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) 845-4781
Email: Andrea.Kuettel@RoswellPark.c

December 9, 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: 90-day Auditee Response to Security Over Electronic Protected Health Information Report 2014-2-67

Dear Mr. Buyce:

This letter provides an update to the written response of Roswell Park Cancer Institute (the Institute) to the audit undertaken by the New York Office of the State Comptroller (OSC) regarding safeguards over electronic protected health information (ePHI).

Safeguarding our patients' privacy and ePHI remains, by necessity, an ongoing effort. We have addressed the recommendations made by the OSC in its July 6, 2015 report, and this response describes those actions. As with our previous response, additional information is available in confidence, upon OSC's request.

Risk Assessment Open Items and Reporting Mechanisms

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. Several risk items appeared open over multiple reporting periods because documentation of risk item closure or re-characterization was not complete.

Since the original report, the Institute's IT Security Team has closed a number of risk items, including those identified by the Institute's Internal Audit team, along with risk items identified through previous IT Security Risk Assessments. In summary, by the end of this calendar year, it is anticipated that there will be no

more than seven risks categorized as high risk and nine risks categorized as moderate risk, all of which will be addressed in the 2016 IT Security Work Plan. The 2016 IT Security Risk Assessment will describe the processes in place to address ongoing risks, rather than documenting these as ongoing unresolved risks, and these processes will be followed in IT Security Risk Assessments going forward.

The IT Security Committee has reviewed the closure of risk items. Additional items to be closed will be reviewed at the December meeting, along with the IT Security Risk Assessment for 2016. Following any adjustments recommended by the IT Security Committee, the Risk Assessment will be finalized and presented to the Institute's Compliance Committee of the Board of Directors at the January 2016 meeting. This process for reviewing risks and determining priorities for addressing risks will continue to be followed annually and as needed, in the event of significant changes in risk or upon request of the Board.

Strengthening Physical Controls

The OSC's audit also determined that the Institute has adequate technical and physical safeguards over ePHI. Since the initial report, the Institute has conducted additional testing, including testing by contracted experts, to determine any additional areas for improvement. Findings will be reflected on the 2016 IT Security Risk Assessment.

Technical Safeguards

RPCI's implementation of the OSC's recommendations for improving the Institute's technical safeguards over ePHI remain in effect as previously noted in our earlier letter.

Thank you for the opportunity to provide this update to RPCI's earlier response. 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

Cc: Mr. Mark Ren
Dr. Candace Johnson
Mr. Michael Joseph
Mr. Michael Sexton