DEPARTMENT OF COMMERCE
Division of Occupational and Professional Licensing

Information Systems Audit of the
Controlled Substance Database
August 13, 2018

Report No. IT 18-01

OFFICE OF THE
STATE AUDITOR

AUDIT LEADERSHIP:
John Dougall, State Auditor
Ethan Heintzelman, CPA, CISA, Director
Leif Elder, MPA, Manager
TABLE OF CONTENTS

BACKGROUND:

Controlled Substance Database Act 1
Purposes of the Controlled Substance Database (CSD) 1
Access to the CSD 2
CSD Patient Dashboard 3

AUDIT OBJECTIVES, SCOPE, METHODOLOGY, AND LIMITATIONS 5

FINDINGS:

1. Inadequate CSD Password Requirements Do Not Comply with DOPL Policy 7
2. Password Requirements for Back-end CSD Users Do Not Conform to Required DTS Policy 8
3. Several Unlicensed Individuals Received CSD Accounts Without Proper Approval 9
4. CSD User Accounts Are Not Periodically Reviewed for Appropriateness 10
5. Practitioners with Expired Licenses Were Improperly Allowed to Perform Queries in the CSD 11
6. Management Has Not Defined Activities That Should Be Monitored 12
7. Inadequate Monitoring of User Activity 13
8. Insufficient Monitoring of Testing Documentation for Application Changes Prior to Deployment 14
9. Data Retention Policy Exposes DOPL to Unnecessary Risk 15

DOPL’s RESPONSE TO HOW IT FULFILLS CSD REQUIREMENTS AND PURPOSES APPENDIX A

DOPL’s RESPONSE TO FINDINGS APPENDIX B
Background

Controlled Substance Database Act

In 1995, the Utah Legislature passed and the Governor signed S. B. 42, Controlled Substance Prescription Database Provisions, which statutorily created the Controlled Substance Database (CSD).

The Legislature significantly bolstered the statutory provisions governing the CSD in 2010 by enacting the Controlled Substance Database Act (Act).

The Act requires the Department of Commerce’s Division of Occupational and Professional Licensing (DOPL) to “administer and direct the functioning” of the CSD.

The Department of Technology Services (DTS) assists DOPL in operating and maintaining the database.

Additionally, the Utah State Board of Pharmacy is tasked with advising DOPL regarding operating and maintaining the database and accessing and controlling the information therein.

Purposes of the Controlled Substance Database

Utah Code outlines specific purposes for the CSD, and mandates the submission and collection of certain data “for each controlled substance dispensed by a pharmacist under the pharmacist’s supervision other than those dispensed for an inpatient at a health care facility.” Appendix A lists DOPL management’s response to how DOPL fulfills CSD data requirements and purposes as outlined in Utah Code.

According to the Act, the CSD was created to facilitate the identification of the following issues with respect to controlled substances:

- Patterns of prescribing and dispensing;
- Practitioners prescribing in an unprofessional or unlawful manner;
- Individuals receiving prescriptions in quantities or frequencies inconsistent with generally recognized standards;
- Individuals presenting false prescriptions to a pharmacy;
- Individuals admitted to a general acute hospital for poisoning or overdose; and
- Individuals convicted for driving under the influence or impaired driving.

1. Laws of Utah, 1995 General Session, Ch. 333.
2. Laws of Utah, 2010 General Session, Ch. 287.
Pharmacists are required to make a daily report to DOPL regarding the controlled substances the pharmacists dispense “other than those dispensed for an inpatient at a health care facility.”

DOPL mandates that several data fields be included in the report, such as:

- Patient name, address, and date of birth;
- Date the prescription was written and dispensed;
- Controlled substance identification number;
- Number of refills authorized and the refill number being dispensed;
- Number of days the prescription covers;
- Identity of pharmacist and prescribing practitioner; and
- Name, type of ID used, and ID number for the individual picking up the substance.

Access to the CSD

Access to the CSD is restricted by statute to approximately twenty specific categories of individuals, including DOPL employees, licensed medical practitioners, and pharmacists. Each group is subject to specific limitations and requirements regarding access to the data. Furthermore, DOPL is required to track who accesses the database and what information the individual receives. As of June 30, 2016, DOPL reported over 70 million prescription records housed within the CSD which are accessible to over 20,000 registered CSD users (see Table 1).

