State University of New York Upstate Medical University

User Access Controls Over Selected System Applications

Report 2019-S-34 | June 2020

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller
Division of State Government Accountability

Audit Highlights

Objective

To determine whether access controls over select State University of New York Upstate Medical University (Upstate) system applications are effective to prevent unnecessary or inappropriate access to those applications. This audit covered the period from January 1, 2015 through October 8, 2019.

About the Program

Upstate, the only academic medical center in Central New York, consists of four colleges, a research enterprise, a clinical system, and a hospital that includes a Level 1 trauma center and a dedicated children's hospital and cancer center. To facilitate patient care, research, and education, Upstate owns and/or administers more than 200 applications that contain a broad range of sensitive and personal information that is considered confidential. Applications may be used not only by Upstate employees, but also by students, visiting or adjunct professors, and various non-employees such as consultants, contractors, emeritus professors, and vendors.

Key Findings

- We found Upstate's access controls are not sufficient to prevent unnecessary or inappropriate access to various applications. Inappropriate access can lead to intentional or accidental modification, destruction, or disclosure of clinical, educational, and research – and otherwise confidential – information. Specifically:
  - 352 user accounts for 113 users maintained unnecessary and inappropriate access to applications due to a change in the users' status (e.g., employment separation, death).
  - 61 of these user accounts were logged into during the period of inappropriate active access, including 8 accounts whose users were deceased at the time.
- We also found 27 users who maintained unnecessary and inappropriate access to certain clinical applications after they had transferred to new jobs that did not require that access. Further, in 12 of 27 instances, it took more than a month for access to be removed.
- Although Upstate has certain measures in place to review the appropriateness of user access, we question the thoroughness and extensiveness of these reviews. We identified 73 user accounts with inappropriate access to 11 different clinical applications that were not identified or remediated during the course of Upstate's reviews.

Key Recommendations

- Improve controls over user access to Upstate applications to ensure they meet the applicable laws, regulations, and policy requirements.
- Remove access for improper user accounts identified in our audit.

Office of the New York State Comptroller
Division of State Government Accountability

June 10, 2020

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

Dear Dr. Dewan:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage their resources efficiently and effectively. By so doing, it provides accountability for the tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit entitled *User Access Controls Over Selected System Applications*. This audit was performed pursuant to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

Division of State Government Accountability

Contents

Glossary of Terms

Term	Description	Identifier
EMR	Upstate's main electronic confidential medical record application	*Computer Application*
HR	Human Resources	*Department*
ISO	Information Security Officer	*Key Term*
MSG	Medical Service Group	*Key Term*
NYS IT	New York State Information Technology	*Key Term*
NYS IT Policy	NYS IT Policy on Information Security	*Policy*
Policy	Upstate's Information Access Management Policy	*Policy*
Upstate	State University of New York Upstate Medical University	*Auditee*
User account	An account assigned to a user to access an Upstate application	*Key Term*

Background

Upstate Medical University (Upstate) has been a part of the State University of New York system since 1950. Considered a clinical enterprise, it consists of four colleges, with an enrollment of 1,592; a research enterprise; a clinical system; and a hospital that includes a Level 1 trauma center and a dedicated children's hospital and cancer center. Upstate is the only academic medical center in Central New York, and serves approximately 1.8 million people. It is also that region's largest employer, with a workforce of more than 10,000 supporting its operations.

Upstate owns and/or administers more than 200 system applications, which facilitate its clinical care, education, research activities, and communication. Upstate's system applications are classified as clinical or non-clinical system applications. Clinical applications contain health information, such as patient medical records. Non-clinical applications do not contain health information and are system applications, such as email or file shares. Users include not only Upstate employees but also students, visiting or adjunct professors, consultants, contractors, contract physicians, external service providers, emeritus professors, 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 (NYS IT) 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.

According to NYS IT standards, agencies must review the appropriateness of user account access to their systems at least annually, and take immediate steps to remove those individuals whose circumstances change and who no longer need access. Further, NYS IT Policy on Information Security (NYS IT Policy) states that State entities are responsible for ensuring all accounts are disabled and access is removed immediately upon separation. In addition, according to Upstate's Information Access Management Policy (policy), when any user separates from Upstate, his or her username and password shall be denied further access to University computing resources, with certain exceptions. Furthermore, department managers are required to annually review user accounts' access to ensure the appropriateness of access to electronic information, including patient, department, and other sensitive data. In addition, auditing of user accounts and access privileges will be performed on a periodic basis to ensure proper access by reviewing account login/logoff, file access, password activity, and usage activity.

