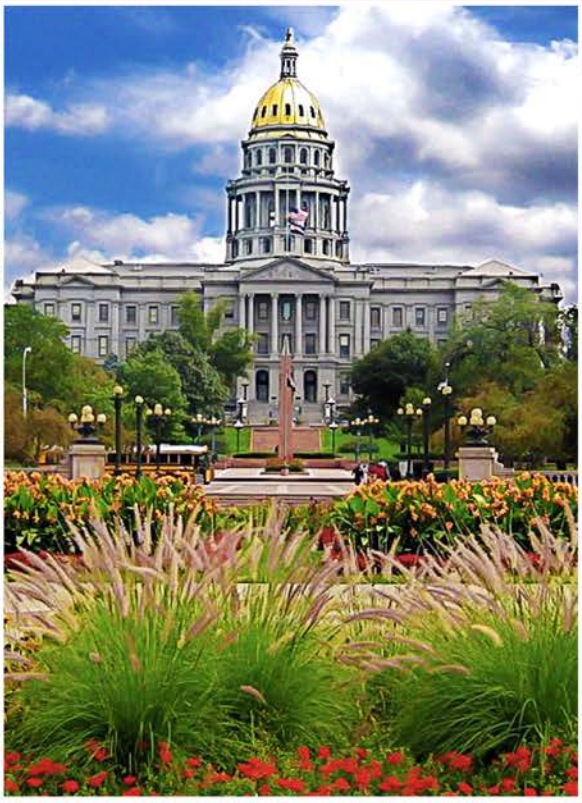
COLORADO
OFFICE OF THE
STATE AUDITOR

We Set the Standard for Good Government

DEPARTMENT OF HUMAN SERVICES, OFFICE OF BEHAVIORAL HEALTH

MANAGEMENT OF SUBSTANCE ABUSE TREATMENT DATA


FEBRUARY 2018 PERFORMANCE AUDIT

THE MISSION OF THE OFFICE OF THE STATE AUDITOR
IS TO IMPROVE GOVERNMENT
FOR THE PEOPLE OF COLORADO

LEGISLATIVE AUDIT COMMITTEE

Senator Tim Neville – Chair

Senator Kerry Donovan – Vice-Chair

Representative Tracy Kraft-Tharp
Representative Timothy Leonard
Representative Lori Saine

Senator Jim Smallwood
Senator Nancy Todd
Representative Faith Winter

OFFICE OF THE STATE AUDITOR

Dianne E. Ray	State Auditor
Monica Bowers	Deputy State Auditor
Jenny Page	Audit Manager
Carleen Armstrong	Team Leader
Meghan Westmoreland	Staff Auditors
Sarah Grider	
Cindi Radke	Other Contributor

AN ELECTRONIC VERSION OF THIS REPORT IS AVAILABLE AT
WWW.COLORADO.GOV/AUDITOR

A BOUND REPORT MAY BE OBTAINED BY CALLING THE
OFFICE OF THE STATE AUDITOR
303.869.2800

PLEASE REFER TO REPORT NUMBER 1751P WHEN REQUESTING THIS REPORT

OFFICE OF THE STATE AUDITOR

DIANNE E. RAY, CPA
STATE AUDITOR

February 28, 2018

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of the Department of Human Services (Department), Office of Behavioral Health's substance abuse treatment data and information systems. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government, and Section 2-7-204(5), C.R.S., which requires the State Auditor to annually conduct performance audits of one or more specific programs or services in at least two departments for purposes of the SMART Government Act. The report presents our findings, conclusions, and recommendations, and the Department's responses.

OFFICE OF THE STATE AUDITOR
1525 SHERMAN STREET
7TH FLOOR
DENVER, COLORADO
80203

303.869.2800

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

CONTENTS

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

REPORT HIGHLIGHTS

MANAGEMENT OF SUBSTANCE ABUSE TREATMENT DATA
PERFORMANCE AUDIT, FEBRUARY 2018

DEPARTMENT OF HUMAN SERVICES
OFFICE OF BEHAVIORAL HEALTH

CONCERN

The Office of Behavioral Health (OBH) should improve its processes for ensuring the security of the Treatment Management System (TMS), which holds data on individuals who receive substance abuse treatment, and improve its coordination with the Governor's Office of Information Technology (OIT), which develops information security policy and completes OBH's system security work requests.

KEY FINDINGS

- OBH's collection of substance abuse treatment recipient data aligns with federal and state statutes and regulations and supports OBH's role as the administrator of the federal block grant and as the State's licensing authority for substance abuse providers. OBH's processes to protect treatment recipient data include tracking recipients using unique identifiers rather than personally identifiable information, encrypting data that providers transmit to OBH, and limiting user access to TMS.

- In 2017, OBH did not terminate TMS access for three of its staff when their jobs changed or for 10 of 20 sampled providers whose licenses had expired. In addition, OBH did not maintain data use agreements for seven of its staff and 15 sampled providers, so there was no evidence that these users had agreed to protect treatment recipient data. Although no instances of improper data access or disclosure were identified, when TMS user access is not terminated in accordance with policies, there is an increased risk that treatment recipient data can be misused.

- OBH did not monitor whether TMS security scans and data destruction (for data aged 10 years) occurred annually, as required by state and OBH policies. This led to a 2-year gap in system security scans from 2015 to 2017, and data destruction occurred only once between Fiscal Years 2012 and 2018. Security scans and data destruction help ensure that systems and data are secure.

BACKGROUND

- OBH regulates, funds, and monitors substance abuse treatment and providers in Colorado; licenses providers; and administers the State's federal block grant program for substance abuse treatment.

- OBH tracks data on substance abuse treatment and individuals treated by licensed providers. OBH uses these data to meet federal and state reporting requirements, help courts track who completes court-ordered treatment, monitor licensees, assess substance abuse and treatment trends, and plan treatment and prevention programs.

