INTERNAL AGENCY RISK ASSESSMENT GUIDE

This resource is meant as a tool to assist IA&B member agencies in assessing risks and vulnerabilities and facilitate development of an Information Security Program so that the agency may comply with the requirements of Pennsylvania's Insurance Data Security Act (Act 2 of 2023). [1]

An **Internal Agency Risk Assessment** serves as the foundation for creating your cybersecurity policy.

This self-assessment helps you identify possible areas of data exposure, both internally and externally. It should be carried out in accordance with established written policies and procedures and have its results documented. Such policies and procedures should include:

1. Criteria to evaluate and categorize identified cybersecurity risks or threats
2. Criteria to assess the confidentiality, integrity, security and availability of the agency's Information Systems and Nonpublic Information (NPI), including the adequacy of existing controls for identified risks
3. Establish criteria to identify risks and how they will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

This risk assessment should be performed periodically to consider technological developments, evolving threats and changes in business operations. It should also consider the particular risks of the agency's operations related to cybersecurity, NPI collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect NPI.

As a first step, consider the questions below. If you are not able to answer the question affirmatively, consider the area and determine if it is an area that your agency should address. You may consider reviewing the questionnaire with your IT Security provider.

INFORMATION SECURITY

1. Are you able to detect Cybersecurity Events?
2. Do you collect the information necessary to detect and respond to Cybersecurity Events?
3. Do you limit user access to systems that store NPI?
4. Do you have policies to ensure the security of NPI by Third Party Service Providers?
5. Do you conduct penetration testing of the information systems that store NPI a minimum of once per year?

A Cybersecurity Event (as defined by the state of Pennsylvania's Cybersecurity Law is "an event resulting in unauthorized access to, disruption of or misuse of an information system or nonpublic information stored on the information system." Note that this can be an internal or external event. Different states may have different definitions of what qualifies as a Cybersecurity Event.

"Internal" exposure is employee driven. The best perimeter defenses and cyber security

[1] If you qualify for an exemption (see last page), you may still consider using this document to assess your vulnerabilities.

6. Do you conduct vulnerability assessments of Information System that store NPI a minimum of twice per year?
7. Is your information system able to reconstruct material financial transactions?
8. Do you use secure development practices for in-house developed applications?
9. Do all individuals accessing your internal networks from an external network utilize Multi Factor Authentication?
10. Are your paper files stored in a secure location?
11. Do you allow the use of email systems not under the control of the Covered Entity (e.g. personal webmail services)?
12. Do you allow the use of cloud storage services such as DropBox, Box, or Office365?
13. Do you or do you plan to regularly review the effectiveness of the safeguards you have in place to protect NPI?

controls can be defeated by untrained or malicious employees.

All controls are important to a robust Cybersecurity program. However, your Information Security Program, which will be designed based on this risk assessment, can take into account the size and complexity of your agency operations.

You should consider adopting a Computer Use policy that requires employees to use the same security standards when accessing agency data from non-company-controlled equipment.

EMPLOYEE RESPONSIBILITY

14. Have you ever conducted staff training on what information is considered NPI?
15. Have you ever conducted staff cybersecurity training and training on your Computer Use policy?
16. Do you or do you plan to require employees to acknowledge they have received and read the "Cybersecurity Policy"?

ASSET INVENTORY AND DEVICE MANAGEMENT

17. Are employees required to adhere to the following provisions in regards to electronic assets and devices:
    a. Are employees required to keep their (personal or company) cell phone in their possession or in a secured location if it has access to NPI?
    b. Are employees required to password protect their mobile devices?
    c. Are employees instructed not to share their passwords or access information with others?

It is impossible to ensure individuals will return all agency data upon separation, but the risk can be mitigated as follows:

1. **Strategic exit interview**
2. **Departure declarations ("I have not taken your information; I have returned all devices and information, etc.")**
3. **Forensic review of agency-issued devices.**

d. Are employees instructed not to put any agency data on thumb drives, laptops or other portable media unless authorized to do so by the agency?
e. If employees are authorized to put data on portable media, is said media encrypted and password-protected?

NOTE: Computer Use polices are important here because, in addition to contractual obligations, they can be used in enforcement actions or litigation to hold former employees accountable for taking NPI.
Remote wiping will not be possible for cell phones without control of the account or device via specialized software; remote wiping of a laptop device also would require specialized systems; best defense is strong password protection PLUS encryption so data is inaccessible; best if Covered Entity keeps record of device serial number.

f. Is there an internal off-boarding policy to ensure employees who no longer work for the agency do not have access to NPI?
g. Is there an internal off-boarding policy to mitigate the risk that employees who no longer work for the agency have taken NPI?
h. Can an employee's access to email and voicemail be immediately disabled, if needed?
i. Is there a policy to force individuals to return all agency data upon separation?
j. Are employees required to report all actual or potential unauthorized access of NPI?

18. Does the agency keep an inventory of all devices that have access to your network (See Device Inventory Template)?
19. Are connected devices encrypted and password protected?
20. Are devices able to be wiped if lost or stolen?
21. Are storage locations of all paper that has NPI on a device locked and secured?