Audit Findings and Recommendations

Despite policies and procedures intended to support compliance with NYS IT security policies and procedures, our audit found that Upstate's access controls are not sufficient to prevent unnecessary or inappropriate access to various applications. Specifically, for certain users, Upstate does not have a formal process to be followed to ensure users' access to systems is deactivated timely when required, resulting in often prolonged periods of inappropriate, unnecessary access. Inappropriate access can lead to intentional or accidental modification, destruction, or disclosure of clinical, educational, and research – or otherwise confidential – information. For example, we found:

- 352 active user accounts, maintained for 113 users, with inappropriate access to applications due to a change in the users' status warranting immediate termination of access. For 61 of these accounts, we also found instances of unauthorized login, including accounts whose users were deceased at the time.
- 27 users with continued access to certain clinical applications after their transfer to new job titles that did not require the same level of access. Further, in 12 of 27 cases, it took more than a month for access to be removed.

Although Upstate has certain measures in place to review the appropriateness of user access, we question the thoroughness and extensiveness of these reviews. We identified 73 user accounts with inappropriate access to 11 different clinical applications that were not identified or remediated during the course of Upstate's reviews.

We note that Upstate officials have been responsive to our audit findings and have started to address the issues we identified, such as taking steps to remove and deactivate user accounts and applications where appropriate.

User Account Access

Inappropriate Access for Users With a Change in Status

In conflict with NYS IT Policy as well as its own policy, Upstate does not always deny users' access to its computing resources upon separation or suspension of their relationship with Upstate and, as such, cannot be confident that its applications and the data within are protected against inappropriate access.

Our analysis of 948 user accounts for 174 users for the 24 applications in our sample found 352 active user accounts (37 percent) for 113 users (65 percent) whose change in status required the account to be disabled, whether due to leave of absence, an off-campus assignment, employment separation, or death. In fact, as shown in the following table and discussed in more detail in subsequent sections, 41 user accounts continued to have access more than six months after the change in status and 17 continued to have access for more than a year.

User Accounts With Access Not Removed Timely

Access No Longer Necessary Due to:	Accounts Reviewed	Accounts With Access Removed Late	Length of Inappropriate Access					
			1–7 Days	8–30 Days	1–3 Months	3–6 Months	6–12 Months	> 1 Year
Leave of absence	120	106	11	19	18	31	18	9
Off-campus assignment	275	105	6	5	30	45	15	4
Separation	420	52	12	25	4	11	0	0
Death	133	89	42	14	21	0	8	4
Totals	**948**	**352**	**71**	**63**	**73**	**87**	**41**	**17**

Employees on Leave of Absence

According to Upstate's policy, generally, employees on a leave of absence should only maintain access to two applications: email and timekeeping. All other existing accounts are to be disabled immediately until the individual returns to campus.

The audit team reviewed 120 user accounts for 28 users who were on a leave of absence at the time of our review. Of the 120 accounts, access to 106 accounts (88 percent) for 28 users was not removed timely. Furthermore, 24 users maintained access to 58 accounts for more than three months and 7 users maintained access to 9 accounts for more than a year. These 106 user accounts comprised 42 clinical user accounts and 64 non-clinical user accounts from 15 applications. In addition, we found that 9 accounts had been inappropriately logged into during the period users were on leave.

We also conducted limited testing on an additional sample: 65 users who were listed as active in the applications at the time of our testing but who Upstate officials stated were on an extended leave of absence during our audit period. We found that all 65 users (130 accounts) retained access following the start of their leave. We also found 2 users logged into their accounts during their leave (one at 168 days and the other at 131 days into their leave period).

