THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

July 6, 2015

Mr. Michael L. Joseph
Chairman of the Board
Roswell Park Cancer Institute
Elm & Carlton Streets
Buffalo, NY 14263

Re: Security Over Electronic Protected Health Information
Report 2014-S-67

Dear Mr. Joseph:

Pursuant to the State Comptroller's authority as set forth in Article X, Section 5 of the State Constitution and Section 2803 of the Public Authorities Law, we examined security over electronic protected health information (ePHI) at the Roswell Park Cancer Institute (Institute) for the period January 1, 2013 through March 6, 2015. Specifically, we audited whether the Institute is properly safeguarding its ePHI and whether it has protection policies in place and a plan to make mandatory notifications when ePHI is lost or stolen.

Background

The Institute is a comprehensive cancer treatment and research complex located in Buffalo, New York. To support its operations, the Institute maintains major computer systems and networks that process, store, and transmit ePHI. Since 2003, all health care providers, including the Institute, are required to comply with a set of information security standards for protecting ePHI, as established in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. All ePHI created, received, maintained, or transmitted by an organization is subject to the Security Rule.

Under the Security Rule, the security process begins with the policies and procedures that establish personnel behavior and provide a framework for acceptable access to and use of ePHI. These administrative controls are the foundation for the HIPAA Security Rule. Physical safeguards support limitations to restricted spaces and equipment, including materials that contain ePHI. Technical safeguards apply specifically to information systems and are measures of protection associated with the actual hardware, software, and networks for these systems.

While the Security Rule provides a continuum of security over ePHI, the federal Health

Information Technology for Economic and Clinical Health Act (HITECH) elaborates on the criticality of following these standards. HITECH, which became effective on February 17, 2010, provides enforcement, accountability, and penalty-related guidelines for organizations involved in sharing or accessing ePHI. Furthermore, HITECH extends certain HIPAA Privacy and Security Rule requirements to health care providers' business associates and establishes new limitations on ePHI disclosure. Health care providers were expected to fully comply with HITECH by September 23, 2013.

In 2006, the Institute developed an Electronic Medical Record (EMR) system to replace paper medical records. The current EMR system supports all aspects of inpatient and outpatient clinical care. The system serves as the primary repository for clinical data related to patient care activities and support clinical research studies. Clinical data that comprises the electronic patient health record can be directly entered through the system or received via interface from other electronic health systems (i.e., laboratory or radiology results). Over 4,000 individuals access the Institute's EMR system and networks that facilitate ePHI access.

Results of Audit

The Institute has established a highly developed information security program to protect the ePHI it creates, receives, maintains, or transmits. During our testing, we found the Institute has taken many steps to safeguard its ePHI and meet Security Rule requirements. In addition, we found the Institute has adequate protection policies in place and a plan to make mandatory notifications when ePHI is lost or stolen. Furthermore, during our audit period, Institute management generally took prompt action when they became aware of potential ePHI security issues. However, we identified some improvement opportunities involving certain administrative, physical, and technical safeguards over the Institute's ePHI. We make four recommendations to address the control weaknesses we identified.

Risk Assessment

The Security Rule requires health care providers to evaluate risks and vulnerabilities to ePHI in their environments. Providers are then expected to implement reasonable and appropriate security measures to protect against these threats. To effectively complete these tasks, it is important that providers account for all of their ePHI, document where the data resides, and determine whether adequate controls exist to protect it. As such, the Department of Health and Human Services recommends that risk assessments start with an inventory of all systems and devices that create, receive, process, maintain, or transmit ePHI.

To meet HIPAA Security Rule and HITECH requirements and protect its technology and data assets, the Institute has developed an Information Risk Management Program (Program) and a Risk Assessment Policy (Policy). The primary components of the Program include planning, periodic risk assessments, risk mitigation, and incident risk reporting and response. As part of its Program, the Institute performs periodic data classifications to determine, among other things, which of its applications and information system resources handle ePHI. In addition, annually the Institute completes a "Risk and Threat Impact and Analysis Assessment Report" (Risk Assessment).

In these Risk Assessments, the Institute ranks risks as high, medium, or low depending on the likelihood of the threat occurring and the resulting impact. As opposed to low risks, high and medium risks present threats that may result in a significant loss of Institute assets or harm its mission or interests. According to the Institute's Policy, the risk rating should be a major consideration when prioritizing corrective action efforts, with high risks having the greatest need for immediate corrective actions if existing security tools and techniques are inadequate. Further, the Policy indicates that risks that remain open over multiple assessment periods should be given additional consideration.

