THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

October 7, 2016

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 2016-F-19

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 have followed up on the actions taken by officials of the Roswell Park Cancer Institute to implement the recommendations contained in our audit report, *Security Over Electronic Protected Health Information* (2014-S-67).

Background, Scope, and Objectives

The Roswell Park Cancer Institute (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 electronic protected health information (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 a health care provider 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 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.

Our initial audit examined whether the Institute was properly safeguarding ePHI and had protection policies in place to make mandatory notifications when ePHI is lost or stolen. The objective of our follow-up was to assess the implementation, as of September 8, 2016, of the four recommendations included in our initial report.

Summary Conclusions and Status of Audit Recommendations

The Institute made significant progress addressing the issues identified in our initial audit. Of the four recommendations contained in our initial report, two have been implemented and two have been partially implemented.

Follow-Up Observations

Recommendation 1

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

Status – Partially Implemented

Agency Action – During our initial audit, we found 53 high- and/or medium-risk items had been open for over a year as of December 12, 2014. As of September 2016, 44 of the 53 items had been closed, while nine risks were still open. Institute officials provided justifications why they felt the risks for two items were at acceptable levels, and also explained that three other open items would be closed by October 2016. However, officials could not provide evidence that specific actions had been taken to resolve the remaining four open risks. According to officials, the Institute must undertake large initiatives that require formal review, approval, and material funding commitments by executive management to resolve such risks. Furthermore, officials indicated that these administrative processes could take up to a year to complete, along with any additional time needed for contract procurements. The four risks in question were first identified in 2012, nearly four years ago. Thus, significant time has elapsed since the deficiencies were identified, and the Institute should take actions to substantively resolve those items soon.

Recommendation 2

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

Status – Partially Implemented

Agency Action – As noted in our initial audit, 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. In addition, the Institute completes an annual "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. According to the Institute's Policy, the risk rating should be a major consideration when prioritizing corrective action efforts, and risks that remain open over multiple assessment periods should be given additional consideration.

However, at the time of our initial audit the Institute did not – and still does not – have procedures to document the underlying reasons to avoid, mitigate, accept, or transfer open risk items. Although the Institute made significant progress in addressing the open high- and medium-risk items cited in our initial audit, some of such risks have not yet been resolved. As noted previously, management could not indicate precisely when four open risks (three medium and one high) from 2012 would be resolved. The fact that high and medium risks pose threats that may result in material loss of Institute assets or harm its interests underscores the importance of maintaining a record of the underlying decisions to defer and accept certain risks. Management indicated that starting October 1, 2016 the Institute will implement a new procedure to better support its risk decisions.

Recommendation 3

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

Status – Implemented

Agency Action – Subsequent to our initial audit report, the Institute implemented a procedure to audit the security of network data closets on a bi-annual basis. We reviewed the results of the Institute's two last security reviews conducted in November 2015 and July 2016 and determined the process was adequate. Furthermore, we sampled 15 locations containing network equipment, including the three that were not adequately secure during our initial audit, and found no exceptions.

Recommendation 4

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

Status – Implemented

Agency Action – The Institute has addressed the technical recommendations made during the initial audit.

Major contributors to this report were Brian Reilly, Mark Ren, Jared Hoffman, Rachael Hurd, and Robert Horn.

We would appreciate your response to this report within 30 days, indicating any additional actions planned to address the unresolved issues discussed in this report. We also thank Institute management and staff for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

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

cc*:* Division of the Budget
Laura Linneball, Roswell Park Cancer Institute