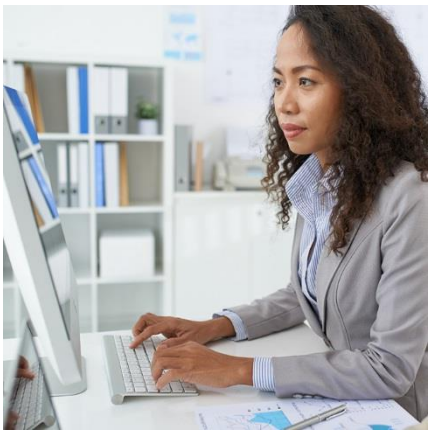
# Healthcare Cyber-Security

## Healthcare Provider Consulting Solutions



Is your organization's information at risk? Data breaches cost the healthcare industry more than $6.2 billion. With the accelerating rise in cyber-attacks and ransomware threats along with significant increases in information access points, is your patient's information safe?

We can help you think through HIPAA security and privacy and Breach needs from both non-technical and technical perspectives including external, internal and wireless penetration testing. We can also perform a mock OCR phase II audit to determine if you are really in compliance. On an ongoing basis we can provide an effective vulnerability management program providing intrusion detection and protection, security information and event management (SIEM), Cyber-Crisis Management Services, Payment Card Industry (PCI) compliance and Forensic investigation if an event occurs.

### Risk Analysis Services

Are you ready for Meaning Use Stage 3 and other federally mandated security requirements? Our risk analysis solution identifies potential risks that could result in a loss of privacy, loss of availability or loss of integrity. We can:

- Review any past security assessments, remediation actions or related initiatives
- Review policies and procedures that reflect required and addressable:
  - Administration safeguards
  - Physical safeguards
  - Technical safeguards
- Conduct a risk analysis in compliance with NIST standards
- Prepare documentation of the observations from all discovery events, and compile recommendations based on HIPAA and HITECH guidelines and best practices for security in IT.

### Penetration Testing

Have you performed an external and internal penetration test, including your wireless network? Penetration testing is the practice of testing a computer system, applications, networks or web application to find vulnerabilities that an attacker could exploit and demonstrate that exploitation.

**Customized Services**

We recognize that not all healthcare providers are the same. Let us customize the cyber-security services and solutions to meet your organization's specific needs.

The process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in, and reporting the findings. The objective of penetration testing is to determine exploitable security weaknesses. This test helps determine an organization's security policy compliance, its employee's security awareness and the organization's ability to identify and respond to security incidents. Actions include:

- Determining the scope of work and type of technical testing services the organization wishes to have performed.
- Performing the following using PCI-QSA-, CISSP-and CISA-certified personnel:
  - Scanning the various devices
  - Demonstrating how an attack would be made by attempting attacks, either bypassing or cracking security mechanisms to gain access
  - Gathering data for analysis
- Performing analysis to determine the traffic being broadcast over the network, including sniffing for user names, passwords and credit card information.
- Providing recommendations to mitigate security vulnerabilities throughout the process and communicate any identified high-risk vulnerability.
- Developing and providing a penetration test report, highlighting matters requiring attention to help prioritize remediation efforts. The report will contain a description of how the team was able to compromise specific systems and data they were able to gather.

**Audit Services**

Are you ready for an OCR or OIG audit? The Phase II audit process requires documented evidence of compliance. We can conduct a mock audit to make sure all the documentation and processes are in place to pass a formal government audit by:

- Sending notification of audit
- Reviewing all specified documentation including:
  - Meaningful Use reports submitted and all support information
  - All security, privacy and breach policies and procedures
  - Security audit information, Security risk assessment, Security remediation plan and Incident reports
- Interviewing staff and other key stakeholders
- Preparing a draft report for review, incorporate all final updates and deliver final report

**Intellectual Capital**

For the past 30 years, Conduent has been an industry leader in healthcare strategic information technology services including planning, operations redesign, systems selections, financial analysis, and Security. Our multidisciplinary approach integrates strategic business equipment/technology planning, with technical knowledge and effective vendor relationships.

