Brochure

Healthcare Cybersecurity Services

Is your organization's information at risk?

Data breaches cost the healthcare industry more than $6 billion annually. With the accelerating rise in cyberattacks and ransomware threats along with significant increases in information access points, is your patient information safe?

We can help you think through HIPAA security and privacy from technical and nontechnical perspectives including external, internal and wireless penetration testing. We can also perform a mock OCR audit to determine your compliance. Our vulnerability management program provides intrusion detection and prevention, security information and event management (SIEM), crisis management, Payment Card Industry (PCI) compliance and forensic investigation.

Risk analysis

Is your organization prepared to meet Meaningful Use Stage 3 and other federally mandated security requirements? Our risk analysis solution identifies potential risks that could result in 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, physical and technical safeguards
- Conduct a risk analysis in compliance with NIST standards
- Prepare documentation of the observations from all discovery events
- Compile recommendations based on HIPAA and HITECH guidelines and bestpractices for IT security

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 and/or web applications to find vulnerabilities through ethical hacking.

The process includes gathering information about the target before the test (reconnaissance), identifying possible entry points including the use of social engineering, 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 vulnerabilities

Trusted partner for your **Digital Journey**

Atos

OCR mock audit

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 supporting information
  - All security, privacy and breach policies and procedures
  - Security audit information
  - Security risk assessment
  - Security remediation plan
  - Incident reports
- Interviewing staff and other key stakeholders
- Preparing a draft report for review, incorporate all final updates and deliver final report

Intrusion detection and prevention

Do you have an intrusion prevention system on your network to notify you about potential risks? The main purpose of an intrusion prevention system is to identify malicious activity, log information about this activity and attempt to block/stop and report it. We have developed a proven, repeatable methodology for the successful deployment and ongoing management of intrusion prevention security (IPS) 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
- Staging the IPS and preloading 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 an Atos Digital Health Solutions Consulting 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 will be automatically identified and alerted to our security experts anytime day or night. Such events may include high or critical severity IPS events that are detected but not automatically blocked by policy. If our initial investigation demonstrates the need for immediate action, we will notify your team members.

Crisis management

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

- Conduct a crisis audit including a communications risk assessment, team interviews and 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, 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 tabletop drill utilizing scenarios to test various aspects of the response plan such as reactions, responses and unanticipated issues
- Utilize the results of the test to update the response plan

Payment Card Industry (PCI) audit

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 provide Report on Compliance (ROC)

Customized services

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

Intellectual capital

Atos has been an industry leader in cybersecurity providing the cyber security for the Olympic Games. Atos is a respected leader in healthcare strategic information technology services including planning, operations redesign, systems selections, contract negotiation and system implementation for all major health IT vendors, financial analysis and security. Our multidisciplinary approach integrates strategic business equipment/technology planning with technical knowledge and effective vendor relationships.

Did you know?

Atos is one of the top 5 IT services providers in the United States and with more than 300 healthcare organizations supported, is focused on becoming the U.S. leader in healthcare digital transformation. With more than 2,500 healthcare associates, 600 healthcare technology consultants and more than 80 clinicians in our Digital Health Solutions Consulting organization, the experts at Atos can help you drive the value of health.

About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 73 countries and annual revenue of around € 13 billion. European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, the Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us
atos.net
ascent.atos.net

Let's start a discussion together

info.na@atos.net