<table>
<thead>
<tr>
<th>Table 1: Controlled Substance Database by the Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Prescription Records as of 06/30/2016</td>
</tr>
<tr>
<td>Total Prescriptions Entered in FY 2016</td>
</tr>
<tr>
<td>Registered Pharmacist Users</td>
</tr>
<tr>
<td>Registered Prescribing Practitioner Users</td>
</tr>
<tr>
<td>Other Registered Users</td>
</tr>
<tr>
<td>Searches Performed between 11/1/16 and 10/31/17</td>
</tr>
</tbody>
</table>

Source: Auditor analysis of the CSD and Utah Department of Commerce 2016 Annual Report.

Utah law requires a “valid search warrant” for “federal, state, and local law enforcement officers” to access the database. However, on July 27, 2017, a federal judge ordered the state to comply with administrative subpoenas issued by the Drug Enforcement Administration.

---

9 Utah Code § 58-37f-203.
11 Utah Code § 58-37f-301(2).
12 Utah Code § 58-37f-203(7).
14 Utah Code § 58-37f-301(2)(m).
The Act requires DOPL to both (1) “effectively enforce the limitations on access to the [CSD]” and (2) “establish standards and procedures to ensure accurate identification of individuals requesting information or receiving information without request from the [CSD].”\(^{16}\) Intentional unauthorized access or misuse of CSD data is classified as a third-degree felony.\(^{17}\)

**CSD Patient Dashboard**

Particularly noteworthy is the “CSD Patient Dashboard” feature (see Figure 1.1). Each time a practitioner searches the CSD before prescribing a controlled substance to a patient, a dashboard of the patient’s recent history of controlled substance prescriptions is displayed. The dashboard allows practitioners to quickly see a patient’s (1) risk of overdose, (2) number of different prescribers used in the last six months, (3) number of different pharmacies used in the last six months, and (4) drug combination risk.

**Figure 1.1  “CSD Patient Dashboard” as Seen by Prescribers**

![CSD Patient Dashboard](https://example.com/csd_dashboard.png)


---

\(^{16}\) Utah Code § 58-37f-301(1).

\(^{17}\) Utah Code § 58-37f-601.
Clicking on each metric allows the prescriber to see additional information and best practice recommendations (see Figure 1.2). These metrics allow the prescriber to make a more informed decision about whether a patient is doctor shopping, abusing medication, at risk for an overdose, etc.

**Figure 1.2 “CSD Patient Dashboard” Metrics**

![Metric Diagrams]


DOPL is currently testing a Prescriber Dashboard that will contain similar metrics to the Patient Dashboard. The Prescriber Dashboard will allow prescribers to view and compare their prescribing behavior with those of their peers. The Prescriber Dashboard is set to be released in 2019.
Audit Objectives, Scope, Methodology, and Limitations

The audit was conducted to assess the quality of security and access controls for the CSD. Our audit scope included a review of the following data and documentation from November 1, 2016 through October 31, 2017:

- Applicable state statutes and administrative rules;
- Applicable DTS, Department of Commerce, and DOPL policies and procedures;
- Audits, risk assessments, and quality assurance reviews conducted by DTS, Deloitte, and DOPL;
- Evidence of configured password policies for applications, databases, servers, and networks relevant to CSD operations;
- User and administrator listings for applications, databases, servers, and networks relevant to CSD operations;
- Logs of CSD and back-end database user activities;
- DTS change tickets documenting and authorizing changes to applications, databases, servers, and networks relevant to CSD operations;
- Logs of changes to the CSD and its associated code repository;
- Documentation of backup schedules and restoration tests for applications, databases, and servers relevant to CSD operations;
- Department of Human Resource Management record of state employee histories; and
- Department of Health’s Office of Vital Records and Statistics death certificate data.

In addition to our review of applicable documentation, we conducted interviews with process owners and stakeholders to understand CSD operations and relevant IT controls. Using the information provided in these interviews combined with our review of relevant evidence, we documented the design of 22 IT controls related to the following areas:

- Logical Access
- Computer Operations
- Change Management
- Data Security

Having documented the design of our 22 selected IT controls, we conducted a series of tests to verify that each control operated according to its intended design. If a control did not operate as intended or we deemed it was not designed effectively, we looked for any substantive findings associated with the failed control. Our test procedures included the following methods:

- Real-time observation of controls in operation;
- Review of screenshots documenting controls in operation;
- Analysis of application user accounts and access logs;
• Random sampling of sensitive activities by application administrators and review of authorizing documentation;
• Random sampling of changes made to application code and review of authorizing documentation; and
• Direct confirmation of management approval for sensitive access at the network, server, database, and application levels.

