CDSystems

HIPAA Security Assessment

WHO IS IT FOR?

- **Covered Entities** – Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing Homes, Pharmacies, etc.
- **Business Associates** – Any entity that performs functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a Covered Entity.

WHY IS IT IMPORTANT?

- **It's not optional** – Organizations who must comply with HIPAA regulations must, by law, perform risk assessments and engage in ongoing risk management activities.
- **Things change** – Addressing risk is not a one-time ordeal. As business objectives change, employees come and go, and technology advances, the need for cybersecurity risk assessment services is constant.
- **Fines are real** – HIPAA fines can be categorized as "unknowing" all the way to "willfully negligent" with individual fines ranging from $1,000 to at least $50,000 per occurrence. Several recent breaches have resulted in multi-million-dollar fines. Addressing risk upfront helps you steer clear of fines.

HOW CAN WE HELP?

- **Stay compliant!** – Our risk assessments will help you adhere to HIPAA Security Rule §164.308(a)(1)(ii)(A) which requires covered entities and business associates to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information."
- **Identify gaps** between the existing environment and the HIPAA Security Rule.
- **Develop a roadmap** to remediate gaps in HIPAA compliance.

WHAT IS INCLUDED?

- Correlation of your business objectives, its departments, and its workflows
- Mapping how data is ingested, stored, and transmitted.
- **Interviewing key personnel** – People play a large part in cybersecurity.
- **Configuration review** of critical IT infrastructure.
- **What-if scenarios** – What if we contracted ransomware? What if we lost power? What if a storm took out our datacenter? What if an unencrypted mobile device was left in a cab?
- **Internal and external vulnerability scanning** – Prioritized reporting of all discovered technical vulnerabilities, both internal and internet-facing.
- **C-level and granular reporting** – Executive-level summary as well as detailed reporting.