Learn More About the Clearwater HIPAA Compliance 10-Point Strategic Assessment:
Powerful and Dynamic with a Proven Methodology.

Current Climate

- Increasing frequency of healthcare data breaches
- Increasing severity of healthcare data breaches
- Greater enforcement by Federal and State agencies
- Significantly greater civil monetary penalties
- Increasing interoperability and data sharing driving more potential exposures
- Significantly more patient/member/consumer complaints
- More and larger class-action law suits

→ SIGNIFICANTLY GREATER BUSINESS RISK
→ GREATER EXPECTATIONS OF RESPONSIBILITY FOR EXECUTIVE TEAM AND BOARD

The Solution

- Institute HIPAA Compliance 10-Point Strategic Assessment™
- Receive specific, tangible, actionable strategic plan to address gaps
- Assess effectiveness in ten (10) critical areas
  - Privacy, Security, Risk and Compliance Governance
  - HIPAA Privacy, Security and HITECH Breach Notification Policies & Procedures
  - Workforce Privacy, Security and Compliance Training
  - HIPAA Security Risk Analysis and Risk Management
  - HIPAA Security Non-Technical Evaluation
  - HIPAA Security Technical Evaluation
  - Privacy Rule and Breach Notification Rule Compliance Assessments
  - Business Associate Management Program
  - Insurance Coverage (e.g., Cyber Liability, D&O, E&O, P&C)
  - Remediation Planning and Execution

Executive Summary

<table>
<thead>
<tr>
<th>Critical Assessment Area</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Set Privacy and Security Risk Management &amp; Governance Program in place (45 CFR § 164.308(a)(1))</td>
<td></td>
</tr>
<tr>
<td>2. Develop &amp; Implement comprehensive HIPAA Privacy and Security and Breach Notification Policies &amp; Procedures (45 CFR §164.530 and 45 CFR §164.316)</td>
<td></td>
</tr>
<tr>
<td>3. Train all Members of Your Workforce (45 CFR §164.300(b) and 45 CFR §164.308(a)(5))</td>
<td></td>
</tr>
<tr>
<td>7. Implement a Strong, Proactive Business Associate / Management Program (45 CFR §164.502(e) and 45 CFR §164.306(a)(8))</td>
<td></td>
</tr>
<tr>
<td>8. Complete Privacy Rule and Breach Rule compliance assessments (45 CFR §164.530 and 45 CFR §164.400)</td>
<td></td>
</tr>
<tr>
<td>9. Assess your current insurance coverage (e.g., Cyber Liability, D&amp;O, P&amp;C)</td>
<td></td>
</tr>
<tr>
<td>10. Document and act upon a remediation plan (45 CFR §164.300(a)(1)(ii)(B) and 45 CFR §164.306(a)(1)(ii)(2)(ii) and (4))</td>
<td></td>
</tr>
</tbody>
</table>

One of our portfolio companies was on a tight schedule and the Clearwater team stepped in, completed a high-level assessment, formulated a strategic plan and delivered on the established priorities while minimizing distraction of our workforce.

Stephen Phenneger
Operating Partner, Cressey & Co.

About Clearwater Compliance

Clearwater Compliance, LLC, focuses on helping healthcare organizations and their service providers improve patient safety and the quality of care by assisting them to establish, operationalize and mature their information risk management programs. Led by veteran, C-suite healthcare executives, Clearwater provides comprehensive, by-the-books software and tools, educational events, and expert professional/advisory services for healthcare organizations ranging from major healthcare systems, hospitals, health plans and Fortune 100 companies, to medical practices and healthcare startups. Since 2003, the company has served over 500 organizations.

Register for your complimentary initial consultation today.
Call 800.704.3394
or email sales@clearwatercompliance.com

Clearwatercompliance.com
Key 10-Point Strategic Assessment Features

- Execute a fast, efficient, highly-effective review
- Learn business risks and exposures
- Identify key opportunities for improvement
- Develop a prioritized roadmap for the implementation of solutions
- Strengthen compliance program in critical areas
- Fixed price, so there are no cost surprises
- Board-ready executive-level Findings, Observations & Recommendations presentation
- Engage senior-level executives for optimal results
- Leverage industry-leading assessment/alignment tools
- Review and assess your Cyber Liability, D&O, E&O, and P&C insurance program
- Utilize secure online project work room for ultimate confidentiality
- At your option, complete work under direction of outside counsel
- Receive regular updates for Project Executive and immediate escalation of critical items found

Key 10-Point Strategic Assessment Benefits

- Be Educated: learn and understand all your sources of information risks and liabilities
- Be Confident: utilize the proven approach and methodology used by 100s of organizations
- Be On-Record: exercise good-faith effort and demonstrate seriousness of intent
- Be Assured: Your assessment is being done by healthcare experts
- Be Diligent: exercise the business care and prudence expected of an organization seeking to satisfy a legal requirement
- Be Proactive: receive and execute on a plan of action tailored to your unique business requirements
- Be Clear: De-Mystify a complex process by using a by-the-regulations approach
- Be a Better Decision Maker: Make sound decisions and justify expenditures for safeguards and controls most needed for your organization
- Be Covered: ensure reasonable, appropriate and effective insurance coverage complements risk mitigation actions

**Recommended Action Plan**

**Agree on Privacy, Security & Compliance Vision**

Phase I
2. Formalize the Privacy and Security Risk Management & Governance Program (45 CFR § 164.308(a)(1))

Phase II
5. Train all Members of Your Workforce (45 CFR §164.530(b) and 45 CFR §164.308(a)(5))
6. Complete Privacy Rule and Breach Rule compliance assessments (45 CFR §164.530 and 45 CFR §164.400)
7. Implement a Strong, Proactive Business Associate / Management Program (45 CFR §164.502(e) and 45 CFR §164.308(a)(5))

Phase III
8. Document and act upon a remediation plan
9. Maintain Technical Testing of your Environment (45 CFR § 164.308(a)(5))

**Detailed Findings and Recommendations**

<table>
<thead>
<tr>
<th>Assessment Area</th>
<th>Rating</th>
<th>Key Findings</th>
<th>Key Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Complete a HIPAA Security Risk Analysis (45 CFR §164.308(a)(1)(ii)(A))</td>
<td>Poor</td>
<td>Customer has not conducted a bona fide Risk Analysis that adheres to the 9-step methodology prescribed by HHS. The assets identified on the Clearwater Compliance “ePHI and PHI Asset Inventory” do not appear to be in alignment with the assets identified on the audit documentation provided for review.</td>
<td>Complete and document a bona fide Risk Analysis as soon as reasonably possible. Ensure the organization considers the potential risks and vulnerabilities to all e-PHI that is created, received, maintained, or transmitted. This includes e-PHI in all forms of electronic media (both company owned and BYOD, if permitted), such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmssion media, or portable electronic media.</td>
</tr>
</tbody>
</table>