We found the Institute's December 2014 Risk Assessment contained a number of risk items, including some considered high risk, that have remained open for more than one year, as summarized in Table 1.

Table 1
Medium and High Risks Open More Than One Year

Year Identified	Outstanding Risks	
	High	Medium
2009	0	4
2010	0	0
2011	5	1
2012	13	25
2013	1	4
Totals	**19**	**34**

In response to our finding, Institute management stated the 2014 Risk Assessment includes several risks that have been resolved, but had not yet been documented in the Risk Assessment. Management indicated that, as of April 2015, 4 of the 19 high risks identified in Table 1 were now closed, progress was being made toward fixing 6 others, and 2 were being deferred for future Risk Assessments. For the 34 medium risks, management indicated 3 were now closed, progress was being made toward fixing 15 others, and 3 were being deferred. For the remaining 20 risks (7 high and 13 medium), management either did not provide a status update or indicated the risks were still open.

Both the 2013 and 2014 Risk Assessments revealed deficiencies in the Institute's accountability over the systems and devices that create, receive, process, maintain, or transmit ePHI. In fact, the 2013 Risk Assessment identified risks related to ePHI accountability that dated back to 2008. Furthermore, the 2014 Risk Assessment identified nine other open risks pertaining to the need for additional policies and procedures that, as of April 2015, still had not been addressed, including facility access control, contingency planning and testing, ePHI access monitoring, emergency access, change management, and device security. Of these nine open risks, four first appeared on the Institute's 2011 Risk Assessment, two each on the 2012 and 2013 Risk Assessments, and one on the 2009 Risk Assessment.

We noted that neither the 2013 nor 2014 Risk Assessments indicated when all the open risks would be addressed. Upon review of the most recent Risk Assessment, management informed us only 18 of the 53 risks will remain open beyond fiscal year 2015-16. In their response to our preliminary findings, management indicated Institute personnel had done a brief assessment to assign a risk priority ranking of ePHI data/applications (for the purposes of contingency planning). Based on the assessment, they indicated the Institute determined it to be more prudent to prioritize the use of its resources to first address other identified risks. They indicated that this approach to risk management is allowed under the Security Rule.

While this practice for prioritizing risk remediation does not violate the Security Rule, we believe it contradicts the Institute's own policy of promptly addressing high risks, especially those that remain open over multiple periods. Of the 18 risks that the Institute had no formal plans to address as of April 2015, seven were considered high-risk items, including one related to accounting for all ePHI assets. Even though five of these high-risk items date back to the 2011 Risk Assessment, the Institute has worked on fixing more than half of the open medium-risk items. Without a formal comprehensive assessment (i.e., cost vs. benefit) of the recommended controls for all open risk items, it is not apparent whether the Institute effectively addresses the highest priority risks.

ePHI Access Controls

The Security Rule requires health care providers to restrict ePHI access to only those workforce members or business associates who require access to that data to perform their job functions. Access controls and procedures must be in place for all information systems that maintain ePHI to guard against unauthorized access to the data. Also, security mechanisms and procedures must be implemented to limit access to facilities and physical areas in which the information systems reside.

With a few exceptions, we found the Institute had established adequate technical and physical safeguards over ePHI. However, while most facilities housing or facilitating access to ePHI were physically secure, we found three data communication closets were not locked at the time of our testing. Upon notifying management about the unlocked data communication closets, they took prompt steps to secure the locations. In the future, they indicated the Institute would increase random checks of data communication closet security.

Technical Safeguards

Under the Security Rule, technical safeguards relate to the information technology (i.e., firewalls and anti-virus software) that protects ePHI and controls access to it. Health care providers are expected to determine which security measures and specific technologies are applicable and appropriate to implement based upon their risk assessments and environments. During our audit, we identified findings and made recommendations for corrective actions related to the Institute's ePHI technical safeguards. These findings and recommendations were presented in detail to Institute officials throughout the audit. To further ensure ePHI security, these findings and recommendations are not included in this final report. Subsequent follow-up audits will

address the detailed findings and recommendations.

Recommendations

1. Take steps to resolve risk items that have remained open over multiple periods.

2. Implement reporting mechanisms to support risk mitigation priorities including decisions to defer or not address specific risks.

3. Continue efforts to strengthen physical security over the systems that receive, store, process, transmit, and maintain ePHI.

4. Implement the recommendations detailed during the audit for strengthening technical safeguards over ePHI.

Audit Scope, Objectives, and Methodology

We audited the Institute to determine if it was properly safeguarding ePHI and had protection policies in place to make mandatory notifications when ePHI is lost or stolen. The audit period covered January 1, 2013 through March 6, 2015.

