Data Privacy Risk Assessment Questionnaire

Organization Name

Your Name

Your Position with the Organization

General Inquiries

1. Briefly describe the organization and its primary function(s).

2. Briefly describe any subsidiaries, affiliates, or divisions of the organization.

3. How many employees does the organization have?

4. Where does the organization operate (identify applicable states and countries)?

Analysis and Determinations

5. Has the organization reviewed its records and databases to determine if it owns, licenses, stores or maintains Personally Identifiable Information ("PII"), Protected Health Information ("PHI") or Payment Cardholder Information ("PCI")?

□ Yes □ No □ In Development

6. Has the organization identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices, containing PII/PHI/PCI?

□ Yes □ No □ In Development

7. Has the organization identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PII/PHI/PCI?

□ Yes □ No □ In Development

8. Has the organization chosen, as an alternative, to treat all records as if they all contain PII/PHI/PCI?

□ Yes □ No □ In Development

9. Has the organization evaluated the effectiveness of current safeguards to determine adequacy and generate a baseline for any additional compliance safeguards?

□ Yes □ No □ In Development

10. Has the organization determined 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?

□ Yes □ No □ In Development

11. Has the organization determined 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?

□ Yes □ No □ In Development

Data Privacy Procedures & Safeguards

12. Does the organization store records (electronic or paper) and data containing PII/PHI/PCI in locked facilities, storage areas or containers?

□ Yes □ No □ In Development

13. Does the organization shred records containing PII/PHI/PCI upon disposal?

□ Yes □ No □ In Development

14. Is access to PII/PHI/PCI records limited 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?

□ Yes □ No □ In Development

15. Does the organization require ongoing employee training on best practices for safeguarding and protecting PII/PHI/PCI?

□ Yes □ No □ In Development

16. Does the organization invoke disciplinary measures for violators of data privacy policies?

□ Yes □ No □ In Development

17. Does the organization immediately block terminated employees' physical and electronic access to PII/PHI/PCI records (including deactivating their passwords and user names)?

□ Yes □ No □ In Development

18. Are the organization's security measures reviewed 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?

□ Yes □ No □ In Development

Items Specific to Electronic Records

19. Does the organization have in place secure authentication protocols that provide for:

a. Control of user IDs and other identifiers?

□ Yes □ No □ In Development

b. A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?

□ Yes □ No □ In Development

c. Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect?

□ Yes □ No □ In Development

d. Restricting access to PII/PHI/PCI to active users and active user accounts?

□ Yes □ No □ In Development

e. Blocking access after multiple unsuccessful attempts to gain access?

□ Yes □ No □ In Development

20. Does the organization have secure access control measures that restrict access, on a "need to know" basis, to PII/PHI/PCI records and files?

□ Yes □ No □ In Development

21. Does the organization assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?

□ Yes □ No □ In Development

22. Does the organization, 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?

□ Yes □ No □ In Development

23. Does the organization, to the extent technically feasible, encrypt all PII/PHI/PCI stored on laptops or other portable devices (i.e., USB drives, backups, etc.)?

□ Yes □ No □ In Development

24. Does the organization have monitoring in place to alert it to the occurrence of unauthorized use of or access to PII/PHI/PCI?

□ Yes □ No □ In Development

25. On any system that is connected to the Internet, does the organization have reasonably up-to-date firewall protection for files containing PII/PHI/PCI; and operating system security patches to maintain the integrity of the PII/PHI/PCI?

□ Yes □ No □ In Development

26. Does the organization have reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions?

□ Yes □ No □ In Development

Written Information Security Program ("WISP")

27. Does the organization have a comprehensive, written information security program ("WISP") applicable to all records containing PII/PHI/PCI?

□ Yes □ No □ In Development

28. Has the organization designated one or more employees to maintain and supervise WISP implementation and performance?

□ Yes □ No □ In Development

29. Has the organization instituted a procedure for regularly 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 for upgrading the WISP as necessary?

□ Yes □ No □ In Development

Incident Response Plan & Team

30. Has the organization developed an Incident Response Plan?

□ Yes □ No □ In Development

31. Has the organization updated the Incident Response Plan in the last year?

□ Yes □ No □ In Development □ N/A

32. Has the organization assembled an Incident Response Team?

□ Yes □ No □ In Development

33. Has the organization identified any of the following external breach response resources?

□ Legal Counsel

□ Forensics

□ Notification

□ Call Center

□ Credit Monitoring/Remediation

□ Crisis Communication/PR Management

34. Has the organization developed a process for reporting suspected data security incidents and how they are escalated?

□ Yes □ No □ In Development

35. Has the organization conducted any tabletop breach exercises with the Incident Response Team using the Incident Response Plan as a guide?