- During Fiscal Year 2017, a total of 697 substance abuse treatment provider locations were licensed in Colorado and they treated approximately 65,000 people.

KEY RECOMMENDATIONS

- Implement procedures to identify the staff and providers who no longer need system access and remove access in a timely manner, work with OIT to create written policies requiring those with system access to complete data use agreement forms annually, and maintain all forms.
- Work with OIT to implement procedures and clarify staff roles for ensuring security scans occur and the results are provided to the Department, implement policies for ensuring that system-related work requests are completed as requested, and train staff on the new policies and procedures.

The Department agreed with these recommendations.

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

CHAPTER 1

OVERVIEW

The Office of Behavioral Health (OBH) within the Department of Human Services (Department) is the State's behavioral health authority [Sections 26-1-111(5) and 27-80-102, C.R.S.]. OBH is responsible for administering and overseeing Colorado's behavioral health system, which includes administering substance abuse (alcohol and drug) treatment and prevention programs in Colorado. OBH regulates, funds, and monitors substance abuse treatment and providers; administers the State's federal block grant program for substance abuse treatment; and licenses providers. In Fiscal Year 2017, OBH licensed about 300 substance abuse treatment providers at about 700 sites throughout the state.

TREATMENT DATA AND INFORMATION SYSTEMS

To carry out its responsibilities, statute authorizes OBH to collect and report data on individuals receiving substance abuse treatment from licensed Colorado providers [Section 27-81-106(4), C.R.S.]. OBH collects information on recipients' treatment from providers using OBH's Treatment Management System (TMS), which has several modules or databases. The module that is relevant to this audit is the Drug/Alcohol Coordinated Data System (DACODS), which maintains information on substance abuse treatment recipients. For example, DACODS contains statewide data on recipients' alcohol and drug use patterns, history of substance abuse, prior treatment episodes, service utilization, and outcome measures. OBH uses these data to monitor licensees, assess substance abuse and treatment trends, and meet reporting requirements. For example, every month, OBH reports de-identified aggregate DACODS data to the Substance Abuse and Mental Health Services Administration (SAMHSA) within the U.S. Department of Health and Human Services for federal block grant reporting.

OBH is responsible for granting and removing user access of TMS, while the Office of Information Technology (OIT) within the Governor's Office is responsible for the information system infrastructure and data security. OBH plans to implement a new system to replace TMS in summer 2018. The new system will be administered by a third party vendor, which will reduce OIT's role in managing system security.

FUNDING

During Fiscal Years 2015 through 2017, OBH received about $24 million in federal funds and about $22 million in state funds per year for substance abuse prevention and treatment programs. OBH's substance abuse prevention and treatment programs are primarily funded with 2-year federal block grants from SAMHSA and with state funds. The State is required to contribute a minimum amount each year

based on the average amounts the State contributed in the prior 2-year grant period. OBH maintains about 5 percent of the block grant for administration and the remaining funds are primarily used to pay providers for treatment services. OBH has about 62 full-time equivalent (FTE) management and staff who have responsibilities related to substance abuse prevention and treatment programs.

AUDIT PURPOSE, SCOPE, AND METHODOLOGY

We conducted this audit pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The audit was prompted by a legislative request, which expressed concerns about the collection and security of substance abuse treatment data. This audit was conducted from July 2017 through January 2018. We appreciate the assistance provided by the management and staff of the Department of Human Services and Office of Behavioral Health during this audit.

We conducted this 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objective of this audit was to determine whether OBH collects appropriate substance abuse treatment recipient data and reasonably protects the data against unauthorized uses and disclosures. To accomplish the objective, we performed the following audit work:

- Reviewed requirements related to Colorado's substance abuse treatment recipient data collection and reporting, including federal grant requirements, case law on data collection as part of provider licensing requirements, and Colorado information security policies.

- Analyzed DACODS treatment admissions data from Fiscal Years 2015 through 2017.

- Reviewed OBH's Fiscal Year 2017 reports to SAMHSA, the General Assembly, other state agencies, and internally to the Department.

- Evaluated OBH's policies and processes for monitoring providers, including communications and training materials related to data system access, processes for protecting data, and data destruction. This included reviewing all data use agreements on file for OBH staff.

- Examined the results of security scans of relevant TMS servers, which were completed in November 2017, and verified physical access controls of data servers. We also observed the physical access controls of OBH staff computer workstations.

- Reviewed other states' data collection practices for substance abuse treatment and prevention programs.

- Interviewed management from SAMHSA, as well as management and staff from OBH and OIT who have responsibilities related to TMS, its security, or substance abuse treatment data.

We relied on sampling to support some of our audit work and selected the following samples:

- **DATA USE AGREEMENTS.** We selected a random sample of 20 data use agreements and business associate agreements out of 488 provider locations that accessed TMS in July and August 2017.

- **PROCESS WALKTHROUGHS.** We selected a non-statistical sample of four providers for process walkthroughs—two funded by the substance abuse block grant in Fiscal Year 2017 and two not funded by the block grant. The sample was selected to ensure coverage of different provider sizes and locations. The walkthroughs reviewed the patient intake process, including processes when treatment recipients do not wish to provide personally identifiable information.

The samples were selected to provide sufficient coverage to test controls of those areas that were significant to the objectives of the audit; the sample testing results were not intended to be projected to the entire population. We designed our samples to provide sufficient and appropriate evidence for the purpose of evaluating the OBH's internal controls related to data access management.

We planned our audit work to assess the effectiveness of those internal controls that were significant to our audit objectives. Our conclusions on the effectiveness of those controls, as well as specific details about the audit work supporting our findings, conclusions, and recommendations are described in CHAPTER 2 of this report.