ACCESS CONTROLS & IDENTITY MANAGEMENT

22. Is each individual able to create and reset passwords to an acceptable standard?
23. Do you force password resets for everyone on a periodic basis?
24. Are employees told not to share passwords?
25. Are employees required to lock computer screens and other portable storage devices when not in use?

Consider:

- **Addressing password creation standards in your Computer Use policy that establish criteria for a strong password: 11 characters including 1 number, 1 capital letter and 1 special character, etc.**
- **Prohibiting employees from sharing passwords.**

26. Are employees trained on how to identify trustworthy sources and the risks of using unapproved software or applications?

Phishing and B2B fraud bypass most internal security controls by duping the recipient. B2B fraud is on the rise and can result in significant financial damage; affects

27. Are employees specifically trained on how to detect fraudulent emails (e.g. phishing, B2B fraud)?

accounts payable but is typically initiated from cyber source.

28. Does the agency restrict access to NPI on its network (e.g. file server)?
29. If NPI is stored on the agency's network (e.g. on a file server), is it encrypted?
30. Does the agency have or plan to have an internal policy on how much NPI will be collected and stored in relation to credit card and banking information?

SYSTEMS & NETWORK SECURITY, OPERATIONS & AVAILABILITY

31. Does the agency utilize an email filter (hardware, software or third-party provided) to restrict and eliminate viruses?
32. Does the agency utilize technology to restrict access to NPI?

Don't be confused! A VPN (Virtual Private Network) is typically used for employee access to internal systems. A SSL (Secure Sockets Layer) establishes an encrypted link between a web server and browser.

33. Does the agency have up-to-date network security and firewall protection on its servers, computers and mobile devices?
34. Are agency backups password protected, encrypted, and stored off-site?
35. Are outgoing emails and attachments that include NPI transmitted through a secure email system?
36. In cases where consumers are entering NPI via the agency's website or portal, is the connection encrypted with SSL?
37. When an employee accesses the agency's systems or any NPI, is the employee required to use the agency's secure VPN connection?

SYSTEM & NETWORK MONITORING

38. Does the agency monitor its Systems for unauthorized or disruptive activity?
39. Does the agency conduct due diligence to ensure their third-party service providers that are provided NPI have required security controls and written policies in place or does the agency plan to put this into place?

Keep in mind that a Cybersecurity event can be internal or external. The Agency needs to choose a method of monitoring Cybersecurity events. If it is too price prohibitive to hire a monitoring firm (which is recommended), some other form of monitoring must be done.

BUSINESS CONTINUITY & DISASTER RECOVERY

40. Are employees trained on how to report a potential or actual security breach?
41. Within your agency, do you have plans for a disaster recovery?
42. Are there protections for customer information included in your disaster recovery plan?

MISCELLANEOUS

43. Does the agency have a backup generator on-site?
44. Does the agency currently have or have plans to complete a risk assessment for each vendor or provider used?
45. Does the agency currently keep or have plans to keep an inventory of all vendors or providers deemed acceptable by the agency through its due diligence process?

NEXT STEP: PREPARE A CYBERSECURITY PROGRAM & POLICY

The program should be based on the results of your risk assessment. It should implement appropriate defensive infrastructure, procedures, employee training and other tactics that your agency chooses to protect your Information Systems and NPI.

REMINDERS

Exemptions (§4532): if your agency has fewer than 10 employees, less than$5 million in gross revenue OR less than $10 million in year-end total assets, the law only requires you to (1) investigate cybersecurity events and (2) notify the Insurance Commissioner within 5 business days of a cybersecurity event.

Unless you are exempt, Pennsylvania's Insurance Data Security Law requires you to perform a risk assessment and to implement and maintain a written Information Security Program (ISP). Even if you are exempt from the risk assessment and ISP under Pennsylvania's Act 2 of 2023:

- you may have to comply with other states where you are licensed and do business;
- other federal and state laws and regulations require an ISP, and you should already have one in place.

Using this risk assessment questionnaire could help you consider possible improvements to your existing Program.

GUIDELINES DISCLAIMER

IA&B is providing these guidelines for conducting an internal risk assessment solely as a tool to assist agencies in complying with Pennsylvania's Insurance Data Security Act (Act 2 of 2023). These sample guidelines are not a substitute for agencies independently evaluating any business, legal or other issues, and is not a recommendation that a particular course of action be adopted. State security breach notification and privacy laws, coupled with insurance laws and regulations, impose varying requirements on agencies. Therefore, it is extremely important for agencies to carefully review applicable laws and regulations in all jurisdictions where they do business in structuring their specific security policies.

If specific advice is required or desired, the services of an appropriate, competent professional should be sought. Any agency that uses these guidelines agrees that IA&B will have no liability for anything related to the use of this tool or the internal risk assessment that is conducted.

This risk assessment was adapted and modified from the Big I New York's resource

Last modified: July 25, 2023 [*based on Feb 4, 2019 version for BigINY.org/cyber]*