□ Yes □ No □ In Development

36. Has the organization suffered any data breach during the past five (5) years?

□ Yes □ No

37. Does the organization have in place a procedure for documenting any actions taken in connection with any breach of security, and does that procedure require post-incident review of events and actions taken to improve security?

□ Yes □ No □ In Development

Agreements and Policies

38. Does the organization have its employees and independent contractors execute a Confidentiality Agreement with specific data privacy provisions?

□ Yes □ No □ In Development

39. Does the organization have its vendors execute a Confidentiality Agreement with specific data privacy provisions?

□ Yes □ No □ In Development

40. Does the organization have its visitors/guests execute a Confidentiality Agreement upon their visit to the organization's premises with specific data privacy provisions?

□ Yes □ No □ In Development

41. Does the organization have an employee handbook?

□ Yes □ No □ In Development

42. Does the organization have a computer & electronic devices usage policy?

□ Yes □ No □ In Development

43. Does the organization have a BYOD (Bring Your Own Device) policy?

□ Yes □ No □ In Development

44. Does the organization have a document retention/destruction policy?

□ Yes □ No □ In Development

45. Does the company have a telecommuting policy?

□ Yes □ No □ In Development

46. Does the company have a social media policy?

□ Yes □ No □ In Development

47. Has the organization developed a privacy policy?

□ Yes □ No □ In Development

Third-Party Vendors (Outsourcing)

48. Does the organization have policies and procedures for when and how records containing PII/PHI/PCI should be kept, accessed or transported off the business premises?

□ Yes □ No □ In Development

49. Does the organization entrust any of its PII/PHI/PCI data with cloud-based vendors?

□ Yes □ No □ In Development

50. Has the organization taken reasonable steps to select and retain third-party service providers (vendors) that are capable of maintaining appropriate security measures consistent with data security regulations?

□ Yes □ No □ In Development

51. Has the organization required such vendors, by contract, to implement and maintain such appropriate security measures for PII/PHI/PCI?

□ Yes □ No □ In Development

52. Has the organization required such vendors, by contract, to immediately notify the organization of any breach of PII/PHI/PCI (or suspected breach of PII/PHI/PCI) that occurred at the vendor?

□ Yes □ No □ In Development

53. Has the organization required such vendors, by contract, to 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)?

□ Yes □ No □ In Development

54. Has the organization required such vendors, by contract, to maintain cyber liability insurance?

□ Yes □ No □ In Development

55. Has a risk assessment/audit of the organization's security practices and safeguards been conducted by a third-party?

□ Yes □ No □ In Development

56. Has a third-party ever conducted any penetration testing on the organization's system(s) and site(s)?

□ Yes □ No □ In Development

Cyber Liability Insurance Coverage

57. Does the organization maintain a cyber liability insurance policy?

□ Yes □ No □ In Development

a. Please indicate whether the policy covers the following:

First-Party Coverages

□ Event management expenses
□ Cyber extortion
□ Data restoration
□ Business interruption

Third-Party Coverages

□ Network security liability
□ Privacy liability
□ Privacy regulatory proceedings
□ Electronic (website) media liability
□ Litigation defense

Payment Card Industry Compliance

58. Is the organization involved in payment card processing (i.e., does the organization transmit, store or process credit/debit cardholder data)?

□ Yes □ No □ In Development

59. Has the organization reviewed the PCI Data Security Standards for compliance?

□ Yes □ No □ In Development □ N/A

60. Is the organization compliant with the PCI Data Security Standards?

□ Yes □ No □ In Development □ N/A

When completed, save the PDF and please return to
dataprivacy@mcdonaldhopkins.com

An attorney from our national Data Privacy and Cybersecurity Practice will contact you to discuss the results of your Risk Assessment Questionnaire. Thank you!

James J. Giszczak
Co-Chair, National Data Privacy
and Cybersecurity Practice
313.407.4049
jgiszczak@mcdonaldhopkins.com

Dominic A. Paluzzi
Co-Chair, National Data Privacy
and Cybersecurity Practice
248.904.9507
dpaluzzi@mcdonaldhopkins.com

We live data privacy 24/7.

24/7 HOTLINE: 855-MH-DATA1
855-643-2821

Compliance Counseling & Risk Assessment • Training • Breach Response Workshops
Breach Coaching • Litigation & Class Action • Regulatory Defense