Data Limitations

For any given query in the CSD, the application records the user’s *current* role rather than the user’s role applicable to the queried time period. Thus, we could not test if a user whose role changed from a generic role to a privileged role performed any searches of the CSD under the generic role.

Additionally, our audit included a review of controls around the database and its supporting infrastructure. Prescription data within the database was not in the scope for this audit and was therefore not reviewed.
Findings

Finding 1: Inadequate CSD password requirements do not comply with DOPL policy

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Logical Access: Application Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>Access to the CSD requires a Utah-ID login plus a 4-digit pin. Other password requirements may be enforced but must be requested by the steward agency and would be application specific. Password requirements for the CSD were intended to follow DTS’s enterprise-wide password policy; however, the CSD had not been configured accordingly. As a result, the CSD did not enforce expiration dates or complexity on passwords for non-State employees.</td>
</tr>
<tr>
<td>Effect</td>
<td>Access to over 99% of CSD user accounts was inadequately enforced, increasing the possibility of unauthorized access.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Comply with DOPL policy by enforcing the DTS enterprise-wide password requirements on all Utah-ID accounts with access to the CSD.</td>
</tr>
</tbody>
</table>
Finding 2: Password requirements for back-end CSD users do not conform to required DTS policy

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Logical Access: Database Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>Password requirements for back-end database access do not comply with the official DTS policy adopted by DOPL. Two of the eight back-end database users had no password complexity requirement enforced. All eight users were permitted more failed login attempts than permitted by DTS policy. None of the eight users were required to change their password within the time frame required by DTS policy, and six of the eight users had no password lifetime enforced. Finally, all eight users were permitted to reuse their password an unlimited number of times while DTS policy states that “a history of a user’s ten most recently used passwords will be maintained to restrict their reuse.”</td>
</tr>
<tr>
<td>Effect</td>
<td>The CSD has increased susceptibility to security breaches.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Comply with DOPL policy by enforcing the DTS enterprise-wide password requirements on all CSD database accounts.</td>
</tr>
</tbody>
</table>
### Finding 3: Several unlicensed individuals received CSD accounts without proper approval

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Logical Access: Authorized Users</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Condition</strong></td>
<td>Licensed practitioners are automatically granted CSD accounts by virtue of having an active license in DOPL’s professional licensing database; however, unlicensed applicants must submit an application to receive access to the CSD. This allows CSD administrators to perform a background check of court records and drug abuse history and ensure the applicant is qualified to access the CSD. Of the 41 unlicensed users sampled who received access to the CSD during the audit period (11/1/16 – 10/31/17), the required approval documentation for five users was never found. Although only one of the five users logged in, each had the ability to do so.</td>
</tr>
<tr>
<td><strong>Effect</strong></td>
<td>Unauthorized individuals had access to the CSD.</td>
</tr>
<tr>
<td><strong>Recommendations</strong></td>
<td>Comply with DOPL policy by ensuring (1) all unlicensed individuals complete an application and are properly verified before receiving access to the CSD, and (2) all required documentation is retained.</td>
</tr>
</tbody>
</table>
Finding 4: CSD user accounts are not periodically reviewed for appropriateness

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Logical Access: Authorized Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td><strong>Application</strong> DOPL does not perform reviews of designee user accounts for appropriateness. Upon login, “Practitioners” (i.e. users with a professional license) are automatically checked against DOPL’s professional licensing database for an active license. Access to the CSD is granted only if an active license exists. However, users authorized as designees of licensed individuals are not reviewed for appropriateness after they receive access. A process exists by which practitioners may request removal of a designee's access, but there is currently no control from DOPL to ensure the removal occurs.  <strong>Database, Server, and Network</strong> DOPL does not conduct regular reviews of system administrators at the database, server, or network levels. As a result of one such review facilitated by the Auditors, DOPL identified one inappropriate account on the database. This account did not appear to have ever logged into the database. The account was removed.</td>
</tr>
<tr>
<td>Effect</td>
<td>Unauthorized users may retain access to the CSD servers, database, and/or application subsequent to an action (e.g. termination, transfer, retirement, etc.) that would render their access unlawful.</td>
</tr>
<tr>
<td>Recommendations</td>
<td>DOPL should carry out periodic access reviews on all CSD-related systems. If practitioners do not confirm their designees with DOPL within a specified timeframe, at a minimum, DOPL should remove those designees' access to the CSD.</td>
</tr>
</tbody>
</table>
**Finding 5: Practitioners with expired licenses were improperly allowed to perform queries in the CSD**