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

CHAPTER 2

TREATMENT RECIPIENT DATA COLLECTION AND PROTECTION

The Office of Behavioral Health (OBH) within the Department of Human Services (Department) collects and maintains data on substance abuse treatment provided by state-licensed providers. The licensed providers collect and input treatment information and recipients' data, such as name, Social Security number, date of birth, and treatment admission date, into a web-based application called the Drug/Alcohol Coordinated Data System (DACODS) which is a module within OBH's Treatment Management System (TMS). During Fiscal Year 2017, a total of 697 provider locations were licensed and served approximately 65,000 recipients.

DATA COLLECTION

Our audit assessed, in part, whether OBH's collection of substance abuse treatment recipient data, including personally identifiable information, is necessary for it to meet its statutory purpose and federal block grant requirements. We found that the OBH's data collection aligns with federal and state statutes and regulations, and appears reasonable to support OBH's role as the administrator of the federal block grant and as the statewide licensing authority for substance abuse treatment providers. We identified four key purposes for OBH's collection of substance abuse treatment recipient data and personally identifiable information, as described below.

STATUTORY AND FEDERAL BLOCK GRANT REPORTING. Federal law requires the Substance Abuse and Mental Health Services Administration (SAMHSA), the federal agency charged with reducing the impact of substance abuse in the U.S., to fund treatment programs through a federal block grant and to collect data on individuals seeking treatment through public and private nonprofit programs [42 USC 6A IIIA Part A 290aa-4(c)(1)]. In Fiscal Year 2017, about one-fourth of licensed provider locations (185 of the 697) in Colorado received federal substance abuse block grant funds through OBH. For the State to receive federal block grant funds for any provider, OBH is required to collect and report de-identified data on treatment recipients to SAMHSA monthly. These data are collectively referred to as the Treatment Episode Data Set (Data Set) and include information such as each recipient's age, gender, ethnicity, residence, admission and discharge dates for each treatment episode, count of treatment episodes, substances used, and type of service for each treatment admission. According to SAMHSA's manual on the Data Set, "the state role in submitting [the Data Set] to SAMHSA is critical, since [the Data Set] is the only national data source for client-level information on persons who use substance abuse treatment services." SAMHSA requires states to submit data, if available, on all individuals receiving treatment regardless of the payment source for treatment.

According to SAMHSA, it uses these data to monitor states, evaluate

the impact of the block grant program on treatment and prevention service performance, issue grants based on current state needs, and study substance abuse trends to inform federal behavioral health services research and policy. A SAMHSA management official that we interviewed stated that SAMHSA does not specify the types of treatment recipient data that states can collect beyond the required Data Set fields because each state system for behavioral health is unique, each state has unique powers and mandates for overseeing substance abuse treatment and providers, and significant differences exist among state data collection systems.

For example, in 2015 SAMHSA reported that 60 percent of states, including Colorado, collected data on treatment recipients funded publicly (such as through the block grant, Medicaid, Medicare, or veterans benefits) and private pay recipients because the states' behavioral health agencies license and monitor both public and private treatment providers. The remaining states collect data only on admissions financed with public funds for a number of reasons such as because their state behavioral health agency does not have the authority to oversee private facilities or individual practitioners, and/or because treatment is administered by the criminal justice system rather than the state behavioral health agency.

STATE CRIMINAL JUSTICE REPORTING AND MONITORING. If a court order requires an individual to complete a substance abuse treatment program, providers must enter the treatment recipient's information into DACODS. These data are used by Judicial Branch and other state officials to verify that a recipient completed the required treatment. According to OBH, the recipient's name, date of birth, and Social Security number are collected and tracked in DACODS to correctly match the recipient's DACODS record to the court record.

PROVIDER LICENSING AND QUALITY MONITORING. DACODS tracks treatment recipient clinical assessment information, such as the licensing location, days the recipient waited to begin treatment, disability accommodations, and the clinician's assessment of the severity of a substance abuse disorder prior to treatment. These data are

collected so that OBH can monitor treatment provider performance and compliance with licensing and grant requirements, which include appropriate billing. In addition, OBH staff use treatment recipient dates of birth and Social Security numbers to check that providers are not double billing both the block grant and Medicaid.

PROGRAM EFFICACY AND MANAGEMENT. To carry out its responsibilities, statute authorizes OBH to collect and report data on individuals receiving substance abuse treatment and on the costs and effectiveness of substance abuse treatment programs in Colorado [Sections 27-81-106(4) and 27-80-110, C.R.S.]. OBH collects demographic and clinical treatment information to analyze substance use and recidivism trends, payment methods, and reasons for treatment; help plan prevention and treatment programs across the state; allocate funding to providers; and identify service needs. To analyze statewide trends, determine treatment outcomes, and track whether the same individuals seek treatment multiple times, OBH uses de-identified treatment recipient data using a unique identifier. For example, in Fiscal Year 2017, OBH compiled information on opioid treatment trends across the state to apply for a SAMHSA grant for opioid emergency response funds, and was awarded a $7.8 million grant to pay for medication-assisted therapy, overdose reversal medications, crisis services, training for doctors and nurses, and residential treatment.

OBH also provides de-identified substance abuse information on statewide substance abuse trends, treatment outcomes, and service needs to the General Assembly and other governmental entities, such as the Department of Public Health and Environment, the Judicial Branch, and local governments, to help these entities evaluate program performance and determine whether state funding is meeting statewide needs for the prevention and treatment of substance abuse. For example, in Fiscal Year 2017, OBH provided aggregate, de-identified substance abuse data on:

- The number of individuals who use detox programs multiple times (at the request of the Joint Budget Committee).

- Treatment admissions by drug type (to the Office of State Planning and Budgeting and various local health departments).

- Individual treatment outcomes and recidivism (to jail-based behavioral health services programs).

While most individuals for whom OBH collects data receive public funds for treatment or are required to obtain treatment by the courts, most licensed providers treat both individuals who receive public funds and who self-pay or are covered by private insurance. The legislative request that prompted this audit raised questions about whether OBH needed to collect data from individuals who self-pay or who are covered by private insurance, and the potential consequences of limiting the OBH's current data collection practices.

