If applicable, the premises has a burglar/intrusion alarm system which, at minimum, is activated after normal working hours.
* All access points to the premises are adequately secured by locks or locking devices.
* Our internal policy outlines which individuals have keys to the premises.
* We have a policy against the duplication of keys.
* We have a policy to secure keys immediately from terminated employees.
* Our premises is sufficiently lit at night.

Visitor Policy and Reception Area

* Visitors are greeted immediately upon entry to the premises.
* Visitors are required to sign in and/or wear a visitor’s badge.
* Visitors will be escorted by agency personnel while on office premises.

Access to Agency Files & Hardware

* Physical access to NPI is restricted to authorized individuals only.
* Records are stored in protected or controlled areas.
* Filing cabinets containing NPI are locked after working hours.
* Our internal policy requires employees not to leave consumer/customer information open to public view.
* Employees are required to follow security procedures if they are permitted to remove files from the premises.
* Employees are instructed to lock their desks after working hours if the desks contain customer files &/or NPI.
* The agency's server is located in a protected or controlled area.
* Employees must keep their computer screens turned away from visitors unless the information shown relates to such visitors.
1. **Customer data privacy**

Existing IA&B resources are available to members

* The agency’s Employee Manual outlines/reiterates procedures regarding the privacy of customer and consumer information.
* The agency’s electronic mail policy precludes the use of email and other information systems in a way that may violate confidentiality of customer/consumer information.
* When in doubt about the security of the transmission, staff must consult with the Chief Information Security Officer or a supervisor before transmitting the agency’s confidential and/or proprietary information over the internet.
* All staff must sign a non-disclosure of confidential information that includes customer information.
* Disclosure of confidential agency, client, policyholder or personnel information to unauthorized persons may result in disciplinary action, up to and including discharge.
1. **Vendor and Third Party Service Provider management**

*For purposes of this Cybersecurity policy, a Third-Party Service Provider (TPSP) means a Person that contracts with the agency to maintain, process or store, or is otherwise permitted to access, Nonpublic Information through its provision of services to the agency.*

As part of the management of Third Party Service Providers, the agency will:

(1) Identify TPSPs who need and have access to NPI in the process of providing services to the agency (including our agency management system provider, IT provider, etc.)

(2) Establish minimum cybersecurity practices that the TPSP will be required to meet prior to doing business with the agency;

(3) Use due diligence when selecting the TPSP and seek information to evaluate the TPSP’s cybersecurity practices; and

(4) Conduct a risk assessment, initially and periodically, focused on the relationship with the TPSP. The agency will document:

* The identification of potential cybersecurity risks specific to the relationship
* The TPSP’s response to these risks
* The agency’s decision regarding doing or continuing to do business with the TPSP based on the risk assessment.

The agency will require that the TPSP implement appropriate administrative, technical and physical measures to protect and secure the Information System and Nonpublic Information to which the TPSP has access or holds. The following guidelines will be incorporated in the review of the services &/or in the written agreement with the TPSP as part of the agency’s due diligence process:

(1) The TPSP’s procedures regarding access control to the agency’s NPI, including multi-factor authentication &/or limiting access to those TPSP individuals who have a legitimate business need to have such access; the TPSP will use access control methods appropriate for the size and complexity of the agency and the sensitivity of the information to be protected;

The agency has 5 business days to notify the commissioner. It may wish to reduce the time for the TPSP to notify the agency.