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Logical Access: Authorized Users</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Condition</strong></td>
<td>Many users in the CSD are authorized to access the database by virtue of their professional licenses issued by DOPL. DOPL policy states a user should not be permitted to access the CSD if a user’s license is no longer active. Between October 26, 2016 and November 7, 2017, seven individuals were able to log in with expired licenses. On November 2, 2017, DOPL discovered a bug in the CSD that prevented it from verifying the user’s license. A bug fix was deployed on November 7, 2017. Before DOPL implemented the fix, six practitioners with expired licenses logged into the application. Five of these practitioners performed searches, with one search being performed more than three-and-a-half years after the individual’s license expired. We noted no searches or logins by users with expired licenses between implementation of the fix on November 7, 2017 and May 1, 2018.</td>
</tr>
<tr>
<td><strong>Effect</strong></td>
<td>Unauthorized individuals accessed the CSD.</td>
</tr>
<tr>
<td><strong>Recommendation</strong></td>
<td>Periodically test that users with expired licenses cannot access the CSD.</td>
</tr>
</tbody>
</table>

---

18 Professionally licensed users include practitioners, pharmacists, advanced practice registered nurse (APRN), registered nurse (RN), etc.
# Finding 6: Management has not defined activities that should be monitored

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Logical Access: Identification of Sensitive Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Condition</strong></td>
<td>DOPL has not formally documented sensitive activities in the database. Performing this assessment would enable targeted monitoring of user activity as well as customization of user roles for better adherence to the principle of providing the least privilege required to complete a task.</td>
</tr>
<tr>
<td><strong>Effect</strong></td>
<td>User role permission sets might not be optimized for database security, and inappropriate activity cannot be effectively monitored.</td>
</tr>
<tr>
<td><strong>Recommendations</strong></td>
<td>DOPL should define sensitive activities in the database. These activities include (1) privileged administrative functions, (2) segregation of duties violations, and (3) suspicious database searches.</td>
</tr>
</tbody>
</table>
## Finding 7: Inadequate monitoring of user activity

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Logical Access: Review of Sensitive Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Condition</strong></td>
<td>DOPL does not perform regularly scheduled reviews of user activity for either general users or “SuperAdmins.”</td>
</tr>
</tbody>
</table>

CSD administrators highlight the felony punishment for inappropriate searches of the CSD as the main deterrent to misuse of the database. As a preventive control, management references the requirement to enter the name and birth date of the person they are searching. As a result, review of user activity in the CSD is reactive, performed only if there is suspicion or report of wrongdoing.

Furthermore, “SuperAdmin” users may require access to sensitive and/or incompatible database activities in order to perform their administrative functions. While the access may be necessary, it creates additional risk that should be controlled.

<table>
<thead>
<tr>
<th><strong>Effect</strong></th>
<th>Inappropriate searches by CSD users, or unauthorized activity by “SuperAdmins”, may go undetected.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommendation</strong></td>
<td>DOPL should implement a proactive monitoring control that detects inappropriate user activity.</td>
</tr>
</tbody>
</table>
Finding 8: Insufficient monitoring of testing documentation for application changes prior to deployment

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Change Management: Control of Changes Migrating from Testing to Final Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>DOPL contracts with DTS to administer the CSD application change management process, which is documented and controlled via change tickets and a DTS-run deployment application. After a developer modifies code, the code is tested and approved by the DTS Quality Assurance (QA) team. A project manager on the development team then creates a change ticket, which triggers an email to the developer with a link to the deployment application. The developer opens the deployment application and enters the link to the modified code. An email is sent to the QA team notifying them to approve the code within the deployment application. The QA team indicates that the code was tested (without retesting it), and the hosting team receives an automatic notification that code is ready for deployment. During the approval process, the QA team neither verifies that the code link being sent to Production matches the link earlier approved in Testing, nor that the change number listed on the deployment application matches the approved change ticket. The QA member only verifies that a change number and link to the code are listed on the deployment application. Of the 10 Production deployments sampled during the audit, two did not have a corresponding deployment in the testing environment.</td>
</tr>
<tr>
<td>Effect</td>
<td>Code that has not been reviewed or approved could be implemented in the CSD.</td>
</tr>
<tr>
<td>Recommendations</td>
<td>The QA team should:&lt;br&gt;(1) create the change ticket to initiate a migration to Production once testing is complete for a particular change.&lt;br&gt;(2) verify that a) the code link being sent to Production matches the link that was tested, and b) the change number listed in the deployment application matches the number of the change ticket they created.</td>
</tr>
</tbody>
</table>
Finding 9: Data retention policy exposes DOPL to unnecessary risk