According to OBH staff and our audit work, limiting OBH's collection of treatment data would impede its ability to comply with federal requirements, as OBH is required to collect and submit all available treatment recipient data regardless of the payment source, and would reduce OBH's ability to monitor licensed providers, research substance abuse, and report to stakeholders. For example, from Fiscal Years 2015 through 2017, between 27 and 49 percent of recipients who voluntarily received opioid treatment were self-pay or covered by private health insurance. By not collecting data on those who self-pay, OBH would have incomplete data needed for monitoring, and the data would not accurately reflect statewide trends, such as the number of treatment admissions and the services provided, or recipient-level trends such as recipients' substance abuse and recidivism history. Finally, according to several treatment providers that we interviewed, individuals move on and off public funding for treatment as their employment status or ability to pay changes, or when public funding covers a portion of their treatment. Requiring providers to only collect and submit data on an individual's treatment when a recipient is publicly funded could be difficult to administer.

CONTROLS OVER DATA PROTECTION

Treatment recipients' personal health information, such as their history

of substance abuse and diagnosis, should be protected by treatment providers and governmental agencies to ensure recipients' privacy. Under federal regulations, organizations that collect and have access to personal health information are required to protect that information to ensure that an individual receiving treatment for a substance use disorder is not made more vulnerable by the availability of their treatment record than an individual who does not seek treatment [42 CFR 2.2(b)(2)]. As the statewide organization that collects and monitors treatment recipient data, OBH must have internal controls, such as written policies, procedures, and systems, to reasonably protect against unauthorized uses and disclosures of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information [42 CFR 2.16].

We assessed OBH's processes for protecting data on treatment recipients and identified several controls that OBH has implemented to protect recipients' personally identifiable information and to ensure the security and integrity of recipient data. These controls include:

- Assigning a unique identifier to each individual treatment recipient, rather than using the recipient's name or other personally identifiable information to track their treatment.

- Requiring users with access to TMS to sign written agreements stating that the data must be kept confidential.

- Limiting data system access to a few staff at each provider location and restricting those users' access to treatment records for their location only.

- Removing information that could specifically identify treatment recipients, such as the date of birth and Social Security number, and encrypting the data when OBH transmits it to SAMHSA.

- Encrypting data that is transmitted from providers to TMS.

- Training OBH staff and treatment providers on appropriate use of

the system and data collection procedures.

- Removing identifying information and aggregating data when using it for research and when providing informational reports to external parties, such as the General Assembly.

- Substituting data values for actual client information when treatment recipients do not wish to provide personally identifiable information, such as their Social Security number, to a provider. For example, the DACODS user manual requires provider staff to enter a mock number instead of the recipient's Social Security number.

Providers we interviewed reported that they understood OBH's data collection requirements, were knowledgeable about how to use DACODS, and explained that treatment recipients sometimes refuse to provide personal information such as the date of birth or Social Security number. The providers reported that their priority is to provide treatment and that a recipient's refusal to provide personal information is not a barrier to treatment.

In 2018, OBH plans to replace TMS, including DACODS, with a new system. According to OBH management, the new system will include many of the same controls as TMS, including assigning a unique identifier to treatment recipients. In addition, the system will include features that should enhance the protection of treatment recipient data, such as encrypting the data at rest, assigning system access roles based on job functions, and automating password management so that each user will have its own unique ID and password.

Although OBH collects treatment recipient information needed to fulfil its statutory, regulatory, and oversight responsibilities and has some processes to reasonably protect the data, we found that OBH needs to improve its controls over user access to TMS and the DACODS data within it, and its processes for ensuring TMS and its data are secure. We discuss these findings and recommendations in the remainder of CHAPTER 2.

TREATMENT MANAGEMENT SYSTEM USER ACCESS CONTROLS

OBH is responsible for granting and removing user access to TMS. OBH has established a process for its staff and provider staff to sign data use agreements; some providers also sign business associate agreements related to protecting Health Insurance Portability and Accountability Act (HIPAA) data. Providers access TMS to input data and track recipients' treatment, while OBH staff access the data to monitor providers and compile data that is primarily used for federal and state reporting. According to OBH staff and providers we interviewed, a provider can only access the records of the treatment recipients who received treatment from the provider's specific building location.

WHAT WAS THE PURPOSE OF THE AUDIT WORK AND WHAT WORK WAS PERFORMED?

The purpose of the audit work was to determine whether OBH is controlling user access to TMS, in line with all federal, state, and OBH requirements. We requested and reviewed all data use agreements on file for OBH staff as of September 2017, as well as the agreements on file for a random sample of 20 of 488 providers that accessed TMS in July and August 2017. We also reviewed TMS access logs for the 488 providers who accessed the system in July and August 2017, and compared the logs to OBH's list of 697 licensed providers. We reviewed regulations and OBH procedures related to system user access. To determine processes for granting system access and OBH staffs' and providers' understanding of data confidentiality and protection, we interviewed OBH staff and a sample of staff from seven providers, all of whom accessed TMS.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

TERMINATION OF SYSTEM ACCESS. OBH does not have written policies related to user access to TMS, but management described two practices that it uses to terminate access to the system:

1 OBH removes access to TMS when a staff member leaves employment or when his or her job no longer requires system access.

2 OBH removes TMS access for providers when the provider location closes or is no longer licensed.

SYSTEM ACCESS AND DATA PROTECTION AGREEMENTS. Colorado Information Security Policies (Security Policies) require:

1 The state agency that owns the system and the Office of Information Technology (OIT) to establish user access policies that describe system users' responsibilities and expected behavior regarding accessing and using data on the system. OIT should review and update these policies annually [CISP-001, 9.16.1 and 9.16.4].

2 System users to sign a form annually acknowledging that they have read, understand, and agree to follow these user access policies [CISP-001, 9.16.2 and 9.16.5].

