Protiviti provides trained practitioners who use their extensive data security and privacy experience to help you prepare for HITRUST certification, remediate issues, and manage your risks related to handling personal health information (PHI).

The Health Information Trust Alliance (HITRUST), in collaboration with healthcare, business, technology and information security leaders, established the Common Security Framework (CSF), a certifiable framework that can be used by organizations that participate in and support the healthcare industry. The CSF is the most widely adopted security control framework in the healthcare industry and leverages existing standards including HIPAA, NIST, ISO, PCI, FTC, and COBIT. HITRUST’s CSF Assurance Program leverages the CSF to provide healthcare organizations and their Business Associates with a common approach to managing security assessments and reporting results to internal and external parties.

As an approved CSF Advisor, Protiviti provides trained practitioners to help you prepare for HITRUST certification, remediate issues, and manage risk.

How We Help Companies Succeed

Protiviti provides security strategy, process and implementation services to help improve an organization's information security needs. With regard to HITRUST CSF certification, we have assisted our clients in three key areas:

- **Gap analysis** – We assess the current state of an organization's information security implementation, compare it to the HITRUST CSF standards and define areas in which changes need to be made.

- **Remediation definition and assistance** – We help define a path to attaining CSF compliance, implement the requisite changes and ensure they are providing the operational value expected.

- **Certification support** – As one of a small number of Certified CSF Assessors, Protiviti has the ability to analyze an enterprise environment and prepare documentation the HITRUST Alliance requires for certification.
Our clients tell us that pursuing HITRUST certification provides several benefits to them:

- **Independent verification** – The organization verifies to patients, partners and members that its information security practices are an imperative and meet industry-defined standards.

- **Risk mitigation** – The organization obtains a clear and comprehensive understanding of its information risk exposure using the CSF.

- **Competitive advantage** – Healthcare organizations want business partners that they can trust to retain and protect their patient information.

- **Industry validation** – The organization relies on the collective decisions of an industry group as validation for which security controls are appropriate.

- **Improved partner security** – The CSF provides the benchmark by which an organization can measure Business Associates to quantify the risks of sharing data.

- **Simplified compliance management and reduced audit overlap** – The CSF supports the compliance reviews and documentation of other major security standards, thereby reducing the time spent on overlapping audits.

**Contacts**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Jeff Sanchez</strong></td>
<td><strong>Richard Williams</strong></td>
<td><strong>Scott Laliberte</strong></td>
</tr>
<tr>
<td>+1.213.327.1433</td>
<td>+1.469.374.2469</td>
<td>+1.267.256.8825</td>
</tr>
<tr>
<td><a href="mailto:jeffrey.sanchez@protiviti.com">jeffrey.sanchez@protiviti.com</a></td>
<td><a href="mailto:richard.williams@protiviti.com">richard.williams@protiviti.com</a></td>
<td><a href="mailto:scott.laliberte@protiviti.com">scott.laliberte@protiviti.com</a></td>
</tr>
</tbody>
</table>