THOMAS P. DINAPOLI
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

July 16, 2021

Mantosh J. Dewan, M.D.
President
State University of New York
Upstate Medical University
750 East Adams Street
Syracuse, NY 13210

Re: User Access Controls Over Selected System Applications
Report 2021-F-8

Dear Dr. Dewan:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law, we have followed up on the actions taken by officials of the State University of New York (SUNY) Upstate Medical University (Upstate) to implement the recommendations contained in our audit report *User Access Controls Over Selected System Applications* (Report 2019-S-34).

Background, Scope, and Objective

A part of the SUNY system since 1950, Upstate's mission is to improve the health of the communities it serves through teaching, research, and patient care. Upstate, the only academic medical center in Central New York, comprises four colleges, a research enterprise, one hospital with two locations (Upstate University Hospital and Upstate University Hospital at Community Campus), and over 80 outpatient clinics and other centers. To facilitate its clinical care, education, research activities, and communication, Upstate owns and/or administers approximately 200 system applications.

Applications not only may be used by Upstate employees but also may be accessed by students, visiting or adjunct professors, consultants, contractors, contract physicians, external service providers, volunteers, and vendors as required and permitted.

As these applications may contain a broad range of sensitive and personal information that is considered confidential for a variety of programs, controls over their access are especially important. To ensure that only authorized users are allowed to access information stored on systems, agencies such as Upstate must follow New York State Information Technology security policies and standards related to security, account management, and access controls. Upstate must also comply with numerous federal and State laws and regulations, including the Health Insurance Portability and Accountability Act, as well as its own policies and guidelines.

Our initial audit report, issued on June 10, 2020, sought to determine if Upstate's access controls over select Upstate applications were effective to prevent unnecessary or

inappropriate access to those applications. Our audit covered the period from January 1, 2015 through October 8, 2019. Overall, we determined that Upstate's access controls were not sufficient to prevent unnecessary or inappropriate access to various applications. We found that Upstate employees maintained unnecessary and inappropriate access to applications after a change in the users' status (e.g., employment separation, death). Some of these user accounts were logged into during the period of inappropriate active access. We also found users who maintained unnecessary and inappropriate access to certain clinical applications after they had transferred to new jobs that did not require that access.

The objective of our follow-up was to assess the extent of implementation, as of April 21, 2021, of the two recommendations included in our initial audit report.

Summary Conclusions and Status of Recommendations

Upstate officials have made significant progress in addressing the problems we identified in the initial audit. Both of the initial report's recommendations were implemented.

Follow-Up Observations

Recommendation 1

Improve controls over user access to ensure Upstate applications meet the applicable laws, regulations, and policy requirements, including but not limited to:

- *Maintaining and regularly reviewing user lists for each application;*
- *Developing policies and procedures that detail requirements for when access must be removed;*
- *Documenting when key decisions are made that allow users to maintain access outside of the requirements in policies and procedures;*
- *Ensuring Upstate practices are consistent with policies and procedures; and*
- *Evaluating whether access to the application is needed if users are not using the application.*

Status – Implemented

Agency Action – Upstate has updated its policies and procedures to meet applicable laws, regulations, and policy requirements. Upstate has:

- Programmed the ability to compare an individual's employment status to the active status of their corresponding user account. This enhancement allows system administrators and Information Management and Technology staff to compare the status of user accounts in the systems they are responsible for to the status of users in the Human Resources system – identifying individuals whose access may not have been removed through other processes in place.
- Updated formal policies that address access and aligned practices to ensure consistency throughout Upstate.
- Implemented an approval process for exceptions that allow users to maintain access outside of the requirements in the policies and procedures. Exceptions

are recorded in the Help Desk ticket system.

- Implemented a more robust audit function in the Office of Information Security to ensure system administrators are adhering to policy requirements concerning access.
- Implemented a system to track whether users have accessed certain clinical systems for the past 180 days. If a user has not accessed the system in 180 days (365 days for medical doctors), the account is disabled.

Recommendation 2

Remove access for improper user accounts identified in our audit.

Status – Implemented

Agency Action – Upstate removed access for the improper user accounts identified in our audit.

Major contributors to this report were Amanda Eveleth, Lauren Bizzarro, Karen Corbin, and Jacqueline Keeys-Holston.

We thank the management and staff of SUNY Upstate for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Theresa Podagrosi
Audit Manager

cc: Michael Jurbala, Upstate
Amy Montalbano, SUNY