A Holistic Approach to Security & Privacy Compliance in Healthcare:  
*Prepared for Today and Tomorrow*

Electronic healthcare initiatives, including broad-based adoption of electronic health records (EHRs), are heralded as the gateway to improved operational efficiency, consumer empowerment and expanded collaboration – with the ultimate goal of improving outcomes while driving down costs. At the same time, however, the digitization of healthcare presents complex new privacy and security risks, and expanded compliance challenges, as legislative and regulatory bodies seek to prevent breaches. Healthcare providers seek solutions that will enable them to confidently leverage new technologies and facilitate compliance by protecting data and controlling and monitoring access at every level of the environment within and beyond the organization – from storage to the network to the presentation layer, accessed via a desktop, laptop or, increasingly, a mobile device.

**New Ways of Communicating Drive New Risks and Requirements**

Responsible data sharing and data management across the IT ecosystem are essential to the success of an electronic healthcare initiative. That ecosystem continues to grow almost daily as providers collaborate with an expanding chain of partners and business associates, and as consumers and providers seek new ways to interact beyond the walls of the healthcare facility – via e-mail, portals, short message service (SMS), social media and more. Secure data storage and transmission, knowledge management and collaboration are essential to enabling these vital new interaction venues.

As the healthcare IT environment grows more complex, so do the compliance requirements designed to ensure privacy and security of health-related data. Among its many provisions, the Health Insurance Portability and Accountability Act (HIPAA) laid the foundation for ensuring the security and privacy of electronic health data. Its impact has been magnified in the last year through stricter enforcement and the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), part of the American Recovery and Reinvestment Act (ARRA) of 2009. HITECH extends complete privacy and security provisions of HIPAA to business associates of covered entities. In addition, it imposes new notification requirements on covered entities, business associates, vendors of personal health records (PHRs) and related entities if a breach of unsecured protected health information (PHI) occurs.

---

**Environmental Assessment**

Providers should begin their compliance journey with an assessment of their environment:

- **Authentication**: Who is accessing each system? What is their role?
- **Authorization**: What rights do authenticated users have? Are these tied to a single directory for automated management of role changes?
- **Access control**: Based on user identity and rights, what content can user access?
- **Audit**: Has user behavior contravened policy?
- **Encryption**: Is data encrypted in storage and in transit?

The average organizational cost of a data breach increased nearly 2 percent from $6.65 million in 2008 to $6.75 million in 2009.

_Ponemon Institute, U.S. Costs of a Data Breach, 2009_
In the wake of HITECH, providers face increased financial and reputational risk in the event of a breach as well as a heavier compliance burden. In addition, they must be prepared to respond to increasingly stringent state mandates as well as non-healthcare-specific privacy requirements, such as Payment Card Industry – Data Security Standards. Flexibility is, therefore, essential in providers’ approach to security and privacy compliance.

A Holistic Approach to Security and Privacy Compliance

Since there are so many regulatory and compliance requirements, it becomes arduous to try and tackle each one separately. Taking a holistic approach based on a provider’s appetite for mitigating and/or accepting risk is the best starting point.

Oracle provides an unmatched end-to-end solution set for data security and privacy compliance that gives providers the confidence that they are protecting their data within and far beyond the walls of their organization. Eclipsing the capabilities of point solutions, Oracle’s holistic approach to security and privacy compliance enables:

- Protection of data through its entire lifecycle from inception through transport, storage and destruction – within and beyond an organization – through comprehensive role, identity and access management in conjunction with robust encryption, data masking and data control capabilities
- Data protection at every level of the environment – including the operating system; virtualization layer; storage platform; and the middleware, application, and presentation layers
- Flexible role management and automation of identity management, using authoritative applications to ensure all changes in a user’s job function or role are reflected instantly in their identity
- A centralized and externalized access control infrastructure across all applications
- Visibility into who accessed what data and when as well as the ability to track the flow of data across and beyond the enterprise

End-to-End Solutions

Managing the healthcare data lifecycle holistically goes a long way toward ensuring compliance today and into the future. Oracle’s industry-leading solutions for data protection and management, access and identity management, as well as governance, risk and compliance are there to support providers at every point along the way. Oracle helps providers create a strong, yet flexible, foundation for ensuring the privacy and protection of sensitive data, giving them the confidence to fully explore the potential of digital medicine to improve care delivery and reduce costs.

CONTACT US

To learn more, call us at +1.800.633.0738 to speak to an Oracle representative or visit http://www.oracle.com/goto/healthcare.com. Outside North America, visit http://www.oracle.com/us/corporate/contact/index.htm to find the phone number for your local Oracle office.