3 The state agency that owns the system to retain the signed acknowledgements [CISP-001, 9.16.3].

According to OBH management, it requires new staff and providers to sign a data use agreement, which contains information regarding access to and confidentiality of records, before they receive access to TMS. One agreement is typically signed per provider location and one provider staff has user access; however, in some instances a provider has multiple staff who need user access at one location, so each of the staff sign an agreement. The agreement form includes space for the user to sign and for the OBH security administrator to sign approving the

access, and for the dates of the signatures. In addition, OBH requires each licensed provider to sign a business associate agreement acknowledging that it will comply with HIPAA requirements to protect confidential health information, and OBH also signs this agreement. Because each of the 20 providers in our sample had one staff who could log into TMS, we expected OBH to have 20 annual data use agreements and 20 business associate agreements on file for each sampled provider. We also expected OBH and providers to sign business associate agreements at approximately the same time.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

Overall, we identified OBH staff and providers with TMS access that was unnecessary and noncompliant with Security Policies regarding data use and business associate agreements, and agreements that were insufficient to protect treatment recipient data. EXHIBIT 2.1 summarizes the problems.

EXHIBIT 2.1. PROBLEMS IDENTIFIED RELATED TO USER ACCESS

PROBLEM DESCRIPTION	NUMBER OF PROBLEMS IDENTIFIED FOR 25 OBH STAFF	NUMBER OF PROBLEMS IDENTIFIED FOR 20 SAMPLED PROVIDERS
TMS access was not terminated for users	3	10
Users accessed TMS without agreements	7	15
Users with outdated agreements	14	16
Data use agreements not signed by OBH security administrator	24	10
Agreements lacked data protection and confidentiality requirements	25	17

SOURCE: Office of the State Auditor analysis of user access data and documentation.

The specific problems that we identified are as follows:

- **SYSTEM ACCESS WAS NOT PROPERLY TERMINATED FOR THREE OBH STAFF.** We identified three of the 25 OBH staff with the ability to access TMS in 2017 who no longer needed access because they

changed job positions within OBH. During the course of our audit, OBH terminated the staffs' access, but the staff had unnecessary access to TMS for between 3 and 5 months.

- **System access was not properly terminated for 10 providers.** We identified 10 of the 488 providers that accessed TMS in July and August 2017 whose licenses had been expired for between 2 months and 5 years. Four of the providers had treatment recipient records in TMS while the remaining providers did not. According to OBH staff, the six providers who accessed the system but did not have system records could have logged in using an expired user ID or OBH staff could have logged into the system using the provider's user ID to provide technical assistance. OBH reported to us that the providers with expired licenses which had accessed TMS were not able to view treatment recipient data, and we verified that the five providers which still had expired licenses in December 2017 could not access the data; the remaining five providers had renewed their licenses and were granted access to the data. The Department also reported to us that it plans to develop a process to prevent expired licensees from accessing TMS altogether.

  We also identified two providers that accessed TMS but were not in OBH's database of licensed providers. According to OBH staff, these providers were licensed and had appropriate access to TMS, but were not in OBH's provider database at the time of our testing because of administrative delays in updating the database.

- **Some OBH staff who accessed TMS did not have signed data use agreements, or had outdated agreements.** OBH did not have data use agreements on file for seven of the 25 OBH staff who had user access to TMS. Four of them needed TMS access as part of their job responsibilities, but OBH could not find their agreements, so it had the staff sign new agreements after we brought the problem to OBH's attention. The remaining three staff without agreements had changed jobs within OBH and their access was removed, as described above. In addition, 14 of the 18 data use agreements that OBH had on file at the time of our request were at least 1 year old.

One of the agreements was not dated and the remaining 13 were signed between 2007 and 2016. These agreements should be reviewed and signed annually to comply with Security Policies [CISP-001, 9.16] regarding access control.

- **MOST SAMPLED PROVIDERS WHO ACCESSED TMS DID NOT HAVE BOTH SIGNED AGREEMENTS, OR HAD OUTDATED AGREEMENTS.** We found that only five of the 20 providers in our sample had signed both the data use agreement and business associate agreement as required by OBH, and that there were problems with all of the agreements that were in place. Specifically:

  - Three providers did not have a data use agreement or a business associate agreement.

  - Seven providers had a business associate agreement only; five providers had a data use agreement only.

  - Nine providers' data use agreements and 10 providers' business associate agreements were at least 1 year old; the agreements were signed between 2008 and 2015. User agreements should be signed annually to comply with Security Policies [CISP-001]. Although there is no requirement for the HIPAA business associate agreements to be signed by providers annually, this would be a best practice.

  - Six of the business associate agreements were signed by the provider at least 1 year after they were signed by OBH. For example, OBH signed one agreement in June 2009, but the provider did not sign it until September 2014, indicating that the provider had access to confidential data before signing an agreement.

- **NO DATA USE AGREEMENTS HAD BEEN SIGNED BY THE OBH SECURITY ADMINISTRATOR.** For all 34 OBH staff and provider data use agreements we reviewed, the signature line for the OBH security administrator to sign granting access was blank. According to OBH staff, this signature line had not been used, and thus there was no documentation that user access for TMS had been approved.

- **OBH'S WRITTEN AGREEMENTS DO NOT SUFFICIENTLY ADDRESS CONFIDENTIALITY REQUIREMENTS.** We found that OBH's data use and business associate agreements do not sufficiently notify users of the requirements to protect recipient data or describe the user's responsibilities for protecting TMS. Specifically:

  - The data use agreement refers to state policies that were repealed in 1987 and does not reference the federal regulations requiring protection of substance abuse treatment recipient data.

  - The business associate agreement, which is meant to protect HIPAA data, does not address confidentiality requirements for substance abuse treatment under the federal regulations and contains different data retention requirements than OBH's policy for DACODS. For example, the business associate agreement contains a provision for providers to maintain data for 6 years, while the data retention policy for DACODS requires the data, which may contain HIPAA data in certain circumstances, to be kept for 10 years.

WHY DID THESE PROBLEMS OCCUR?