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Data Security: Data Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Condition</strong></td>
<td>DOPL implemented a five-year data retention policy for queries and prescription data accessible via the CSD to practitioners and other general users of the database. On the back-end database, accessible only to database administrators and select Department of Health employees, queries and prescription data dated back to 2002 are held indefinitely. Data is never deleted from the back end of the database unless a duplicate entry or other entry error is reported. According to DOPL, the CSD data retention policy follows the five-year record retention schedule required of pharmacies. However, this retention schedule does not appear to apply to the CSD, and DOPL has not performed an assessment to determine the appropriate retention schedule based on statutory expectations. The only purpose in keeping the information indefinitely would be for data analysis by the Department of Health—analysis which could be performed with anonymized information.</td>
</tr>
<tr>
<td><strong>Effect</strong></td>
<td>Sensitive information in the database is exposed to unnecessary risk.</td>
</tr>
<tr>
<td><strong>Recommendations</strong></td>
<td>DOPL should implement policies to: (1) reduce data retention to the minimum necessary time to accomplish the statutory objectives of the CSD patient information. (2) anonymize data in the back-end database archive, if an archive is in fact deemed necessary.</td>
</tr>
</tbody>
</table>

---

19 According to DOPL Management, the five-year policy is based on Utah Code and associated Administrative Rule, which require that pharmacy “…prescription files, including refill information, shall be maintained for a minimum of five years…” [Utah Code § 58-17b-611; Utah Admin. Code R156-17b-612(4)].

### Appendix A  
**DOPL’s Response to How It Fulfills CSD Requirements and Purposes**

<table>
<thead>
<tr>
<th>Data Requirements for the CSD</th>
<th>DOPL’s fulfillment of requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(a)</strong> The purpose of the database is to:</td>
<td>CSD data must be submitted in the standard established by the American Society of Automation in Pharmacy(^{22}) as provided by statute and rule. Currently, the CSD provides for pharmacists to either submit an annual waiver form(^{23}) if they do not dispense controlled substances, or to submit data to the CSD through batch jobs.(^{24}) By December 31, 2018, an automated system will be in place to verify all pharmacies who have not been authorized a waiver, but who have submitted data on a daily basis to the database. This would be in the form of Rx record(s) or a daily &quot;ZERO&quot; report.</td>
</tr>
<tr>
<td>contain the data described in Section 58-37f-203 regarding every prescription for a controlled substance dispensed in the state to any individual other than an inpatient in a licensed health care facility;</td>
<td></td>
</tr>
<tr>
<td><strong>(b)</strong> contain data reported to the division under Section 26-21-26 regarding poisoning or overdose;</td>
<td>DOPL has developed a report submission process for hospital staff to log into the CSD and report an overdose by way of completing an internal form. CSD staff perform a database check on the reported overdose patient for a one-year period. All prescribers identified as issuing a prescription to the overdose patient within the reported period are sent (by U.S. Mail) a written notification of the patient’s overdose, including a copy of the hospital and database record(s) report.(^{25}) The overdose is also linked to the prescriber’s name in the licensing database to document trends and patient reoccurrences. This data aids in the process of academic detailing and in unprofessional and unlawful conduct investigations. The external report may also be seen by the practitioner when they perform a search of the identified patient.</td>
</tr>
</tbody>
</table>

---

\(^{21}\) Utah Code § 58-37f-201(5)

\(^{22}\) 2011 ASAP Version 4.2 Standard for Prescription Monitoring Program

\(^{23}\) Utah Administrative Code § R156-37f-203(6)

\(^{24}\) Utah Administrative Code § R156-37f-203(4)

\(^{25}\) Utah Code § 58-37f-702(2)
(c) contain data reported to the division under Subsection 41-6a-502(4) or 41-6a-502.5(5)(b) regarding convictions for driving under the influence [DUI] of a prescribed controlled substance or impaired driving; and

DOPL has developed a data submission process for the State Courts to submit data to the CSD for reported DUI or impaired driving criminal conviction(s) via an external report record. CSD staff perform a database check of the reported individual for a one-year period. All prescribers identified as issuing a prescription within the reported period are sent (by U.S. Mail) a written notification of the patient's DUI or impaired driving conviction(s), including a copy of the court report and database report. The patient’s conviction is also linked to the prescriber’s name in the licensing database to document trends and patient reoccurrences. This data aids in the process of academic detailing and in unprofessional and unlawful conduct investigations. The external report may also be seen by the practitioner when they perform a search of the identified patient.

