State of Rhode Island and Providence Plantations

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

May 20, 2015

Brigadier General Rick Baccus
Administrator
Rhode Island Veterans Home
480 Metacom Ave
Bristol, RI 02809

Dear General Baccus:

At your request, the Bureau of Audits conducted a risk analysis designed to fulfil the requirements of CFR §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.*

Rhode Island General Laws (RIGL) §35-7-3(b), entitled *Audits performed by the bureau of audits*, states, "… Within one year following the date on which the audit report was issued, the bureau of audits may perform a follow-up audit for the purpose of determining whether the department, agency or private entity has implemented, in an efficient and effective manner, its plan of action for the recommendations proposed in the audit report.." Pursuant to this statute, the Bureau will follow up regarding the corrective actions completed to address the weakness identified in this report.

Also, in compliance with RIGL §35-7-15, *Audits of information security systems*, the details regarding the weaknesses and corrective actions have been removed from this public document.

We would like to express our sincere appreciation to the staffs of the Division of Information Technology and the Rhode Island Veterans Home for the cooperation and courtesy extended to the members of our audit team during the course of this engagement.

Respectfully yours,

Dorothy Z. Pascale, CPA, CFF
Chief

c—Internal Audit Advisory Group
Melba Depeña Affigne, Director, Department of Human Services
Thom Guertin, Chief Digital Officer, Office of Digital Excellence/Division of Information Technology
Dennis Hoyle, Auditor General
Honorable Daniel DaPonte, Chairperson, Senate Committee on Finance
Honorable Raymond Gallison, Chairperson, House Finance Committee

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 a 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 Rhode Island Veterans Home (RIVH) 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 RIVH security posture would be strengthened by addressing recommended control issues identified on the Threat Risk Matrix. The HHS HIPAA Security Series contains 42 standards across administrative, physical, and technical safeguards. After conducting a risk assessment, 34 potential risks were identified relating to the HIPAA Security standards. We noted security measure improvements, which are summarized in the chart below:

Risk Matrix Priority	Total # of Risks	Total # of Issues	Total # Compliant
High	0	0	0
Medium	6	6	0
Low	28	16	12
Total	34	22	12

The nature of these concerns can easily be addressed by modifying policy and procedure, and implementing a security awareness training program.

We performed a policy and procedure gap analysis to identify areas in policy and procedure that would further strengthen the RIVH security posture. The Office of Information Technology and Executive Office of Health and Human Services[1] have policy and procedure that do support the Rhode Island Veterans Home HIPAA security posture. However, we identified HIPAA concerns specific to the Rhode Island Veterans Home that are not

[1] Executive Office of Health and Human Services includes the Department of Human Services, the Division of Veterans Affairs, and the Rhode Island Veterans Home.

addressed in policy and procedure. We used the HIPAA Standards categorization to identify gaps in policy and procedure as "required" or as "addressable." The chart below summarizes our findings.

Policy Gap	Total # of Standards	Total # of Issues	Total # of Compliant
Required	16	12	4
Addressable	15	10	5
Total	31	20	11

The nature of these items would be addressed primarily by implementing policy and procedure specific to the Veterans Home security requirements.

The Bureau's detailed conclusions are summarized in the attached *Risk-Threat Matrix* and *Policy and Procedure Gap Analysis.* The details of these sections have been removed from the public document in accordance with RIGL §35-7-15.

Introduction

At your request, The Bureau of Audits conducted a risk analysis designed to fulfill the requirements of CFR §164.308(a)(1)(ii)(A) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule for the Rhode Island Veterans Home (RIVH). 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.*

Background

The HIPAA Security Rule standards were developed for two primary purposes:

- Provide a safeguard over an individual's health information.
- Permit the appropriate access and use of that information.

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 what are commonly 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 Standards for the Protection of Electronic 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 organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI).

As part of our risk assessment, we reviewed and commented about the updated data agreements, data classifications and data exchanges. Additionally, three working products are conveyed with this report. These work products are designed to provide RIVH with a basis to prioritize and document responses to the identified risks. The three work products are explained below.

1. *Security Standards Report*

A detailed standard by standard explanation of the Security Rule standards with a comment from the Bureau that expresses our assessment of RIVH's compliance with each standard.

2. Threat Risk Matrix

An evaluation of identified risks in relation to the likelihood and probability of occurrence, this matrix documents the controls the Bureau found in place at RIVH to address each risk, as well as recommend control improvements. The matrix is a working document designed to provide RIVH with a basis to prioritize and document their response to the identified risks.

To determine the risk impact threat assessment, we used the "Magnitude of Impact Definitions" of the National Institute of Standards and Technology Special Publication 800-30. These definitions describe the consequences of not properly safeguarding ePHI in terms of high, medium, and low impacts as quoted below:

- High—Exercise of the vulnerability: (1) may result in the high 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.

3. Policy and Procedure Gap Analysis

Identifies policies and procedures that RIVH has or should have in place that govern access to e-PHI. The analysis includes a description of the policy or procedure, and the Bureau's evaluation of their adequacy.

RIVH should use this tool as a guide for developing as well as updating and improving department policies and procedures that relate to the protection of e-PHI.

Objective, Scope and Methodology

Our objective was to perform a security risk analysis of RIVH risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI.

In conducting the security risk assessment, we used the security standards as divided into the categories of administrative, physical, and technical safeguards. Regulatory definitions of the safeguards can be found in the Security Rule at 45 CFR §164.304.

- **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 primarily automated processes used to protect data and control access to data.

We planned and performed the risk assessment to obtain sufficient, appropriate evidence to provide a reasonable basis for our risk assessment report and conclusions based on our HIPAA risk assessment Security Rule compliance objectives. We believe that the evidence obtained provides a reasonable basis for our assessment and conclusions.