(2) The TPSP’s procedures regarding encryption of the agency’s NPI when in transit and when at rest will be provided to the agency;

(3) The TPSP must agree to notify the agency as soon as possible, and no later than 72 hours after discovering a Cybersecurity Event directly impacting the agency’s Information Systems or NPI held by the TPSP;

(4) Proper documentation by the TPSP regarding the cybersecurity policies and procedures implemented by the TPSP regarding:

* the security of the agency’s Information Systems or Nonpublic Information, and/or
* the TPSP’s compliance with any of the following standards:
	+ **40 Pa C.S. §4501 et seq.** (Pennsylvania’s Insurance Data Security law) **or 23 NYCRR 500** (New York State Cybersecurity Requirements for Financial Services Companies)
	+ **ISO/IEC 27000 Family of Standards** (International Organization for Standardization systematic approach to managing and securing sensitive company information)
	+ **SOC2/3 and/or SOC for Cybersecurity** (Service Organizations Controls for Certified Professional Accountants)
	+ **NIST 7621r1** (National Institute of Standards and Technology - Small Business Information Security: The Fundamentals)
	+ **NIST CSF** (NIST Cyber Security Framework)
	+ **OWASP** (Open Web Application Security Project)
	+ **GDPR** (European Union General Data Protection Regulation)
1. **Incident response**

In case of a Cybersecurity Event (“Event”), the following steps will be taken:

* The Chief Information Security Officer (CISO) or individual acting in that capacity, and the agency principal if a different person, must be notified immediately if an Event has occurred or is suspected to have occurred. In their absence, the most senior staff in the agency must be notified.
* The agency will determine if any and to what extent any personal, nonpublic information about policyholders or employees has been stolen or accessed by unauthorized parties. The agency will also determine if sensitive business-related information or the functionality of the agency’s information system were compromised.
* The first goal of the incident response plan is to stop any intrusion, mitigate any damage, ensure the business can continue to function safely, and comply with all legal and regulatory obligations.
* If NPI was accessed by an unauthorized party the agency will continue with the following steps
* If the agency does not have an in-force cyber insurance policy, the agency will do the following tasks. By default, such tasks will be handled by the CISO or individual acting in that capacity, but can be delegated to other staff members, as needed:
	1. contact an attorney knowledgeable about privacy laws to determine the agency’s obligations and next steps,
	2. notify the carrier(s) affected by the breach within the timeframe allotted in the agency contract,
	3. notify the regulator within the timeframe allotted for each state affected (if PA: within 5 business days of discovering a cybersecurity event (if the “event” involves NPI and is reasonably likely to materially harm a Pennsylvania consumer or the agency, or if the event involves 250 or more customers),
	4. notify law enforcement, as required and within the timeframe defined under applicable law/regulation,
	5. notify the affected individuals of the breach or possible theft of their information, and suggest steps they might consider to safeguard against the misuse of their information,
	6. consider notifying the agency’s professional liability (E&O) carrier.
* If the agency has an in-force cyber insurance policy, the agency will first contact its cyber insurance carrier to report the incident and address “next steps” 1) through 6) listed directly above with the assistance of the cyber insurer,
* The cause of the breach will be investigated. If the breach resulted from the compromise of the agency’s hardware or software, such hardware and software will be isolated by disconnecting it from the network and the rest of the agency’s systems, as well as from the internet.
* The agency will work with its security and IT professionals (and/or those assigned by the cyber insurer) to mitigate any remaining risks and remedy any weaknesses in the agency’s systems and prevent further incidents or a spread of the breach.  Any infected files and/or other identifiable cause(s) of the problem will be removed or fully quarantined. Security software vendors will be notified if it is believed the breach is exploiting a new vulnerability of which they should be made aware.
* If the security breach resulted from actions taken by unauthorized employees or third parties, appropriate and/or corrective measures will be taken immediately, including meeting and training with staff, up to disciplining the employees in accordance with the agency’s personnel manual and policies.
* The agency’s business partners (carriers, vendors, etc.) will be notified of the security breach in situations where the breach occurred through the use of their facilities or services, or in cases in which they may have been or may, in the future, be impacted by the breach, or as contractually required (see above).  This notification will enable business partners to safeguard their systems, limit access or take other necessary protective and corrective actions.
* The agency, along with its IT professionals, will determine and implement the appropriate monitoring processes and procedures in an effort to prevent a recurrence of the security breach.  This will include a review of the existing processes to see where they failed. Staff will be trained in any new processes and procedures and in the nature of the security risks they are designed to prevent, and written policies and procedures will be updated to reflect these changes.
* Once the cause of the security breach has been removed or addressed, and corrective or preventive measures have been put in place, the isolated software and equipment will be first tested then brought back into operation.
* This incident response plan will also be reevaluated and updated as needed.
* If warranted (depending on the nature of the breach), the agency will decide whether to call for an independent security audit of the agency by an outside security professional.

