Security Self-Assessment

The HIPAA Security Self-Assessment questions are aimed to help you self-evaluate compliance with HIPAA laws and the protection of client personal and health information. The goal is to enhance your organization's understanding of your data security and privacy preparedness level.

What is Protected Health Information (PHI)?

Section 1: Security Assessment Basics

1. Please tell us who is completing the Self-Assessment *

First Name

Last Name

Title

Company Name

City

Email Address

2. Has your organization completed a security risk assessment (SRA) before?

- Yes
- No
- I don't know

3. Do you ensure you are meeting current HIPAA security regulations?

- Yes
- No
- I don't know

Section 2: Security Policies

4. Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?

- Yes
- No
- I don't know

5. How does documentation for your risk management and security procedures compare to your actual business practices?

- Like for like
- Somewhat similar
- Not at all similar
- N/A

Section 3: Security and Workforce

6. Do you have a designated person responsible for developing, implementing and maintaining information security policies and procedures?

- Yes
- No
- I don't know

7. Do you identify and document the responsibilities of the information security officer?

- Yes
- No
- N/A

8. Do you have specifications of roles and job duties by the need to access to protected health information (PHI)?

- Yes
- No

9. Do you screen your workforce members to verify trustworthiness?

- Yes
- No

10. Do you ensure that all workforce members (including management) are given HIPAA training?

- Yes
- No

11. Are procedures in place for monitoring log-in attempts and reporting discrepancies?

- Yes
- No

12. Is protection from malicious software (including timely antivirus/ security updates and malware protection) covered in your procedures?

- Yes
- No

13. Do you review password security elements in your security training?

- Yes
- No
- N/A

14. Do you apply corrective measures to enforce security procedures?

- Yes
- No

Section 4: Security and Data

15. Do you manage and control personnel access to electronic protected health information (ePHI), systems, and facilities?

- Yes
- No

16. Do you have a process for authorizing, establishing, and modifying access to ePHI?

- Yes
- No

17. How are individual users identified when accessing ePHI?

- Each user has a unique ID username and password
- Several users share a department ID username and password
- I don't know

18. Do you ensure all of your workforce members have appropriate access to ePHI?

- Yes
- No

19. Do you use encryption to control access to ePHI?

- Yes
- No
- I don't know

20. Do you periodically review your information systems for how security settings are implemented to safeguard ePHI?

- Yes
- No

21. Do you have hardware, software, or other mechanisms that record and examine activity on information systems with access to ePHI?

- Yes
- No

22. Do you have a mechanisms in place to log system activity?

- Yes
- No

23. Do you have automatic logoff enabled on devices and platforms accessing ePHI?

- Yes
- No

24. Do you protect ePHI from unauthorized modification or destruction?

- Yes
- No

25. Do you protect against unauthorized access to or modification of ePHI when it is being transmitted electronically?

- Yes
- No

26. Do you periodically review your information systems to identify and mitigate technical vulnerabilities?

- Yes
- No

Page 2

Section 5: Security and the Organization

27. Do you manage access to your facility?

- Yes
- No

28. Do you have physical protections in place to manage facility security risks?

- Yes
- No

29. Do you restrict physical access to equipment that houses PHI?

- Yes
- No

30. Do you manage workforce member, visitor and third party access to electronic devices?

- Yes
- No

31. Do you have physical protections in place to manage electronic device security risks?
(such as cable locks for portable laptops or screen filters for screens visible in high traffic areas)

- Yes
- No

32. Do you keep an inventory record of all electronic devices?

- Yes
- No

33. Do you have requirements in place for retention of audit reports pertaining to physical and electronic system security?

- Yes
- No

34. Do you have data encryption software on your electronic devices?

- Yes
- No
- I don't know

35. Do you ensure access to ePHI is terminated when employment with the workforce member ends?

- Yes
- No

Section 6: Security and Business Associates

36. Do you contract with business associates or other third-party vendors?

- Yes
- No

37. Do you allow third party vendors to access your information systems and/or ePHI?

- Yes
- No

38. Do you have a process to identify which business associates need access to create, receive, maintain or transmit ePHI?

- Yes
- No
- N/A

39. Have you executed business associate agreements with all business associates who create, receive, maintain or transmit ePHI on your behalf?

- Yes
- No
- N/A

Section 7: Contingency Planning

40. Does your organization have a contingency plan in the event of an emergency?

- Yes
- No

41. Have you considered what kind of emergencies could damage critical information systems or prevent access to ePHI at your organization?

- Yes
- No

42. Does your practice have policies and procedures in place to prevent, detect and respond to security incidents?

- Yes
- No

43. Has your practice identified specific personnel as your incident response team?

- Yes
- No

44. Has your organization evaluated and determined which systems and ePHI are necessary for maintaining business-as-usual in the event of an emergency?

- Yes
- No

45. Do you have a plan for backing up and restoring critical data?

- Yes
- No

46. Do you have a process for terminating your emergency procedure after the emergency circumstance is over?

- Yes
- No

47. Do you formally evaluate the effectiveness of your security safeguards, including physical safeguards?

- Yes
- No

Thank You!

You have completed the Security Self-Assessment. We know your time is valuable and appreciate the time taken today.

These results have been submitted to Healthy Alliance IPA for review, and you will receive a confirmation email with a copy of the questions and your answers.

Please reach out to security@abhealth.us if you have any questions.