System and Technology Integrity: Achieving "Best In Class" Capabilities

March 2016

As the industry leader in release of information services and a prominent vendor of health information technology and solutions, including audit management, the integrity of our information technology (IT) security and compliance platform is crucial to our business operations and reputation. Our customers depend on us to ensure HIPAA compliance and the confidentiality, security, and accuracy of protected health information (PHI) that is transmitted through our release of information services.

"Best in Class" IT Capabilities

In an effort to achieve "Best in Class" IT capabilities, we've gone above and beyond what's required to meet security and compliance standards. By identifying and implementing annual baseline goals and service objectives, we have raised the bar on the following dimensions of our IT capabilities:

- Security/Compliance
- Network/Connectivity
- IT Infrastructure
- IT Operations
- Backup/Disaster Recovery
- Organization
- Change Management

CIOX Health has invested in several projects designed to elevate our security reputation and provide our customers with peace of mind that the PHI they have entrusted with us is safe no matter what. This distinguishes us as a forward-thinking health information technology company with a reputation for investing in the reinforcement of our IT infrastructure whether through measures performed by our internal security team or sanctioned by us through third-party firms.

Internal Security Audits

System Vulnerabilities

Our Security Team is actively involved in performing the following internal audits and assessements of our security platform and IT infrastructure:

- Regularly scheduled vulnerability scans of all systems for potential threats.
- Rule sets and scans that correlate security alerts and events.
- Diagnosis and recommendations of security fixes that should be made to allow for intrusion detection and prevention monitors on external firewalls.

Performed on an annual basis or more, these audits provide a vulnerability threshold for our internal programs so that additional safeguards can be created and implemented to protect the internal systems that our associates utilize to securely transmit PHI on a daily basis.

Disaster Recovery Plan

During times of disaster or distress, it is important that our customers know that we have a plan and processes in place to guarantee the recovery of PHI. Our Disaster Recovery Plan identifies critical levels of compromised information and provides for a process hierarchy in notifying our customers of the compromise and backup procedures to reduce any threats to the security of this information. As part of our security commitment and recovery objective, we complete semiannual audits on our data and application backup and restoration capabilities. Our audit process identified new opportunities for us to enhance our IT infrastructure even more with the addition of intrusion detection blades to improve monitoring and alerting of network activity, completed failover testing for select database servers allowing for recovery of all Oracle® databases, and an internal vulnerability scan server. We will continue to build out our disaster recovery infrastructure to further solidify our business continuity which includes our associates, processes, and technology as well as back end processes in the event we are faced with an unplanned risk to our stored information or application systems.

Third-Party Security Audits

SSAE 16 SOC Report

Statement on Standards for Attestations Engagements NO. 16 (SSAE 16) Reporting on Controls at a Service Organization is a widely recognized auditing standard. In 2012, the security and compliance of our IT infrastructure and operational processes completed the SSAE 16 Type 2 examination with the issuance of a final Type 2 SSAE 16 Report. SSAE 16, Type 2 examination indicates that selected CIOX Health Release of Information processes, procedures, and controls have been formally evaluated and tested by an independent accounting and auditing firm. The examination included our controls related to release of information service delivery, security monitoring, change management, support services, backup and environmental controls, logical and physical access. The Type 2 Report not only includes our description of controls, but also includes detailed testing of the design and operating effectiveness of the identified controls.

SSAE 16 is designated by the U.S. Securities and Exchange Commission (SEC) as an acceptable method for a user organization's management to obtain assurance about service organization internal controls without conducting separate assessments. With the issuance of a SSAE 16 report, we offer our customers yet another demonstration of how the secure and compliant exchange of protected health information is a top priority along with third-party verification regarding the operating effectiveness of our IT capabilities.

In today's technology-focused society, health information technology providers like us must demonstrate adequate controls and safeguards when we host or process customer data. Although a significant financial investment, SSAE 16 audit is evidence that CIOX Health is committed to providing the most secure and efficient platform for customers and will leverage this action as part of our initiative to provide technology that is a "Best in Class" approach to the industry.

Penetration Testing

We complete annual penetration testing of our information technology security platform which includes an invaluable technique that evaluates the security of a network by simulating an attack from a source and providing an active analysis of our system by a third party security firm. The penetration test involves an audit and assessment of the following security safeguards we have in place:

- Audit and intrusion attempt of the physical facility.
- Discovery of any potential attack vectors or services that could be used for potential compromise of our network hosts and information assets.
- Determination of the vulnerabilities and threats that affect the data processing environment in terms of confidentiality, integrity and availability.
- Identification and evaluation of existing security controls and policies.
- Assessment of security infrastructure for attack visibility and derived information value.

We will continually make significant additions and improvements to the security systems and controls in place. As a result of the third-party findings identified in the previous year's audit of the penetration testing, we have implemented a consistent practice of vulnerability assessment and remediation including:

- The implementation of a company-wide security awareness training program.
- Implementation of security information and event management (SIEM).
- Updated security policies and procedures.
- Increased security perimeter controls by deploying intrusion prevention in the perimeter and core of our security architecture.

Although not required, penetration testing is a direct reflection of the aggressive approach and consistent actions we have taken to enhance our security platform. Actions that, based on our penetration test results and findings, have reduced the level of risk within our organization and resulted in significant improvements to our security posture, architecture, and operational

procedures. Our team of security experts will continue to work non-stop to provide an even deeper level of security and further strengthen our technology platform so that we continue to receive positive penetration test results.

Financial Transaction Security Standards

In an effort to protect the financial data of our customers and requesters, we are in full compliance with the PCI Data Security Standard (PCI DDS). The PCI DDS represents a common set of industry tools and measurements required by entities like CIOX Health that accept payment via credit card.

To ensure the safe handling of sensitive information, compliance with the PCI DDS is an ongoing process that involves adhering to 12 requirements for security management, polices, procedures, network architecture, software design and other critical protective measures. To meet the requirements, we work with our financial banking vendor and utilize the tools for compliance offered by the PCI Security Standards Council comprised of the five founding payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa.

CIOX Health is doing its part to ensure that customer credit card information is safe and secure throughout every transaction. We thoroughly assess our financial transaction operations, fix any vulnerabilities that are identified, and make the required reports to our banking institution and card brands we do business with so that our customers have confidence that they are protected against the risk of data breaches.

Going a Step Beyond

Increasing both the security systems and the security awareness within the company is a top priority for CIOX Health. While neither the SSAE 16 examination nor penetration testing is required, we have and will continue to go an important step further by continuously giving our IT security system a thorough and complete evaluation so that we can identify areas of improvement and potential threat risks. We are highly committed to the confidentiality and security of PHI and the satisfaction of our customers. This proactive direction allows us to incorporate operational efficiencies that will further strengthen the security of our system and reduce the threat that the secure, compliant transfer of PHI could be compromised.

Our Commitment to Meaningful Use Initiatives

As part of our efforts to assist our customers with meeting the Meaningful Use requirement related to responding to requests for an electronic copy of medical records within three business days, our release of information application, eSmartlog℠, has received the federal government's "meaningful use" stamp of approval by earning inpatient and ambulatory electronic health record module certification.