State of Rhode Island and Providence Plantations

Department of Administration
BUREAU OF AUDITS
One Capitol Hill
Providence, RI 02908-5889
TEL #: (401) 574-8170

April 22, 2015

Ms. Deborah Dawson
Associate Director
Division of Human Resources
One Capitol Hill
Providence, RI 02908

Mr. Thom Guertin
Chief Digital Officer
Office of Digital Excellence
One Capitol Hill
Providence, RI 02908

Dear Ms. Dawson and Mr. Guertin:

At your request the Bureau of Audits conducted a risk analysis and policy gap assessment designed to fulfil the requirements of §164.308(a)(1)(ii)(A) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The Security Rule requires that covered entities, "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity."

The risk assessment uses the risk factors of threats, vulnerabilities, operational impact and likelihood of occurrence to help management assess the current security risks. The gap analysis measures the existing Office of Employee Benefits HIPAA security policies against emerging risk and industry best practices. This gap analysis is intended to provide management with a basis to improve existing security posture and compliance with HIPAA policies, procedures, and practices.

Rhode Island General Laws (RIGL) §35-7-3(b), entitled *Audits performed by the bureau of audits*, state that, "Within twenty (20) days following the date of issuance of the final audit report, the head of the department, agency or private entity audited shall respond in writing to each recommendation made in the final audit report." Pursuant to this statute, the Bureau may follow up regarding the corrective actions completed to address the weakness identified in this report within one year following the date of issuance.

Also, in compliance with RIGL §35-7 the details of the security weaknesses and corrective actions identified have been removed from this public report.

We would like to express our sincere appreciation to the staffs of the Office of Employee Benefits, Legal Division, and Division of Information Technology for the cooperation and courtesy extended to the members of our team during the course of this audit.

Respectfully yours,

Dorothy Z. Pascale, CPA, CFF
Chief

c--Internal Audit Advisory Group
Michael DiBiase, Director, Department of Administration
Michael Sliger, Esq., Legal Counsel, Division of Legal Services
Paul Cofone, Administrator, Office of Employee Benefits
Dennis Hoyle, Auditor General
Honorable Daniel DaPonte, Chairperson, Senate Committee on Finance
Honorable Raymond Gallison, Chairperson, House Finance Committee

Table of Contents

Security Rule Risk Assessment Overview

Executive Summary

The Bureau's detailed conclusions are summarized in the attached *Risk-Threat Matrix* and *Policy and Procedure Gap Analysis.*

- The Risk-Threat Matrix assigns risk ratings based on the likelihood and impact of threat occurrence. The matrix considers existing controls and recommends actions to minimize risk.

- The Policy and Procedure Gap Analysis was conducted to provide an overview of OEB and Division of Information Technology (DoIT), current policies and procedures, as well as identify policies and procedures that should be developed and/or modified to comply with the HIPAA Security Rule Requirements.

The HHS HIPAA Security Series contains 42 standards across administrative, physical, and technical safeguards. Of the 42 standards, the Bureau has suggested action for the OEB regarding 26 standards to improve current security safeguards. However, there were noted security measures in place for all except three standards.

Background

Hybrid Entity

The Department of Administration (DOA) determined that it meets the criteria of a hybrid entity as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) laws and regulations. As a hybrid entity, DOA is a single legal entity whose business activities include both HIPAA-covered and non-covered functions. Components that perform covered functions are "health care components" and are subject to HIPAA, while the remainder of DOA is not subject to the Act. By designating certain divisions and offices as HIPAA-covered health care components, DOA limits HIPAA compliance obligations to covered units, i.e., the OEB. Therefore, in compliance with HIPAA, the OEB is required to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of ePHI.

Security Standards

The HIPAA security standards were developed for two primary purposes:

- Implement appropriate security safeguards to protect electronic health care information.

- Protect an individual's health information while permitting appropriate access and use of said data.

HIPAA required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published guidance known as the *HIPAA Privacy Rule* and the *HIPAA Security Rule.*

- The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information.

- The Security Rule, or Security Standards for the Protection of Electronic Protected Health Information, establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that must be implemented to secure electronic protected health information (ePHI).

Further, 45 CFR§ 164.308(a) (1)(ii)(A) *Security Risk Analysis* mandates covered entities to:

> *Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity.*

Methodology and Work Performed:

The risk assessment was performed using the following techniques:

- Questionnaires concerning the management and operational controls used for the IT system
- On-site interviews with management personnel
- Personal observation
- Document review

Threat Risk Matrix Magnitude of Impact Definitions

To determine the impact of identified risks, we used the *Magnitude of Impact Definitions* by the National Institute of Standards and Technology (NIST) Special Publication 800-30. These

definitions describe the consequences of not properly safeguarding ePHI in terms of high, medium, and low impacts. Detail definitions are quoted below:

- High—Exercise of the vulnerability: (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.

- Medium—Exercise of the vulnerability: (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.

- Low—Exercise of the vulnerability: (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Security Risk Assessment and Gap Analysis Structure

We structured this security risk assessment and gap analysis based on the HHS HIPAA Security Series which is divided into the categories of administrative, physical, and technical safeguards as defined below:

- Administrative safeguards: The administrative functions that should be implemented to meet the security standards.
- Physical safeguards: The mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion.

- Technical safeguards: The automated processes used to protect data and control access to data.

The above security safeguards are classified into required and addressable standards:

- **Required standards**: Must implement policies and/or procedures that meet the implementation specification.

- **Addressable standards**: Assess whether it is a reasonable and appropriate safeguard considering the entity's existing environment.[1]

[1] U.S. Department of Health and Human Services HIPAA Security Series Chapter 1 "Security 101 for Covered Entities."

The decisions regarding security measures to implement are dependent upon on a variety of factors, including:

- Identified vulnerabilities
- Current security measures
- Cost-benefit analysis

Additionally, the Bureau developed a Threat- Risk Matrix and Policy Gap Analysis to identify risk and prioritize a risk management mitigation plan. The following steps were included in the completion of the Threat-Risk Matrix:

- Threat identification
- Vulnerability identification
- Review of existing mitigating controls
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendation

Objectives

Our objective was to perform an assessment of potential risks and vulnerabilities to the confidentiality,[2] integrity,[3] and availability[4] of electronic protected health information (ePHI) held by the Department of Administration, Office of Employee Benefits (OEB). The risk assessment will be provided to management as a tool to assist with improving the control environment. To accomplish our objectives, we prepared this report and addendum which includes the:

1. Threat risk matrix
2. Policy and procedure gap analysis
3. Security standards

[2] **Confidentiality** is "the property that data or information is not made available or disclosed to unauthorized persons or processes." NIST 800-66 Revision 1 *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Rule.*

[3] **Integrity** is "the property that data or information have not been altered or destroyed in an unauthorized manner." NIST 800-66 Revision 1 *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Rule.*

[4] **Availability** is "the property that data or information is accessible and useable upon demand by an authorized person." NIST 800-66 Revision 1 *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Rule.*