Upstate's access controls did not align with its own access control policy, allowing users to maintain access during leaves if they are using time accruals. Authentication access is disabled only when a user's status is updated to "leave with pay" or "leave without pay" in Human Resources' (HR) master file. Thus, for employees who are on leave (i.e., maternity leave, family medical leave) but who are using accruals (and not reclassified as either "leave with pay" or "leave without pay"), their status remains active, as does their access. Additionally, Upstate's system design allows for users to maintain access to their files on Upstate's servers while on leave because, per Upstate policy, they maintain access for time accrual purposes. Although file shares are considered a non-clinical application, there is a risk that users could have inappropriate access to confidential information on their file share while on leave.

Upstate officials agreed with our findings and indicated that documentation procedures should be enhanced, as required by policy.

Employees With an Off-Campus Assignment

Pursuant to the bargaining agreement between New York State and the United University Professions union, certain employees may be given an off-campus assignment. Off-campus assignments are typically part of settlement agreements for employees who are going through the disciplinary process. Additionally, Upstate uses off-campus assignments to remove certain employees from campus to ensure safety and protect access to confidential information. At the onset of our audit, Upstate officials informed us that, although they do not have formal written procedures, individuals with an off-campus assignment are not allowed access to any Upstate resources, including email.

Our review included 275 user accounts for 38 users with an off-campus assignment. Of the 275 accounts, 105 (38 percent) for 35 users were not removed timely. These 105 user accounts included 8 clinical user accounts and 97 non-clinical user accounts from 11 applications.

Although 27 of these user accounts were for a timekeeping application, which Upstate officials have deemed to be of low risk, 6 were for Upstate's main electronic confidential medical record application (EMR). All 6 remained active for lengthy periods following the user's assignment: 2 between one and three months; 2 between three and six months; and 2 between six months and one year.

We also found 19 user accounts were logged into after the start of the user's off-campus assignment. This includes one user with an EMR account (see discussion above) who, with EMR access still active, continued to log into the confidential EMR application more than 100 days after the off-campus assignment start date. This user's access was not terminated despite the supervisor confirming that Upstate resources were not required to complete the assignment and a service call ticket requesting removal of access to all applications for this user. In addition to the EMR, this user also maintained access to five other non-clinical applications and continued to log into two other accounts, email and file shares, after the start of the off-campus assignment.

Upstate officials responded to our audit findings stating that, "while OSC was initially informed that all employee's access must be turned off, in practice, there are times when access is left on because the individual has been deemed low risk." This statement is contrary to what was conveyed at the onset of our audit and during audit meetings with supervisors of employees on off-campus assignments. Upstate officials also stated that an employee on off-campus assignment would still need access to certain applications. For each of these employees, HR determines what access, if any, should be disabled; users who are allowed to keep access are considered low risk based on the judgment of HR. In some instances, Upstate officials were able to provide documentation to support that access was allowed for select users as part of their off-campus assignment, and we subsequently removed

these individuals from our audit findings. However, for the 105 user accounts that still maintained access, Upstate officials were unable to provide documentation showing the user accounts had HR approval to remain active.

Users Who Have Separated From Upstate

According to Upstate's policy, when a user separates from Upstate, his or her username and password shall be denied further access to Upstate computing resources. Further, NYS IT Policy states that State entities are responsible for ensuring all accounts are disabled and access is removed immediately upon separation. However, certain populations are allowed extended access to email: resident doctors are allowed access to their email for up to one month after leaving Upstate, and students are allowed access to email for four months after graduation. To ensure access to accounts is disabled, Upstate generates a daily termination report, which is sent to the appropriate system administrators responsible for ensuring access to their applications is disabled.

We reviewed 420 user accounts associated with 74 separated users to determine whether their access to applications was appropriately terminated. We determined that, for 29 users with 52 accounts, access was removed late, including 11 accounts (11 users) where access was removed between three and six months after separation. These 52 user accounts included 8 clinical user accounts and 44 non-clinical user accounts for nine applications. We note that, during the period of inappropriate access, there were 25 instances of user login to various non-clinical accounts.

In addition, for 64 of the 74 users reviewed, the date of separation status change in the HR master file did not match the user's actual separation date, and in some cases was more than a year later. Inaccurate separation dates in the HR master file inappropriately enable employees to maintain their access to applications for the length of the discrepant period.