**IMPORTANT NOTE**

[Check box if applicable (exemption criteria are listed on the next page)]

* Our agency qualifies for the limited exemption under 40 Pa C.S.A. §4532. Our Information Security Program was developed although it is not a requirement under §4513 for agencies of our size (see Appendix A below).

If this exemption no longer applies in the future, additional sections will be added to this Information Security Policy, as required by the PA statute, to include more specific elements including:

* Conducting regular penetration testing (§4513(c)(2)(viii));
* Establishing audit trails ((§4513(c)(2)(ix))
* Establish procedures, guidelines and standards for development of in-house developed applications (§4513(c)(2)(v)
* Using multi-factor authentication, if needed (§4513(c)(2)(vii));
* Providing regular cybersecurity awareness training for all personnel §4513(5);
* Other items, as applicable.

**APPENDIX A**

**Limited exemption** - Applicable provisions based on agency characteristics (§4532):

|  |  |
| --- | --- |
| Agencies which have:**(1)** Fewer than 10 employees, **OR****(2)** Less than $5,000,000 in gross annual revenue, **OR****(3)** Less than $10,000,000 in year-end total assets. | All other agencies doing business in PA |
| If you qualify for the above **limited exemption**Agencies that qualify for the limited exemption are still required to comply with the following provisions:* Investigating cybersecurity events
* Providing notice of a “cybersecurity event” to the PA Insurance Commissioner within five (5) business days of the determination of an event (§4518(a));
* When applicable, providing notice to consumers as required under the Breach of Personal Information Notification Act (§4518(d)).
 | If you **do not qualify for the limited exemption**, you need to comply with the entire regulation, including:* Performing a risk assessment as described under §4512
* Developing, implementing and maintaining an Information Security Program as described in §4513.
* Implementing corporate oversight of the program – applicable if the agency has a Board of Directors (§4514)
* Implementing the oversight of third-party service provider arrangements described under §4515
* Investigating cybersecurity events
* Providing notice of a “cybersecurity event” to the PA Insurance Commissioner within five (5) business days of the determination of an event (§4518(a));
* When applicable, providing notice to consumers as required under the Breach of Personal Information Notification Act (§4518(d)).
 |

**Automatic compliance**

If your agency is subject to the privacy, security and breach notification rules issued under 45 CFR Pts. 160 (**HIPAA** – HITECH), **and you maintain nonpublic information in the same manner as Protected Health Information (PHI)**, you are considered compliant with this law. You are still required to provide the notifications under section 4518(a), (b) and (c) if you experience a cybersecurity event.

**APPENDIX B**

Excerpt from [Pennsylvania Insurance Data Security Law](https://www.legis.state.pa.us/cfdocs/Legis/LI/uconsCheck.cfm?txtType=HTM&yr=2023&sessInd=0&smthLwInd=0&act=2) set forth at T. 40 Pa C.S.A. section 4513

**§ 4513.  Information security program.**

(a)  Requirement for implementation and objectives.--Each licensee shall develop, implement and maintain a comprehensive written information security program based on the licensee's risk assessment that:

(1)  Contains administrative, technical and physical safeguards for the protection of nonpublic information and the licensee's information systems.

(2)  Is commensurate with the following:

(i)  The size and complexity of the licensee.

(ii)  The nature and scope of the licensee's activities, including the licensee's use of third-party service providers.

(iii)  The sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control.

(3)  Is designed to protect:

(i)  The security and confidentiality of nonpublic information and the security of the information systems.