### Intrusion Detection and Prevention

Do you have an intrusion prevention system on your network to notify you about a potential risk? The main purpose of an intrusion prevention system is to identify malicious activity, log information about this activity, attempt to block/stop and report it. We have developed a proven, repeatable methodology for the successful deployment and ongoing management of Intrusion Prevention (IPS) security devices by:

- Conducting an architecture review including technical and operational components to determine the right IPS for your organization
- Developing a configuration design to ensure that systems are properly monitored Our security experts then stage the IPS and preload the configuration
- Assisting with the deployment of the IPS
- Providing tuning and ongoing management of the IPS

### Security Information and Event Management (SIEM)

Who is looking at your log files to determine if an event is happening? Our SIEM service provides log aggregation, log monitoring, event analysis and 24x7 response to critical severity events. This service leverages commercial SIEM tools as well as custom tools and methodologies to determine important events and then correlate, validate and alert on those events by:

- Providing log aggregation for the most common systems, firewalls, email appliances, web filtering, domain controllers, servers, anti-virus and IPS devices. Logs are collected via an on-site collector running in your environment. Logs are securely tunneled to Conduent™ Healthcare Provider Solutions colocation facility and retained for a minimum of 12 months.
- Reviewing all significant events on a daily basis by a Senior Security Analyst. A written report including findings and recommendations are delivered weekly to the client.
- Escalating any security events that need immediate attention through automated tools to our Security experts 24x7x365. Events that warrant immediate attention, such as high or critical severity IPS events that are detected but are not automatically blocked by policy, will be automatically identified and alerted to our security experts anytime day or night. If our initial investigation demonstrates the need for immediate action, we will notify your team members.

## Cyber-Crisis Management Services

Are you prepared to deal with the national news and your own stakeholders regarding a cyber-event at your organization? Do you have a formal cyber-crisis response plan? We can:

- Conduct a crisis audit including a communications risk assessment, team interviews, discussion of various crisis scenarios
- Develop a cyber-crisis response plan including delineation of crisis management team participants and roles, communications tools, dark site and other digital recommendations and when to activate them
- Conduct training for executives focusing on practices to manage reputation, key audiences and message delivery, stakeholder matrix, minute-by-minute checklist, call trees and templates, how to take control in a crisis, ways to deliver proactive messages and how to strengthen relationships in advance of the crisis
- Conduct a table top drill utilizing scenarios to test various aspects of the response plan. The test scenarios simulate events in reaction to the crisis, some unanticipated issues, media response, etc.
- Utilize the results of the test to update the response plan

## Payment Card Industry (PCI) Audit Services

Are you storing Credit Card information in your systems? Our PCI Qualified Security Assessor (QSA) will conduct a PCI audit to determine your compliance with the Payment Card Industry Data Security Standard (PCI DSS) requirements.

- Conduct a PCI DSS gap analysis
- Prepare a report for review that includes a recommended remediation plan
- Conduct the PCI DSS audit and provided Report on Compliance (ROC)

### About Conduent

Conduent is the world's largest provider of diversified business process services with leading capabilities in transaction processing, automation, analytics and constituent experience. We work with both government and commercial customers in assisting them to deliver quality services to the people they serve.

We manage interactions with patients and the insured for a significant portion of the U.S. healthcare industry. We're the customer interface for large segments of the technology industry. And, we're the operational and processing partner of choice for public transportation systems around the world.

Whether it's digital payments, claims processing, benefit administration, automated tolling, customer care or distributed learning – Conduent manages and modernizes these interactions to create value for both our clients and their constituents. Learn more at **www.conduent.com/caremanagement**.

**Contact Us**

**hcprovider@conduent.com**

CONDUENT

© 2017 Conduent Business Services, LLC. All rights reserved. Conduent™ and Conduent Design™ are trademarks of Conduent Business Services, LLC in the United States and/or other countries. BR19760C