OBH has not established written policies and procedures that outline the controls over user access to TMS or users' responsibilities when accessing system data, as required by Security Policies. Currently, OBH has no written policies or procedures related to the following critical controls:

- **CHECKING AND REMOVING USERS' SYSTEM ACCESS.** OBH does not have a procedure for a security administrator to sign data use agreements documenting approval of users' system access. Further, OBH has no written policies or procedures requiring OBH staff who grant and remove system access to regularly review access to TMS to identify those OBH staff and providers who no longer need access and to remove their access. For example, OBH does not require a regular comparison of the provider licensing list to TMS access logs, or have a written policy or procedure to remove access within a specified time after determining access is no longer needed. Although OBH has a process to restrict

users' ability to view records, this control relies on manual data entry and there is a risk of data entry error. OBH staff responsible for terminating user access reported to us that they rely on (1) word of mouth from other OBH staff to learn about changes in staff job positions and (2) notification from providers or other OBH staff about a provider closing or not being licensed. A better control for identifying the users whose access should be terminated would be a periodic process, such as biannual or annual, which compares OBH staff user access to their job responsibilities to ensure access is necessary, and which checks the status of all licensed providers and immediately removes a provider's access when it closes or its license expires.

- **ENSURING THAT THOSE WITH ACCESS UNDERSTAND AND AGREE TO COMPLY WITH INFORMATION SECURITY REQUIREMENTS.** OBH management reported to us that they believed OBH was exempt from compliance with the Security Policies requiring annual signed acknowledgements for system users. Consequently, OBH has not established written policies that describe TMS user responsibilities and expected behavior regarding data usage, such as protecting the data from disclosure or misuse. OBH does not have a procedure to annually require all users to acknowledge they have read, understand, and agree to follow these policies or conditions before receiving access to the system, or a process for consistently maintaining the acknowledgments. Also, OBH does not have a policy or procedure to periodically update the standard data use and business associate agreements to accurately reflect current, applicable requirements for protecting substance abuse treatment recipient data.

  In addition, OBH does not follow its own procedure for requiring providers to sign both a data use agreement and business associate agreement before granting access to TMS. OBH staff reported to us that significant turnover of Department staff who oversee HIPAA compliance contributed to misunderstanding about which agreements providers should sign. Staff could not explain why some providers did not sign both agreements. Establishing one standard agreement form that covers all federal, Security Policies, and OBH requirements for provider data use and confidentiality would be an efficient control.

WHY DO THESE PROBLEMS MATTER?

When OBH does not have sufficient internal controls for removing TMS user access for OBH staff and providers, and ensuring system users understand their responsibilities for protecting treatment recipient data, OBH is not reasonably protecting the data from improper use and disclosure. While we did not identify instances of OBH staff improperly accessing or disclosing data, we did identify providers that were able to access the system after their licenses had expired. By not terminating OBH staff and provider access to TMS, when appropriate, OBH has an increased risk of fraud or misuse of substance abuse treatment recipient data.

When OBH does not have policies for system users to review and sign clear, comprehensive user agreements or business associate agreements each year, it misses a key opportunity to inform users of requirements related to protecting data, promote their understanding of the requirements, and document their acknowledgement that they will comply with the requirements. Further, fostering understanding and acceptance of the requirements through the agreements supports accomplishment of the intent of Security Policies [CISP-001], which were established to ensure consistency in information security across the State and help reduce security risks that can be caused by agency staff.

Finally, by not having written policies around data security, OBH is out of compliance with federal regulations and Security Policies. Federal regulations require entities that maintain substance abuse treatment records to have "formal policies and procedures to reasonably protect against unauthorized uses and disclosures of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information" [42 CFR 2.16(a)]. Failure to comply with federal regulations creates a risk that substance abuse treatment recipient data could be misused; for example, a treatment recipient's health records or Social Security number could be disclosed. Similarly, Security Policies [CISP-001, 9.16] require state agencies, including OBH, to establish policies regarding user access to systems which describe staffs' and providers' responsibilities and

expected behavior when using information on state computing resources. By not complying with Security Policies [CISP-001, 9.16], OBH risks the suspension of TMS' operation. According to the Security Policies [CISP-001], the State's Chief Information Security Officer can temporarily suspend the operation of TMS until OBH is in compliance.

RECOMMENDATION 1

The Department of Human Services (Department) should ensure that the Office of Behavioral Health (OBH) improves controls over system user access and protection of substance abuse treatment data by:

A Establishing and implementing written policies and procedures for identifying the staff and providers who no longer need user access, such as biannually or annually, and removing access in a timely manner.

B Working with the Governor's Office of Information Technology to create written policies for data use and system access that are reviewed and updated annually. The policies should require (1) staff and providers with system access to annually complete a written acknowledgement agreement signifying they have read, understand, and agree to follow applicable information security and data confidentiality requirements; (2) new staff and providers to sign the acknowledgement form before receiving access to the system; and (3) the Department to maintain all forms.

C Developing an acknowledgement agreement for system and data users which contains current and accurate information security requirements, user responsibilities for protecting data, and a process for updating the form periodically. In addition, OBH should consider utilizing one standard agreement that includes all applicable requirements and user responsibilities, and is signed by all providers and OBH staff.

RESPONSE

DEPARTMENT OF HUMAN SERVICES

A AGREE. IMPLEMENTATION DATE: JULY 2018.

The Department of Human Services (Department) will ensure that the Office of Behavioral Health (OBH) improves controls over system user access and protection of substance abuse treatment data by implementing a written policy to identify and remove staff and providers that no longer need user access. For OBH staff, identification and removal of unused or unnecessary user access will be done through an annual review of users. For providers, identification and removal of unused or unnecessary user access will be done annually. Based on the reviews, access will be removed in a timely manner as defined in the new policy.

B AGREE. IMPLEMENTATION DATE: JULY 2018.