(ii)  Against any threats or hazards to the security or integrity of nonpublic information and the information systems.

(iii)  Against unauthorized access to or use of nonpublic information and that minimizes the likelihood of harm to a consumer.

(4)  Defines and periodically reevaluates a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

(b)   Designation of responsibility.--A licensee shall designate one or more employees, an affiliate or an outside vendor to act on behalf of the licensee who shall be responsible for the information security program of the licensee.

(c)  Standards.--A licensee shall develop an information security program based on its risk assessment and shall:

(1)  Design its information security program to mitigate the identified risks, in a manner that is commensurate with the following:

(i)  The size and complexity of the licensee.

(ii)  The nature and scope of the licensee's activities, including the licensee's use of third-party service providers.

(iii)  The sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control.

(2)  Determine which security measures are appropriate and implement the security measures by:

(i)  Placing access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information.

(ii)  Identifying and managing the data, personnel, devices, systems and facilities that enable the licensee to achieve business purposes in accordance with their relative importance to business objectives and the licensee's risk strategy.

(iii)  Restricting physical access to nonpublic information only to authorized individuals.

(iv)  Protecting, by encryption or other appropriate means, all nonpublic information transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media.

(v)  Adopting secure development practices for in-house developed applications utilized by the licensee.

(vi)  Modifying the information systems in accordance with the licensee's information security program.

(vii)  Utilizing effective controls, which may include multifactor authentication procedures, for any employees accessing nonpublic information.

(viii)  Regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.

(ix)  Including audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee.

(x)  Implementing measures to protect against destruction, loss or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures.

(xi)  Developing, implementing and maintaining procedures for the secure disposal of nonpublic information in any format.

(3)  Include cybersecurity risks in the licensee's enterprise risk management process.

(4)  Stay informed regarding emerging threats or vulnerabilities and utilize security measures when sharing information relative to the character of the sharing and the type of information shared.

(5)  Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

(d)  Monitoring, evaluation and adjustment.--A licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with:

(1)  Any relevant changes in technology.

(2)  The sensitivity of the licensee's nonpublic information.

(3)  Internal or external threats to information.

(4)  The licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

(e)  Incident response plan.--As part of its information security program, each licensee shall establish and maintain a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity or availability of nonpublic information in its possession, the licensee's information systems or the continuing functionality of any aspect of the licensee's business or operations. The incident response plan shall address the following areas:

(1)  The internal process for responding to a cybersecurity event.

(2)  The goals of the incident response plan.

(3)  The definition of clear roles, responsibilities and levels of decision-making authority.

(4)  External and internal communications and information sharing.

(5)  Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls.

(6)  Documentation and reporting regarding cybersecurity events and related incident response activities.

(7)  The evaluation and revision of the incident response plan following a cybersecurity event, as necessary.

1. If you are unsure, contact IA&B [↑](#footnote-ref-1)
2. Note that (1) the nature of the Cybersecurity event will determine what, if any, notification is required (see §4518(a); (2) notification letter templates may be available on IA&B’s website (for members only); (3) the need to notify the media under 5. d. generally depends on the number of individuals whose information was breached; refer to applicable law before proceeding. [↑](#footnote-ref-2)
3. This Disposal Rule stems from the Fair & Accurate Credit Transactions Act (F.A.C.T.A.), and governs the disposal of certain information contained in Consumer Reports, such as credit or insurance scores, MVRs, C.L.U.E. reports, etc. [↑](#footnote-ref-3)
4. The agency should scrutinize the agreement with the Third-Party Service Provider to verify that a provision is included whereby the TPSP agrees to implement security controls and safeguard NPI that are at least as strong as those implemented by the agency. If it is not, an addendum should be executed separately and made part of the agreement. [↑](#footnote-ref-4)
5. If a provision on the duty to notify the agency is not currently included in the contract with the TPSP, the agreement should be amended or a new one executed. [↑](#footnote-ref-5)