(d) contain data reported to the division under Subsection 58-37-8(1)(e) or 58-37-8(2)(j) regarding certain violations of the Utah Controlled Substances Act.

DOPL has developed a data submission process for the State Courts to submit data to the CSD regarding criminal conviction(s) as an external report. This section was omitted in 58-37f-703, and therefore no notification to providers is provided at this time. DOPL is working to get this added in the next legislative session. The patient’s conviction is also linked to the prescriber’s name in the licensing database to document trends and patient reoccurrences. This data aids in the process of academic detailing and in unprofessional and unlawful conduct investigations. The external report can also be seen by the practitioner when they perform a search of the identified patient.

---

<table>
<thead>
<tr>
<th>Data Identified by the CSD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>27</strong>The division shall maintain the database to facilitate use of the database for identification of:</td>
</tr>
<tr>
<td>(a) prescribing practices and patterns of prescribing and dispensing controlled substances;</td>
</tr>
<tr>
<td><strong>DOPL's fulfillment of purposes</strong></td>
</tr>
<tr>
<td>DOPL works in conjunction with the Utah Department of Health to provide data to produce public health data and educational detailing for practitioners.</td>
</tr>
</tbody>
</table>

---

26 Utah Code § 58-37f-703(1)
27 Utah Code § 58-37f-201(6)
<table>
<thead>
<tr>
<th>(b) practitioners prescribing controlled substances in an unprofessional or unlawful manner;</th>
<th>DOPL investigates complaints of practitioner over-prescribing. Data from the CSD is used for investigations as a means of confirming the pharmacy where prescriptions were dispensed. The CSD also performs data analysis to identify high-prescribers, and evaluate their prescriptive behavior within the standards of the profession and established prescribing guidelines. Practitioners identified as prescribing amounts that are reckless or endangering are investigated by DOPL for administrative action. Practitioners identified as prescribing beyond established standards and guidelines are provided additional training and detailing by DOPL.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(c) individuals receiving prescriptions for controlled substances from licensed practitioners, and who subsequently obtain dispensed controlled substances from a drug outlet in quantities or with a frequency inconsistent with generally recognized standards of dosage for that controlled substance;</td>
<td>The CSD performs data analysis to identify high prescribers and evaluate their prescriptive behavior within the standards and norms of their profession and established prescribing guidelines (see Figure 1.1). Practitioners identified as prescribing amounts that are reckless or endangering are investigated by DOPL for administrative action. Practitioners identified as prescribing beyond established standards and guidelines are provided additional training and detailing by DOPL.</td>
</tr>
<tr>
<td>(d) individuals presenting forged or otherwise false or altered prescriptions for controlled substances to a pharmacy;</td>
<td>When prescription(s) or individual(s) are identified as fraudulent, pharmacies and practitioners are instructed to report the information to their local law enforcement agency for criminal investigation. The CSD provides pharmacy alerts (through email notifications) to all state-licensed pharmacies with information about the alleged fraudulent prescription or individual. DOPL is prohibited from providing any identifiable CSD data to law enforcement.</td>
</tr>
<tr>
<td>(e) individuals admitted to a general acute hospital for poisoning or overdose involving a prescribed controlled substance; and</td>
<td>See above response to (c).</td>
</tr>
<tr>
<td>(f) individuals convicted for: (i) driving under the influence of a prescribed controlled substance that renders the individual incapable of safely operating a vehicle; (ii) driving while impaired, in whole or in part, by a prescribed controlled substance; or (iii) certain violations of the Utah Controlled Substances Act.</td>
<td>See above response to (c).</td>
</tr>
</tbody>
</table>
Appendix B

DOPL’s Response to Findings
Friday, August 10, 2018

Mr. John Dougall, State Auditor
Office of the State Auditor
East Office Building, Suite E310
Utah State Capitol Complex
Salt Lake City, Utah 84114

Subject: Response to “Information Systems Audit of the Controlled Substance Database.”
(Report No. IT 18-01)

Dear Auditor Dougall:

Thank you for the opportunity to review and respond to “Information Systems Audit of the Controlled Substance Database.” Some of the recommendations were already being addressed by DOPL staff prior to the audit, while others were not. DOPL has implemented or will implement each recommendation made in the audit.

Sincerely,

Mark Steinagel
Director