[DATA SYSTEM]: Privacy and Security

October 2013

Data Storage, Privacy, and Security

Following is a description of the technical and physical safeguards [data system operator] uses to protect the privacy and security of the data in [data system]. It is worth noting here that human systems must still develop and enforce relevant policies and procedures like HIPAA Business Associate Agreements, authorization and de-activation of users, determination and approval of role-based and user-specific permissions, and initial and recurring user training in privacy and security. [Data intermediary] and [data system operator] can be of assistance with these policies and procedures.

Regulatory Compliance

Privacy of all person-level records will be maintained by utilizing two-factor authentication and the encryption (Advanced Encryption Standard (AES) 256) of all personally identifiable information (PII) and electronic personal health information (ePHI) while traveling in the public network and at rest within the Oracle database. PII and ePHI are not synonymous terms, but the risks and safeguards are similar and they will be treated together here except for provisions specific to HIPAA regulations.

[Data system operator] utilizes automation tools to identify assets in the Virtual Data Center (VDC) and find any vulnerabilities, misconfigurations and malware exposure that may put ePHI at risk.

Contextual information into the level of risk posed by each vulnerability will help prioritize remediation and mitigation to ensure PII/ePHI is truly secure. [Data system operator] maintains HIPAA / HITECH compliance utilizing these "always on" tools. [Data system operator] also conducts internal penetration testing to verify all configurations in the VDC. [Data system operator] can:

- Detect PII/ePHI data in environment.
- Get top-down visibility of risk to assets and business operations, enabling us to organize and prioritize assets and quickly focus on the items that pose the greatest risk.
- Get a clear map of the real risk posed to ePHI by the identified vulnerabilities across the VDC landscape.
- Combined with Common Vulnerability Scoring System (CVSS) base scores, temporal scoring, environmental considerations (e.g., any mitigating controls in place), and asset criticality for risk classification.
- Take inventory of systems, services, and installed applications using the latest fingerprinting technologies.
- Detect the presence of unauthorized software on information systems and notify designated officials through alerts on an automated mechanism.
- Perform comprehensive unified vulnerability scanning of all vital systems including networks, operating systems, web applications, databases, enterprise applications, and custom applications.
- Generate detailed reports combined with role-based access controls
- Compare the results of vulnerability scans over time to determine trends in information system vulnerabilities through an automated mechanism.

- Audit users and groups on systems.
- Set-up automated monitoring access controls (including adherence to policies for role- based access) to validate enforcement of access restrictions.
- Test the efficiency of access control systems and policies

[Data system operator]'s data center is ruled under the following FISMA policies:

- Access Control
- Awareness and Training
- Audit Accountability
- Contingency Plans
- Incident Response Policy
- Risk Assessment Policy
- Physical and Environmental Policy
- Planning Policy and Procedures
- Configuration Management Plan
- Information Security Policy
- Identification and Authentication Policy
- Systems Communication Policy and Procedures

These policies along with a system security plan are available upon request.

Administrative Safeguards

[Data system operator] requires that all personnel complete all training requirements outlined by the training manager of the contract, consistent with the methodology of National Institute of Standards and Technology (NIST) Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, which applies to all employees as well as remote researchers and collaborators working on [data system operator] projects. The component must include awareness activities, basics and literacy training activities for general users, and role-based training for specialized users. In accordance with the Code of Federal Regulations, Title 5, Part 930, Subpart C, Section 930.301 (a)(1), [data system operator] requires that each user engage in annual basics and refresher training to sustain such access.

In addition, training is conducted on HIPAA Awareness, HIPAA Privacy Rule, which applies to safeguarding Protected Health Information (PHI) in oral or written form and HIPAA Security Rule, which apply to electronically stored or transmitted PHI and technical protections for electronic Protected Health Information (ePHI).

Physical Safeguards

Public access to [data system operator]'s data center is forbidden. Only personnel with the appropriate clearance are allowed in the server areas of data center, and the two-person rule always applies. Access to the data center is monitored by a security system and security cameras and controlled by two independent security doors with both cypher and magnetic card locks. Two independent monitoring companies (ADT and Protection One) actively monitor data center at all times.

Technical Safeguards

The data system has been designed as a redundant system with 24/7 availability with 99.9% up time. The system contains two CISCO ASA firewall systems, one Proxy Firewall, redundant application servers on a de-militarized zone (DMZ), and a redundant Oracle database. Compliance patching has been done utilizing IBM software BigFix that constantly monitors for FISMA compliance. Following a recent purchase, we are in the process of installing and configuring IBM VMware vCloud Suite Enterprise with Health Insurance Portability & Accountability Act (HIPAA) and Health Information Technology for Economic & Clinical Health (HITECH).

Compliance and Configuration Management

The Public Reports interface (described in Section V below) and aggregate data queried through it are freely accessible by anyone with an internet connection and web browser. (Data is suppressed where cell size is lower than 30.) Login to the secure area (Private Reports and the person- and family-level dashboard) person-level record requires two-part authentication and user acceptance of terms and penalties for violating those terms. (Two-part authentication requires *knowing* the username and password and *having* a one-time use code or "token" generated via an app called WiKID.) All system use and edits are logged.

