Top 10 recommendations to Begin your Cybersecurity Setup

SEPTEMBER 2019

1. The generally accepted **FIRST STEP** is to conduct a Risk Assessment.
   A. One option to meet this requirement is an external HIPAA Compliance audit
   B. This is an Annual event/process. There are many checklists available on the web for the audit.

2. A **SECOND STEP** is to assure that all of your PHI data is encrypted.
   A. Encrypt data (A) at rest, (B) during transfers (C) on backups
   B. This is **your "Safe Harbor"** if you are hacked. *Very Important.*

3. To **HELP YOU BE SURE YOU ARE MEETING CYBERSECURITY** standards, contract for annual audits by an external group.
   A. Implement an audit using one or more of the following standards:
      (a) ISO Standards, (c) Soc II requirements,
      (b) HiTrust standards, or (d) NIST standards.

      This will help your EAP organize your P&P to assure you meet the "Trust Services Criteria" in Security, Confidentiality, Availability, Privacy and Process Integrity.

   B. Complete a HIPAA Compliance Audit internally or again have an external group complete this review. To assure yourself that you know where all of the data resides that needs to be protected, complete a PHI Inventory.

   C. Complete or have completed Penetration Tests. Conduct annually using available software or an external group.

4. Something you can do next week to strengthen your security are:
   A. **Add strong passwords** (15 or more characters).
   B. Begin to plan adding 2F Authentication to your sign-ons.

5. **Equipment** recommendations:
   A. Update your firewall daily if needed.
   B. Updated anti-virus and malware software daily if needed.
   C. Update software and firmware at least weekly
   D. Put a time limit on how long monitors are allowed to display data.

6. Appoint a CISO or have one on retainer.

7. Backup your data nightly and keep off-site 1-night p/week.

8. Have Disaster Recovery & Business Continuity Plans & conduct tests.

9. Don't have PII on same network (segmented networks).

10. See Our List of Recommended Policies and Procedures and if you are from the European Union you need to be aware of and comply with GDPR.

DISCLAIMER: This list is in no way a declaration of either priorities or all-inclusive tasks to prepare your EAP for Cybersecurity. There are many more standards, but these will go a long way to introducing you to the complex, standards that you need to implement. The external audits will provide a very detailed list of Policies and Procedures you need to meet.