We note that 11 of the 29 users inappropriately maintained access to their email because Upstate's practice conflicted with its policy. Although Upstate's policy allows students access to their email for 120 days after graduation, we found that Upstate's practice actually allows students to access email for 150 days. Upstate officials agreed with these findings and stated that the majority of the findings were a result in delays in processing from either HR or payroll.

Deceased Non-Employees

Non-employees are individuals who are not employed by Upstate but have an approved educational or business need for access. According to Upstate officials, this group primarily consists of retirees with titles such as retiree associate, emeritus, and voluntary faculty but also includes contracted employees, other vendor-contracted employees, and volunteer associates. Non-employees are hosted by a sponsoring department, which maintains their information. The host is responsible for renewing the active status of each non-employee on a regular basis. User accounts

for emeritus and voluntary faculty are reviewed and attested to every 12 months, while retiree associates, vendor-contracted employees, and volunteer user accounts are reviewed and attested to every 4 months. User accounts for non-employees who are found to be deceased from one review period to the next are deactivated. In addition, Upstate HR officials deactivate deceased users' accounts upon knowledge of the death (e.g., notification, obituary announcement).

We reviewed a population of 133 user accounts for 34 non-employees who were deceased during our scope period. Despite the above-mentioned controls, access for 89 accounts (67 percent) with 21 users was not removed timely. These 89 user accounts contained 15 clinical user accounts and 74 non-clinical user accounts from 11 applications.

We also found eight user accounts that were used to log into two applications after the user's date of death. In response to our inquiry, Upstate officials suggested that it could have been a proxy login – that is, another individual who is allowed to access the account. Three of these eight users did not have a proxy listed on their account.

We also reviewed deceased non-employees' employment start and end dates. We found seven user accounts that were still active with future-dated end dates, including five with an end date of 2020 and two with an end date of 2099.

According to officials, Upstate has knowingly accepted the level of risk inherent in this area and reviews non-employees either every 4 or 12 months depending on the type of non-employee. Upstate officials conveyed that controls are functioning as designed.

Inappropriate Logins

In total, our login testing of the 352 user accounts identified 61 that had been inappropriately logged into while their accounts remained unnecessarily active.

For 131 of the remaining 291 user accounts, we were unable to determine if there was an inappropriate login due to issues with the data that Upstate provided to us:

- For five applications, we were unable to determine if there were any inappropriate logins.
- In other instances, instead of a last login date, the data field stated "not found in local user store." Upstate officials acknowledged they have already started to address the issues identified during our audit by removing and deactivating applications and user accounts where appropriate, resulting in login data being eliminated for users who have been removed from certain applications.
- In other instances, Upstate simply provided data that stated "no login found in the audit." For example, for one application, the audit team was provided the last login dates for only 4 of the 15 users requested; the remaining 11 were noted as "no login found in the audit." We question the necessity of user accounts that have not been used.

Furthermore, we found that one of the applications provided by Upstate and reviewed in our sample was not an actual application but rather a keypad code device used to protect medication rooms and that nonetheless warranted adequate security mechanisms. Upstate has approximately 25 to 30 secure medication rooms, which contain medications as well as medical equipment that can be accessed by nurses, pharmacy staff, and central supply staff. The list of users provided by Upstate was actually a list of employees who were given the code to access the secure rooms as part of their job duties. However, according to Upstate officials, the code has never been changed. Given the static nature of the code in place, there is a risk that employees who no longer need access to these secure medication rooms, as well as former employees, could still be able to access them.

Unnecessary Access for Transferred Employees

Upstate's Privacy Office reviews clinical application access for transfers through a daily transfer report. Based on the report and the supervisor's verification of access need, the Privacy Office determines whether the level of access to clinical applications should be removed and, if so, notifies the Information Security Officer (ISO). The Privacy Office maintains a transfer log documenting the transfer reviewed and the results. Although Upstate's policy and procedures do not specify a time frame for when a user's access must be removed, according to the NYS IT standard for account management/access control, when there is a position change, access is immediately reviewed and removed when no longer needed.

We selected a random sample of 25 days from the transfer log where the determination was made to remove/discontinue access. The sample of 25 days encompassed 32 employee transfers that required further action for access removal; that is, the employees' change in job duties no longer required them to have access to certain clinical applications. Using Upstate's service call ticket system, we verified the actual dates that clinical application access was removed. We found that 27 of 32 users maintained inappropriate access to clinical applications after they had transferred to new job titles. Further, in 12 of these 27 cases, it took more than a month for access to be removed.

