STATE OF NEW YORK
OFFICE OF THE INSPECTOR GENERAL
EMPIRE STATE PLAZA
AGENCY BLDG. 2, 16TH FLOOR
ALBANY, NEW YORK 12223
(518) 474-1010

61 BROADWAY, SUITE 2100
NEW YORK, NEW YORK 10006
(212) 635-3150

65 COURT STREET, 5TH FLOOR
BUFFALO, NEW YORK 14202
(716) 847-7118

Catherine Leahy Scott
INSPECTOR GENERAL

June 17, 2013

Mr. James Cox
Medicaid Inspector General
800 North Pearl Street
Menands, New York 12204

Dear Mr. Cox:

On May 8, 2012, the New York State Inspector General commenced an investigation into allegations that confidential information was disseminated by certain Office of the Medicaid Inspector General (OMIG) employees to former OMIG employee [redacted] who retired from OMIG employment on August 13, 2010, and former Medicaid Inspector General [redacted] who resigned OMIG employment on July 30, 2011.

The Inspector General reviewed archived OMIG e-mail accounts for the periods of approximately July 2010 to May 2012. The review revealed numerous e-mails from OMIG employees to a personal e-mail of [redacted] a personal e-mail of [redacted] and [redacted] e-mail at NYC Human Resources Association (HRA), where [redacted] is currently employed.

The e-mails between the OMIG employees[1] and [redacted] were largely personal in nature, although a small number contained references to OMIG matters and/or records. For instance, on October 5, 2010, then OMIG employee [redacted] sent an e-mail from his state computer using the OMIG e-mail system to [redacted] personal e-mail that included an attachment containing Medicaid guidelines. In addition, on July 25, 2011, [redacted] forwarded an e-mail to [redacted] with the subject line "Proprietary NF Chain/Owners," which contained an attached spreadsheet listing various hospital locations, names of hospital owners and the number of beds per hospital. The Inspector General found no confidential or Health Insurance Portability and Accountability Act (HIPAA) protected information contained in the e-mails or attachments sent to [redacted] Rather, both the October 2010 and July 2011 e-mails contained information that is publicly available.

[1] With the exception of one employee, all of the individuals found to be sending e-mails to [redacted] and [redacted] have either since retired or resigned their OMIG employment.

The Inspector General also found no confidential or HIPAA-protected information contained in the e-mails or attachments sent to [redacted] Rather, the e-mails between the OMIG employees and [redacted] also were largely personal in nature, although a small number contained references to OMIG matters and/or records. However, [redacted] who is currently employed by NYC Human Resources Association (HRA), continues to work with OMIG employees due to HRA's nexus with statewide OMIG programs.

While the investigation found no confidential or HIPAA-protected information contained in the e-mails or attachments sent by OMIG employees to [redacted] and [redacted] certain e-mails still contained OMIG documents. The investigation further revealed that OMIG employees were using their state computers and OMIG e-mail system for e-mails of a personal nature. Accordingly, the Inspector General recommends that OMIG review and implement uniform guidelines relating to computer usage and security that the Inspector General recently disseminated to all agencies under our jurisdiction. The guidelines include the following provisions:

- Create/review its computer usage policy and update it annually as needed.
- Distribute the computer usage policy to all new staff at commencement of employment and to all other employees on an annual basis.
- Ensure employees understand internet and e-mail use policies and acknowledge in writing their receipt/understanding of this policies.
- Conduct periodic, system-wide reviews of employee internet and e-mail usage to identify employees who use most frequently; check results to see whether internet and e-mail use is appropriate.

OMIG should review its computer usage and security policies (including the prohibition of unauthorized dissemination of proprietary and sensitive information) to ensure conformity with the guidelines described above. The Inspector General recommends that, on an annual basis, OMIG train all employees on OMIG's computer usage and security policies. Additionally, the Inspector General recommends that all OMIG staff be provided with copies of OMIG policies on computer, Internet, and e-mail use, and annually sign acknowledgements of their receipt, review and understanding of these policies.

Within 45 days, please provide information concerning OMIG's review and actions, including copies of any revised polices. If you require further information about our investigation, please contact Deputy Inspector General Audrey Maiello Cunningham at 518-474-1010.

Very truly yours,

[redacted]

Catherine Leahy Scott
Inspector General