The Department of Human Services (Department) will ensure that the Office of Behavioral Health (OBH) improves controls over system user access and protection of substance abuse treatment data by working with Department staff and the Governor's Office of Information Technology staff to create a written policy for data use and system access that will be reviewed and updated annually. OBH staff will sign the mutually agreed upon acknowledgment form annually as part of their continued access to the system. New OBH staff and new providers will sign the acknowledgment form before being granted access to the system. Existing providers will sign the acknowledgment form annually as part of their continued access to the system. The signed acknowledgment forms will be maintained by OBH as defined in the new policy.

C AGREE. IMPLEMENTATION DATE: OCTOBER 2018.

The Department of Human Services (Department) will ensure that the Office of Behavioral Health (OBH) improves controls over

system user access and protection of substance abuse treatment data by developing a standard agreement(s) that will include current and accurate information security requirements, user responsibilities for protecting data, and a process for updating the acknowledgement agreement(s) periodically. OBH will work with Department staff and Governor's Office of Information Technology staff to determine if one standard agreement is possible. Initial conversations indicate that a standard agreement may not be feasible, but OBH will ensure that the process is simplified.

SYSTEM AND DATA SECURITY

According to statute, OBH is responsible for licensing providers that provide substance abuse treatment and receive public funds (e.g., federal block grants, Medicaid, and Judicial Branch vouchers) or dispense controlled substances [Sections 27-81-106(1) and 27-80-204(1)(a), C.R.S.]. As part of licensing, OBH requires providers to collect information about the individuals who receive substance abuse treatment and submit the information into TMS.

Responsibilities for managing TMS, including DACODS, are divided between OBH and OIT. OBH is the owner of the data stored in TMS and is responsible for granting and removing user access, submitting work orders to OIT for system changes, providing technical support for system users, and checking the validity of data entered into TMS. OIT is responsible for completing system change work orders, developing and implementing a system security plan for TMS, and ensuring that the plan complies with Security Policies. The system security plan outlines the system controls, such as password requirements, log-in timeout intervals, and system patches that help ensure the security and integrity of the data in the system. OIT is also responsible for assessing system and server security by installing software patches and conducting security scans that identify system vulnerabilities.

In the summer of 2018, OBH plans to implement a new system for tracking substance abuse and mental health treatment, which will replace TMS. OBH, through OIT, contracted with a third party vendor to develop and administer the system and maintain its security.

WHAT WAS THE PURPOSE OF THE AUDIT WORK AND WHAT WORK WAS PERFORMED?

The purpose of the audit work was to determine whether TMS security

assessments and DACODS data destruction were occurring according to state and OBH policies. We reviewed OBH's system security plan for TMS, documentation of the work orders that OBH submitted to OIT during Fiscal Years 2017 and 2018, the results of the work orders, and documentation of the data destruction of DACODS treatment recipient records in Fiscal Year 2017. We reviewed Security Policies and OBH policies and procedures related to system security and data destruction. We also interviewed OBH and OIT staff to understand processes for work orders related to TMS and DACODS, what security assessments had been completed for TMS, and what data destruction had been completed for DACODS in Fiscal Years 2017 and 2018.

The scope of our audit was to evaluate OBH's management of system and data security, and not to evaluate OIT's operations. As such, in those cases where we found that OIT had not carried out tasks in accordance with Security Policies or with OBH work orders, our findings and recommendations address OBH's responsibilities. We do not make recommendations to OIT in this audit.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

OBH IS RESPONSIBLE FOR MONITORING AND PRIORITIZING WORK ORDERS RELATED TO SECURITY SCANS AND DATA DESTRUCTION FOR ITS SYSTEMS. Security Policy [CISP-004] requires OBH, as the data owner, to prioritize its project work orders and follow up with OIT about whether the work orders and security assessments have been completed. Security Policies [CISP-004, 9.1.2 and 9.1.3] require OIT to assess the security controls and the operational environment of agency systems annually and correct any vulnerabilities that it identifies. According to OIT staff, assessing the security controls and operational environment of TMS should include updating system security policies as well as inspecting the system for security vulnerabilities by conducting annual scans of the servers that host TMS. Security Policies [CISP-004, 9.1.3] require OIT to document the results of the assessment and distribute the results for action, planning, or remediation and to assist the organization that

owns the system to understand its risk posture. In addition, Security Policies [CISP-004, 8.3.7] require OBH, as the owner of TMS, to ensure that OIT is providing appropriate status information and explanation of work orders and system administration.

To assess OBH's compliance with its responsibilities, we reviewed how it (1) monitored whether the annual assessments were being completed by OIT; (2) obtained the results of the assessments and determined what system corrections, if any, were needed; and (3) communicated other system needs to OIT and monitored OIT's completion of any work requested.

OBH POLICY REQUIRES ANNUAL DATA DESTRUCTION. In Fiscal Year 2012, OBH developed a data retention and destruction policy for records contained in TMS. According to this policy, substance abuse treatment recipient data stored in DACODS must be deleted 10 years after the recipient's discharge date. To initiate data destruction, OBH staff submit a work order to OIT at the beginning of each fiscal year requesting deletion of all records that are within the destruction period.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

We found that annual system security scans of the server hosting TMS and the destruction of data for DACODS have not occurred annually. First, OIT updated policies but did not conduct any other annual system security assessment of TMS, including scans, between December 2015 and November 2017, which is out of compliance with Security Policies. According to OIT staff, they had intended to start the security scan process at the beginning of our audit in July 2017; however, we found that OIT did not conduct the scans until October 2017, after we had requested the scan results. Thus, the server hosting TMS has not undergone a security scan in nearly 2 years.

Second, only one annual data destruction for DACODS has occurred since OBH approved its data retention and destruction policy in Fiscal

Year 2012. The only data destruction was in Fiscal Year 2017, about 5 years after OBH implemented its policy. The Fiscal Year 2017 destruction deleted all records for treatment recipients who had a discharge date prior to Fiscal Year 2007. We found that no annual data destruction had occurred for Fiscal Year 2018 as of January 2018, so records from Fiscal Year 2007 still exist in DACODS.