Based on our review of the daily transfer log, we attributed delayed termination of access to the following:

- Users' supervisors not being responsive to Privacy Office requests for verification;
- The ISO not requesting removal of user access in a timely manner; and
- A lag between the Privacy Office's review of the daily transfer reports and its request for supervisor verification of access need.

Upstate officials responded to our finding by stating that "the majority of transfers are within clinical systems and patient care must be considered first. Access for these individuals may at times be more expansive when a transfer occurs, however overall

it is appropriate for them to have clinical access." Although these users maintained a level of clinical access, we maintain that, where Upstate determines access to certain applications is no longer necessary for a transferred employee's new job duties, access to those applications should be removed immediately.

Audit and Monitoring of Account Access

Upstate's policy states that all access to information, including patient, department, and other sensitive data, will be reviewed on an annual basis by department managers to ensure the appropriateness of access to electronic information. It also states auditing of user accounts and access privileges will be performed on a periodic basis. Upstate has several processes by which department managers review user access; however, our audit determined these processes are not comprehensive, and may allow users to maintain access inappropriately.

Department managers of 18 Medical Service Groups (MSGs) conduct an annual security compliance review, which includes reviewing a sample of user accounts with access to Upstate's EMR application to ensure the appropriateness of access to electronic information. A full list of EMR users is sent to each MSG manager by Upstate's ISO along with a request to review a sample of five to ten users. Although Upstate officials contend that some MSG department managers review more than five to ten users, they are only asked to review a minimum of 90 user accounts (5 user accounts per 18 MSGs) and a maximum of 180 user accounts (10 user accounts per 18 MSGs). Overall, this accounts for only 1 percent of the 13,000 total user accounts reported by Upstate for its 2018 annual review population. In fact, only 20 percent of user accounts for Upstate's main EMR were for users within a MSG and, as such, subject to review during the security compliance review. Further, according to data provided by Upstate, only 12 percent of users were actually reviewed as part of the annual security compliance review. The remaining 88 percent of user accounts for Upstate's main EMR were not reviewed as part of the annual security compliance review process. This includes those users who have access to Upstate's EMR but are not part of one of the MSGs. In addition, access to other applications that contain medical data or other sensitive or confidential data are not reviewed as part of this process.

Upstate also generates a daily Department Changes report, which contains a list of employees who have changed departments along with the applications they currently have access to. This report, as well as a biweekly Department Changes follow-up report, is sent to key individuals, including the ISO, the Institutional Privacy Officer, and the Internal Audit Director, for their review. However, Upstate could not provide documented procedures outlining how the reviews should be conducted; Upstate officials relayed that only access for clinical applications is reviewed. A termination report is also generated daily and sent to the appropriate system administrators responsible for ensuring that access to their respective applications has been disabled.

Although Upstate has certain measures in place to review the appropriateness of

user access, the thoroughness and extensiveness of these reviews is questionable. The audit team identified 73 user accounts with inappropriate access to 11 different clinical applications that were not identified or remediated during the course of Upstate's reviews.

Upstate officials have been responsive and have started to address the issues identified during our audit by beginning to remove and deactivate applications and user accounts where appropriate. For example, we determined the number of user accounts for their main EMR application decreased by 25 percent between March 2019 and July 2019. In another instance, during the same four-month period, an application containing patient radiology data, which Upstate deemed "obsolete" as it had been replaced in 2016, still had nearly 450 users with read-only access as of March 2019. During the course of our audit, in April 2019, Upstate decommissioned the application and, with the exception of administrator accounts, removed 99 percent of users.

Recommendations

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.

2. Remove access for improper user accounts identified in our audit.

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether access controls over select Upstate applications are effective to prevent unnecessary or inappropriate access to those applications. The audit covered the period from January 1, 2015 through October 8, 2019.

To accomplish our objective and assess related internal controls, we reviewed relevant laws, regulations, and NYS IT and Upstate policies. We also interviewed Upstate officials to gain an understanding of their processes and the applications used and maintained by Upstate.

