Data Privacy Risk Assessment
Recommendations for Consideration and Implementation

Jim Giszczak and Dom Paluzzi, McDonald Hopkins PLC

Analysis and determinations

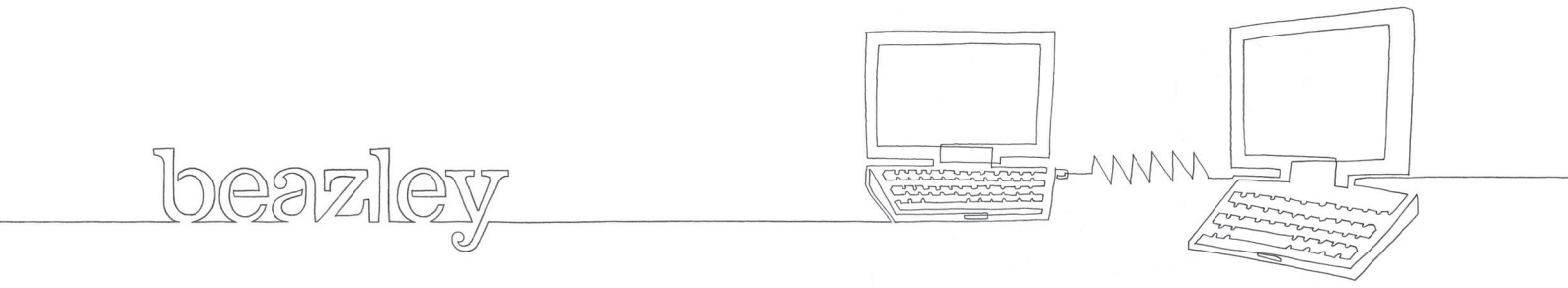
- Review records and databases to determine if the organization owns, licenses, stores or maintains personally identifiable information (PII), protected health information (PHI) or payment cardholder information (PCI).
- Identify the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices containing PII/PHI/PCI.
- Identify and evaluate reasonably foreseeable internal and external risks to paper and electronic records containing PII/PHI/PCI.
- Alternatively, treat all records as if they all contain PII/PHI/PCI.
- Evaluate the effectiveness of current safeguards to determine adequacy and generate a baseline for any additional compliance safeguards.
- Ensure that that the amount of PII/PHI/PCI collected is limited to the amount reasonably necessary to accomplish legitimate business purposes or to comply with state or federal regulations.
- Ensure that the length of time records containing PII/PHI/PCI are stored is limited to the time reasonably necessary to accomplish legitimate business purposes or to comply with state or federal regulations.

Data privacy procedures and safeguards

- Store records (electronic or paper) and data containing PII/PHI/PCI in locked facilities, storage areas or containers.
- Shred records containing PII/PHI/PCI upon disposal.
- Limit access to PII/PHI/PCI records to those persons who have a "need to know" in connection with the organization's legitimate business purpose, or in order to comply with state or federal regulations.
- Require ongoing employee training on best practices for safeguarding and protecting PII/PHI/PCI.
- Invoke disciplinary measures for violators of data privacy policies.
- Immediately block terminated employees' physical and electronic access to PII/PHI/PCI records (including deactivating their passwords and user names).
- Review security measures at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PII/PHI/PCI records.

Items specific to electronic records

- Put in place secure authentication protocols that provide for
  - control of user IDs and other identifiers
  - a reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)
  - control of data security passwords such that passwords are kept in a location and format that does not compromise the security of the data they protect
  - restricting access to PII/PHI/PCI to active users and active user accounts
  - blocking access after multiple unsuccessful attempts to gain access
- Ensure secure access control measures that restrict access, on a "need to know" basis, to PII/PHI/PCI records and files.
- Assign unique identifications plus passwords (which are not vendor-supplied default passwords) to each person with computer access that are reasonably designed to maintain the security of those access controls.
- To the extent technically feasible, encrypt all PII/PHI/PCI records and files that are transmitted across public networks, and that are to be transmitted wirelessly.
- To the extent technically feasible, encrypt all PII/PHI/PCI stored on laptops or other portable devices (i.e., USB drives, backups, etc.).
- Put in place monitoring to alert to the occurrence of unauthorized use of or access to PII/PHI/PCI.
- On any system that is connected to the Internet, make sure firewall protection for files containing PII/PHI/PCI and operating system security patches to maintain the integrity of the PII/PHI/PCI are kept reasonably up to date.
- Maintain reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions.



Written information security program (WISP)

- Implement a comprehensive written information security program (WISP) applicable to all records containing PII/PHI/PCI.
- Designate one or more employees to maintain and supervise WISP implementation and performance.
- Institute a procedure for regular monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PII/PHI/PCI, and upgrade the WISP as necessary.

Incident response plan and team

- Develop an incident response plan (IRP) and keep it up to date.
- Identify the incident response team (IRT) members.
- Develop a process for reporting suspected data security incidents and how they are escalated.
- Conduct tabletop breach exercises with the IRT using the IRP as a guide.
- Develop a process for documenting any actions taken in connection with any breach of security, and after incidents conduct a post-incident review of events and actions taken to improve security.

Agreements and policies

- Have employees and independent contractors execute a confidentiality agreement.
- Have vendors execute a confidentiality agreement with assurances on privacy compliance.
- Consider having visitors and guests execute a confidentiality agreement upon their visit to the organization's premises.
- Consider the following policies:
  - Employee handbook
  - Computer and electronic devices usage policy
  - BYOD (bring your own device) policy
  - Document retention/destruction policy
  - Telecommuting policy
  - Social media policy
  - Privacy policy

Third-party vendors (outsourcing)

- Ensure that policies and procedures cover when and how records containing PII/PHI/PCI should be kept, accessed, or transported off the business premises.
- If any PII/PHI/PCI data is entrusted to cloud-based vendors, take reasonable steps to select and retain third-party service providers (vendors) that are capable of maintaining appropriate security measures consistent with data security regulations. Ensure that such vendors are required by contracts to
  - implement and maintain such appropriate security measures for PII/PHI/PCI
  - immediately notify the organization of any breach of PII/PHI/PCI (or suspected breach of PII/PHI/PCI) that occurs at the vendor
  - immediately return or destroy PII/PHI/PCI in the vendors' possession when the contract terminates (or when there is no longer a legitimate business need to possess such PII/PHI/PCI)
  - maintain cyber liability insurance
- Have a third party conduct a risk assessment/audit of the organization's security practices and safeguards.
- Consider third-party penetration testing on the organization's system(s) and site(s).

Cyber Liability Insurance Coverage

- Consider both first party and third party breach response/cybersecurity insurance coverage options.

Jim Giszczak and Dom Paluzzi co-chair the Data Privacy and Cybersecurity practice group at McDonald Hopkins PLC.

Their team advises organizations on data privacy and cybersecurity risks on both a national and international basis, including proactive compliance, incident response strategies and management, and defense of regulatory enforcement actions and single-plaintiff and class action litigation. They have counseled clients through over 1,000 data breaches and privacy incidents where they work closely with local, state and federal law enforcement, forensic investigators and third-party vendors to offer clients efficient and effective breach response services.