[Data system operator]'s system utilizes security appliances that can be configured to accept connections from the customer's domain only. Hard identification tokens will be used as required by the customer. The system will accept connections only from authorized users.

[Data system operator] systems utilize programming controls that obscure the feedback of authentication information. All information traveling via the public network is encrypted using Federal Information Processing Standard (FIPS) compliant encryption algorithms.

Breach Notification

An incident will be considered any physical, technical or personal activity or event that increases the (HIPAA) Covered Entity's risk to inappropriate or unauthorized use or disclosure of PHI or causes the Covered Entity to be considered non-compliant with the Administrative Simplification provisions of HIPAA/HITECH as determined by the Department of Health and Human Services. Notification will be made by Business Associate to Covered Entity by telephone or secure fax of any HIPAA/HITECH Electronic Transactions and Code Sets, Privacy, Security or Standard Identifier Incident, or Use or Disclosure of PHI not provided for by this BAA.

A written report of the incident, submitted to Covered Entity within ten (10) business days after initial notification, will document specifics surrounding the incident, what mitigation procedures were implemented to lessen the impact of the incident and what processes have been established to prevent the incident from occurring in the future (reasonable and appropriate safeguards).
This report should be documented as a letter.

Similar criteria and procedures are used to define and handle an "incident" involving data contributed by agencies not considered to be a Covered Entity under HIPAA regulations. In general, HIPAA sets the

higher privacy and security standard, and procedures that are HIPAA- compliant exceed FERPA requirements.

Hosting

[Data system] could be hosted anywhere, but [data system operator] is the currently-contracted host. [Data system operator]'s Data Center is specifically designed to receive and process, display, store, and transmit data in an ultra-secure environment. To be able to host data and applications for federal customers, [data system operator] has met all Federal Information Security Management Act (FISMA) requirements and has earned DoD Information Assurance Certification and Accreditation Process (DIACAP) certifications. [Data system operator]'s systems are Health Insurance Portability and Accountability Act (HIPAA) compliant, Health Information Technology for Economic and Clinical Health (HITECH) compliant, and Family Educational Rights and Privacy Act (FERPA) compliant.

[Data system operator] has the processes in place to handle large databases up to 42 terabytes. The web server utilizes an X.509 PKI Server Certificate and has 128-bit Transport Layer Security (TLS) version 1.1 (or SSL version 3.0) enabled at all times. All connections are via https (128-bit encrypted SSL) over port 443. All encryption algorithms are National Institute of Standards and Technology (NIST) / Federal Information Processing Standards (FIPS) certified.

[Data system operator] provides 99.99% uptime, offers High Availability and Fault Tolerance, and is monitored 24/7. If a total utility power outage occurs, all data centers' power systems are designed to run uninterrupted, with every server receiving conditioned Uninterruptible Power Supply (UPS). If an extended utility power outage occurs, [data system operator]'s routinely tested, on-site generator can run indefinitely.

Permissions and Consent

To date, users have been authorized and parent data-sharing consent has been granted at the point of service and documented on paper, and so far this method has been manageable. But many partners beyond the [collective impact initiative] will sooner rather than later need to see data at the record level or in aggregate. So in Spring 2013 [data intermediary] and [collective impact initiative] identified the need for a much more robust way of controlling data sharing and views.

An electronic user management module has already been built and is restricting or enabling data views based upon privileges granted to the user. [Role 1 users] might be granted privileges to see identified data for 7th graders at XXX Middle School, while the [Role 2 users] might have privileges to see identified data for all students at the schools it serves, and the [Role 3 users] might have privileges to see data only in aggregate. Someone authorized to access Private Reports but not PII would see only an aggregate report of, say, what percent of African-American children passed the third-grade reading assessment. But someone with both sets rights of rights could click on that cell in the table to generate a list of those actual children. The user management module includes a "User Type Template" feature that could capture, store, and apply standardized user profiles/data access levels for the five user types summarizes in Section 2.2 of the Requirements Specification. A screenshot of the user management area is included as Appendix 5.

A separate electronic consent module in development now will allow the person (or parent) whom the data is about to select which service providers (or categories of service providers) may see

what indicators (or categories of indicators). That parent might enable the [role 1 user] working with her/his child to see that child's school data and out-of-school time program participation data, but not (when eventually connected) the child's mental health data or the parent's employment data. By creating a central database of consent information, a person or authorized proxy (parent/guardian) may grant or revoke data-sharing or data-view privileges at any point of service at any point in time.

Together the user management module and the consent module will maximize the likelihood that a user sees only data that s/he has been authorized by both the parent/resident and the partner agency(ies). Again, the human systems are critical. Care must be taken that an agency cannot/does not authorize one of its' own staff to view another agency's data. Informed consent is a process and series of decisions over time, not a single decision. Helping people understand their rights and the risks and benefits of consent is not easy when educational level, worldview, language, and data and tech literacy vary so greatly.