In accordance with our audit scope and objective, we reviewed access controls for a sample of users from several populations, including those who transferred departments, went on a leave of absence, separated from Upstate, were considered non-employees, or were engaged in an off-campus assignment during our audit, to determine if their access to certain applications was removed timely.

We judgmentally selected a sample of 32 user accounts for employees who transferred to and from different departments from the daily transfer spreadsheet compiled by Upstate during our scope period. Based on the spreadsheet, we compiled a listing of days where Upstate determined that access should be discontinued for at least one person, resulting in 71 of 725 days of logs. From the 71 days, we used statistical sampling software to select a random sample of 25 days of transfer logs containing 32 user accounts to review. We reviewed the service call tickets for each of the 32 user accounts to determine when access was changed/removed.

We selected leave of absence transactions that occurred between January 1, 2015 and February 7, 2019 based on the leave status description. We judgmentally selected 155 of 3,793 employees who were on leave according to a list provided by Upstate. Then we looked up the current status for those 155 employee IDs in Upstate's system. Of the 155 employees, we selected 141 employees whose current status was leave of absence or active. Of the 141:

- 36 employees were still on a leave of absence at the time of our testing; 6 were excluded because of their type of leave, 1 was excluded because the leave began before our scope period, and 1 was excluded because the individual was not on a continuous leave. Therefore, 28 employees were reviewed further for access to the 24 applications in our sample.
- 105 employees were active at the time of our testing, though only 65 were on extended leave during our audit period. We performed limited testing of two applications for these 65 users to determine if the users retained access to any of the 130 accounts inappropriately during their leave of absence or logged into those accounts.

We judgmentally selected 88 of 4,879 employees who separated during our scope period based on the population of separations generated on November 13, 2018 for a prior audit (Report 2018-S-57). Starting with the population of 284 users reviewed

by the audit team for that audit, we selected all employees who did not have both an employee clearance and separation form as well as employees whose forms had a different date than what was reflected in the HR application. Next, we removed 14 users who were active at the time of our testing, resulting in 74 total users reviewed.

We selected a judgmental sample of 34 non-employee users based on their deceased status. Starting with the total population of 22,285 non-employees provided by Upstate, we identified deceased users by reviewing and searching the employees listed on Upstate's memoriam webpage and by conducting an obituary search.

We reviewed all 38 employees placed on an off-campus assignment between January 1, 2015 and November 11, 2018, except for one employee whose assignment was being reviewed by another entity.

For each sample of users, we reviewed access to 24 Upstate applications. Initially, we judgmentally selected a population of 25 applications from more than 200 applications provided by Upstate. We selected these applications based on the description of the data contained therein. Two applications we selected were actually the previous and current versions of the same application; we eliminated the previous version, resulting in a population of 24 applications. Of the applications selected, 14 were clinical applications and 10 were non-clinical applications; 15 used one authentication method while 9 used another. In addition, although 3 of the applications selected have since been decommissioned and are currently obsolete, they were used during our scope period and retained in our sample population. A fourth application was also kept in our population despite it not being an actual application but instead a keypad code used to limit access to secure medication rooms. We also retained a fifth application that, while not actually owned or maintained by Upstate, is used and accessed by Upstate employees. For all samples, we reviewed applicable documentation and associated data available for each of the 24 applications in our population. These samples cannot be projected to the population as a whole.

Statutory Requirements

Authority

The audit was performed 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 conducted our performance 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.

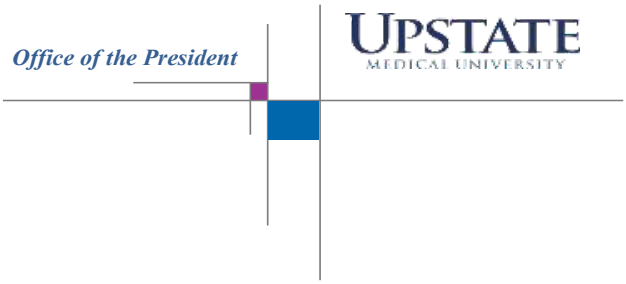
In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, 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 Upstate officials for their review and formal written comment. Their comments were considered in preparing this final report and are attached at the end in their entirety. The officials agreed with the report's recommendations and stated that incorporating the recommendations included in this audit report will serve to enhance its control structure.

