Healthcare data breaches are increasing, both in frequency and severity. Also on the rise are enforcement actions by federal and state agencies, class action lawsuits and consumer complaints. The resulting financial penalties coupled with negative media exposure can cripple an organization.

Your organization’s current information privacy, security and breach notification program will be assessed in relation to key Office for Civil Rights (OCR) focus areas.

**1. Compliance and Cyber Risk Management Program**
(45 CFR § 164.308(a)(1))

**2. HIPAA Privacy, Security and Breach Notification Policies and Procedures**
(45 CFR §164.530 and 45 CFR §164.316)

**3. Workforce Training**
(45 CFR §164.530(b) and 45 CFR §164.308(a)(5))

**4. HIPAA Security Risk Analysis**
(45 CFR §164.308(a)(1)(ii)(A))

**5. HIPAA Security Risk Management Program**
(45 CFR §164.308(a)(1)(ii)(B))

**6. HIPAA Security Non-technical Evaluation**
(e.g. “Compliance Assessment”)
(45 CFR § 164.308(a)(11))

**7. Technical Testing Of Your Environment**
(45 CFR § 164.308(a)(8))

**8. Business Associate Management Program**
(45 CFR §164.502(e) and 45 CFR §164.308(b))

**9. Privacy Rule and Breach Notification Rule Compliance Assessments**
(45 CFR §164.530 and 45 CFR §164.400)

**10. Documentation and Remediation Plan**
(45 CFR §164.530(c) and 45 CFR §164.306 (a))

Identify key gaps & obtain a recommended, prioritized, tactical plan to establish and implement your HIPAA compliance and cyber risk management program.
10-Point Tactical HIPAA Compliance & Cyber Risk Management Assessment™

**Key benefits**

- Learn and understand all your sources of information risks and liabilities
- Utilize the proven approach and methodology used by 100s of organizations
- Exercise good-faith effort and demonstrate seriousness of intent
- Receive and execute on a prioritized tactical plan tailored to your unique business requirements
- Demystify a complex process by using a by-the-regulations approach
- Make sound decisions and justify expenditures for safeguards and controls most needed for your organization

**High-level, Sample Recommended Action Plan**

**Agree on HIPAA Compliance & Cyber Risk Management Vision**

| PHASE 1 | 1. Complete a HIPAA Security Risk Analysis (45 CFR §164.308(a)(1)(ii)(A)) |
|         | 2. Formalize HIPAA Compliance and Cyber Risk Management Program (45 CFR § 164.308(a)(1)) |

| PHASE 2 | 3. Develop and Implement HIPAA Security Risk Management Program (45 CFR §164.502(e) and 45 CFR §164.308(b)) |
|         | 4. Train All Members of Your Workforce (45 CFR §164.530(b) and 45 CFR §164.308(a)(5)) |
|         | 5. Complete Privacy Rule and Breach Rule Compliance Assessments (45 CFR §164.530 and 45 CFR §164.400) |

| PHASE 3 | 6. Document and Act Upon Remediation Plan |
|         | 7. Maintain Technical Testing of Your Environment (45 CFR § 164.308(a)(8)) |

**Understand Your Compliance & Cyber Risk Posture**

Find out where you stand, and get a clear plan of action with our tactical assessment of your current HIPAA compliance and cyber risk management program. Meet the challenges of increasing interoperability and data sharing while being confident that your organization is following HIPAA regulations.

**Key features:**

- Efficient, 4-week Discovery & Assessment
- Engagement Fixed Price = No Cost Surprises
- Receive a High-Level, Prioritized Tactical Plan for HIPAA Compliance & Risk Management Program
- Board-Ready Executive-Level Findings, Observations & Recommendations (FOR) Presentation

See what Clearwater can do for you.

800-704-3394
clearwatercompliance.com