WHY DID THESE PROBLEMS OCCUR?

OIT could not explain why it did not conduct the required annual scans or the data destruction, other than it made a mistake and had forgotten about the data destruction work orders. OBH staff reported to us that OIT does not provide any written results of its security assessments as required by Security Policies [CISP-004, 9.1.3], and discusses the security scans only if there are critical issues found. OBH staff told us that they were unaware that they are responsible for following up with OIT to check the status of system security assessments and the results. OBH staff stated that they have monthly meetings with OIT but the security assessment is not discussed.

With respect to the lack of annual data destruction, OBH staff told us that they had submitted work orders to OIT for the data destruction in Fiscal Years 2013, 2014, 2015, and 2016, and that the destruction process was delayed beginning in 2013 because OBH asked OIT to prioritize the implementation of a new data system ahead of conducting the data destruction, and due to understaffing at OIT. However, OBH was unable to provide documentation of its work orders, and when no deletion had been completed for Fiscal Years 2013 through 2016, OBH did not communicate to OIT that data destruction still needed to occur or follow up to ensure that the data were deleted. OBH staff told us that they were not aware that they needed to ask OIT to prioritize the data destruction after it had requested the delay and that no data destruction had been completed for Fiscal Year 2017.

Overall, OBH has not developed sufficient procedures to communicate with OIT regarding system security administration or staff roles for ensuring that annual system security assessments occur. In addition, OBH does not have written policies or procedures that reflect its

responsibilities for adherence to Security Policy requirements such as policies requiring staff to (1) obtain the results of security assessments from OIT, (2) work with OIT to determine how to remediate security vulnerabilities when they are found during assessments, and (3) monitor work orders and follow up with OIT to ensure that they are completed.

WHY DO THESE PROBLEMS MATTER?

The lack of controls over the assessment of system security for TMS creates a risk that OBH and OIT are not reasonably ensuring that treatment recipient data, which contains sensitive personal information and health records, are secure. When OBH does not follow up with OIT to request information about security scans, there is a risk that security scans will not be performed and system vulnerabilities will not be detected. In addition, if OBH does not follow-up to review the results of the required security scans and work with OIT to address vulnerabilities, there is a risk that treatment recipient records, which contain names, birthdates, Social Security numbers, and substance abuse treatment information, could be accessed without authorization and misused without detection.

When OBH does not comply with its data retention and destruction policy, it creates a risk that health records that should have been deleted, and are no longer necessary for research or audit purposes, can still be accessed and potentially mishandled. Additionally, according to a 2012 court order, OBH must have a data destruction policy to require providers to submit treatment recipient data into DACODS. If OBH has not fully implemented its policy, then it may not be in compliance with the intent of the court order. Failure to adhere to the intent of the court order could put OBH's authority to require providers to submit treatment recipient data at risk and prevent OBH from obtaining data it needs to monitor licensed providers.

If OBH does not maintain documentation of its work order requests, monitor their status, and follow up on the results of work orders, then OBH lacks mechanisms to check whether OIT meets deadlines or completes required work. The new system vendor in 2018 will need to

comply with Security Policies and OBH policies and report that compliance to OBH and OIT. OBH will be responsible for working with OIT to oversee the vendor to ensure compliance with Security Policies, including maintaining system security, and holding the vendor accountable if it fails to comply with the terms of the contract.

RECOMMENDATION 2

The Department of Human Services (Department) should ensure that the Office of Behavioral Health's (OBH's) substance abuse treatment data are secure by:

A Working with the Governor's Office of Information Security (OIT) to implement procedures and clarify staff roles for ensuring annual system security assessments occur, as required by Colorado Information Security Policy (Security Policy), and for ensuring that the results of the assessments are provided to the appropriate Department staff so that any security vulnerabilities can be remediated.

B Implementing written policies and procedures that specify the Department's responsibilities for ensuring compliance with Security Policy and that require OBH staff to (1) document work orders submitted to OIT or the third party vendor, and (2) follow up to ensure work orders are completed as requested.

C Training OBH staff on the new policies and procedures recommended in PARTS A and B.

RESPONSE

DEPARTMENT OF HUMAN SERVICES

A AGREE. IMPLEMENTATION DATE: JULY 2018.

The Department of Human Services (Department) will ensure that the Office of Behavioral Health's (OBH's) substance abuse treatment data are secure by working with the Governor's Office of Information Technology (OIT) to implement procedures to clarify both staff roles for ensuring annual system security assessments occur and that the results of the assessments are provided to the appropriate Department staff. OBH has already begun discussions with OIT to ensure that security assessment scans are done in a timely manner and that results are shared with the necessary Department and OBH staff. All security assessment scans are being followed up on by OBH staff to ensure proper resolution. Upon completion of this process refinement with OIT staff, procedures for follow-up and the clarification of staff roles will be written and standardized.

B AGREE. IMPLEMENTATION DATE: OCTOBER 2018.

The Department of Human Services (Department) will ensure that the Office of Behavioral Health's (OBH's) substance abuse treatment data are secure by standardizing and implementing a written policy and procedures that specify the Department's responsibilities for ensuring compliance with the Security Policy and following up to ensure work orders are both documented and completed. The policy will include work orders submitted to the Governor's Office of Information Technology or a third party vendor.

C AGREE. IMPLEMENTATION DATE: OCTOBER 2018.

The Department of Human Services (Department) will ensure that the Office of Behavioral Health's (OBH's) substance abuse treatment data are secure by ensuring that all necessary staff have been properly trained on the new policies and procedures established as a result of

this audit. A staff presentation will be given to necessary OBH staff to ensure awareness of the new policies and procedures. In depth training will occur with OBH's Data and Evaluation staff to ensure understanding and compliance with all new policies and procedures.