Within 180 days after final release of this report, as required by Section 170 of the Executive Law, the President of Upstate Medical University 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.

Agency Comments



May 15, 2020

Brian Reilly, Audit Director
Office of the State Comptroller
Division of State Government Accountability
110 State Street - 11th Floor
Albany, NY 12236-0001

RE: Audit Report 2019-S-34 User Access Controls Over Selected System Applications

Dear Mr. Reilly:

Thank you for your review of our user access controls over selected system applications. Below, please find State University of New York Upstate Medical University's (Upstate) responses to the key recommendations included in your draft report, Audit Report 2019-S-34 User Access Controls Over Selected System Applications.

Upstate is committed to its mission to improve the health of the communities it serves through teaching, research and excellent patient care. Our Information Management and Technology department (IMT) is responsible for providing a secure technology infrastructure to protect the confidentiality, integrity, and availability of information on SUNY Upstate systems. As Central New York's largest employer, IMT performs this task with an infrastructure comprising more than 200 system applications containing broad range of sensitive and personal information utilized by a broad range of individuals across four colleges, a research enterprise, a hospital with four main locations (Upstate University Hospital-Downtown, Upstate University Hospital-Community Campus, Upstate Golisano Children's Hospital and Upstate Cancer Center) as well as a network of outpatient clinics and other care facilities.

While we believe Upstate has a robust system of internal controls and processes in place to prevent unnecessary or inappropriate access to our system applications, incorporating the recommendations included in this audit report will serve to enhance our control structure.

Recommendation:

Improve controls over user access to Upstate applications to ensure they meet the applicable laws, regulations and policy requirements.

750 East Adams Street | Syracuse, NY 13210 | Ph: 315.464.4513 | Fax: 315.464.5275 | www.upstate.edu | State University of New York

Upstate Response:

Upstate considers user access over system applications to be one of its most critical operational functions to ensure that patient, student and staff information in our dynamic and complex institution is protected. We have extensive internal controls relating to user access that are continually challenged and reviewed and are in the process of enhancing those controls with the recommendations included in OSC's audit report. Our Information Management and Technology (IMT) and Human Resources (HR) departments are working closely together to address those findings and recommendations including:

- Ensuring all applications are merged with the IMT Security application as well as user lists uploaded and stored within the merged application.
- Creation of enhanced reports comparing application user lists to the Human Resources Information System (HRIS) database and related additional audit and review procedures associated with exceptions.
- Enhancing our documentation of all changes and decisions made through the enhanced use of our HEAT ticket system.
- Ensuring all dates of terminations and transfers in the HRIS are the driver for system access decisions.
- Review of all IMT policies to ensure that our IMT practices are in alignment.

Recommendation:

Remove access for improper user accounts identified in our audit.

Upstate Response:

Upstate's IMT department has removed any improper user access identified in the audit. Upstate would like to highlight that no compromises of information were found during the audit.

Upstate appreciates the efforts of OSC during this audit period which highlighted areas for improvement while also validating existing practices required to manage user access for a workforce of over 10,000. If you have any questions regarding the response, please contact Michael Jurbala, AVP Internal Audit and Advisory Services at (315) 464-4692.

Best Regards,

Mantosh Dewan, MD
Interim President
SUNY Distinguished Service Professor

cc: Chancellor Johnson, Ph.D.
Eileen McLoughlin
Amy Montalbano

750 East Adams Street | Syracuse, NY 13210 | Ph: 315.464.4513 | Fax: 315.464.5275 | www.upstate.edu | State University of New York

Contributors to Report

Executive Team

Tina Kim - *Deputy Comptroller*

Ken Shulman - *Assistant Comptroller*

Audit Team

Brian Reilly, CFE, CGFM - *Audit Director*

Nadine Morrell, CIA, CISM - *Audit Manager*

Amanda Eveleth, CFE - *Audit Supervisor*

Holly Thornton, CFE, CISA - *Examiner-in-Charge*

Nicole Cappiello - *Senior Examiner*

Mary McCoy - *Supervising Editor*

Contact Information
(518) 474-3271
StateGovernmentAccountability@osc.ny.gov
Office of the New York State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller
For more audits or information, please visit: www.osc.state.ny.us/audits/index.htm