Risk Analysis and Management Assessment 2021

1. What Electronic Protected Health Information (EPHI) exists for this organization? Where does it reside?

2. Is there any new EPHI since the last audit? Have considerations been made for that new EPHI?

3. Who has access to the EHR system and the EPHI contained?

4. Do all employees have the same access to data?

5. Does your practice have EPHI on mobile computing or storage platforms? How is this information protected?

6. How will I know if EPHI has been disclosed or potentially compromised?

7. How will storage equipment or computers containing EPHI be disposed to protect data?

8. How are backups secured?

9. Is EPHI being exchanged with patients or other entities electronically?

10. Who in the office will be generating EPHI?

11. Is there a process to ensure that EPHI is not modified or deleted?

12. How will EPHI availability be ensured by my organization? Will this data be available as needed for authorized after hours or emergency purposes?

13. Is there a backup strategy in place?

14. Do we train employees on the use of EPHI? Do employees understand the importance of protecting EPHI?

15. As employees come into or leave our organization, do we have processes to ensure that access controls are updated accordingly?

16. Do we have an incident response policy in the event of a security incident involving EPHI?

17. Do staff know who to contact in the event they feel there may have been an incident?

18. Does my practice have a contingency plan in case of extended loss of access to EHR due to natural disaster, internet outage, server downtime, extended power loss, or similar emergency?

19. What processes exist for transferring EPHI with other entities?

20. Do we have physical protection in place for our office and devices containing EPHI?

21. Are workstations secured from unauthorized access to EPHI?

22. Are mobile / external devices secured to prevent loss of EPHI?

23. Are staff members trained and performing basic computer security principles?

24. Is my EHR secured using best-practice security?

25. Is there other software on my computers that are not required for business use that may put EPHI at risk?

26. Are systems containing EPHI receiving security updates such as Windows updates, virus pattern updates, etc.?

27. Does my organization use wireless or other mobile networks? If so, what security precautions are taken to mitigate these potential risks?

28. Is my facility located in an area prone to any natural disasters? Have considerations been made for how this may affect my EPHI?

29. Who in the organization will be in charge of performing audits?

(605)977-1250 |support@foxfiresg.com