To accomplish our objectives, we assessed the Institute's internal controls related to safeguarding ePHI and breach identification and disclosure practices. We also interviewed Institute management responsible for the oversight of controls and safeguards over ePHI. In addition, we reviewed Institute policies, procedures, and laws relevant to our audit scope; technical tests, business associate listings and agreements, relevant training records, security monitoring and violation reports, vulnerability assessments, risk assessments and related plans, and business continuity and disaster recovery plans; and related firewall, system, and device configurations.

During our audit, we checked physical access to data server rooms, data communication closets, and overall facility access. To assess logical access, we tested authentication controls and compared user access lists to human resource records. In addition, we identified components of the Institute's information systems and networks to determine where ePHI is created, processed, maintained, or transmitted. We used auditing software to test the network for unauthorized devices and improper device configurations.

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and

approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Reporting Requirements

We provided a draft copy of this report to Institute officials for their review and comment. We considered the Institute's comments in preparing this report and have included them in their entirety at the end of it. Institute officials agreed with our recommendations and indicated the Institute has taken steps to address them.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Institute's Chairman shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

Major contributors to this report were Brian Reilly, Mark Ren, Kathleen Hotaling, Robert Horn, Barbara Mann, Andrew Philpott, Gerry Cochran, and Marzie McCoy.

We thank the management and staff of the Institute for the courtesies and cooperation extended to our auditors during this audit.

Very truly yours,

John F. Buyce, CPA, CIA, CFE, CGFM
Audit Director

cc: Division of the Budget

Agency Comments

ROSWELL PARK CANCER INSTITUTE
Elm & Carlton Streets | Buffalo, NY 14263
716-845-2300 | www.roswellpark.org
E-mail: askrpci@roswellpark.org

UNDERSTAND PREVENT

Andrea C. Kuettel, RN, JD
Associate Counsel for HIPAA/HITECH
Office: (716) 845-3802
Fax: (716) 845-3132
Email: Andrea.Kuettel@RoswellPark.c

June 18, 2015

John F. Buyce, CPA, CIA, CFE, CGFM
Audit Director
State of New York Office of the State Comptroller
110 State Street
Albany, New York 12236

Via email: jbuyce@osc.state.ny.us

Re: Security Over Electronic Protected Health Information Report 2014-2-67

Dear Mr. Buyce:

This letter serves as the formal written response of Roswell Park Cancer Institute (the Institute) to the audit undertaken by the New York Office of the State Comptroller (OSC) to determine whether the Institute was properly safeguarding electronic protected health information (ePHI) and had appropriate protection policies in place.

The Institute is committed to protecting all aspects of our patients' privacy, including, in particular, the ePHI we create, receive, maintain and transmit in connection with our patients' care and treatment. Accordingly, we are gratified by the OSC's overall assessment that the Institute has a highly developed information security program to protect ePHI and has adequate protection policies in place. In keeping with our efforts to improve continually our information privacy and security programs, we also appreciate the recommendations for improvement that were included in the audit report. As discussed below, these recommendations were immediately addressed by the Institute and corrective actions are currently in effect. For detail in each of these areas, additional information is available in confidence, upon OSC's request

Risk Assessment

As noted in the OSC audit report, the Institute has developed an Information Risk Management Program and a Risk Assessment Policy to comply with federal and State regulatory requirements. We agree with the OSC's observation that more

thorough documentation of our assessment of controls for risks identified in our annual risk assessment is needed. Such documentation better demonstrates that the Institute is effectively addressing the highest priority risks as required by our policies. The Institute has updated our documentation to provide more accurate and relevant information and more meaningful measurement of progress toward establishing controls of open risk items.

Technical Safeguards

The OSC audit determined that the Institute has adopted reasonable measures to meet the Security Rule's technical standards, and made recommendations for improving technical safeguards over ePHI. These recommendations have been addressed, with changes implemented, and currently in effect.

ePHI Access Controls

The OSC's audit also determined that the Institute has adequate technical and physical safeguards over ePHI. To further improve our program, the Institute has implemented the policy of random checks referenced in the OSC's audit report. Our Information Technology Security Team will review and document this issue twice per year.

Thank you for the opportunity to respond to the audit report. We appreciate the professionalism and collegiality shown by your staff and their willingness to share information and best practices to further enhance the Institute's information security program. Should you have any questions about the information in this response, please do not hesitate to contact me at the telephone number or email on this letterhead.

Sincerely yours,

Andrea C. Kuettel

Andrea C. Kuettel

Cc: Mr. Mark Ren
Mr. Michael Joseph
Mr. Michael Sexton