ARIZONA DEPARTMENT
OF HEALTH SERVICES

September 23, 2019

Ms. Lindsey Perry, Auditor General
Arizona office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

RE: Statutory Sunset Factors Audit

Thank you for the opportunity to respond to your audit on our statutory sunset factors. We appreciate the role that the Auditor General plays in supporting the legislative Sunset Review process in providing information used to evaluate whether departments are meeting their statutory obligations and continue to be needed in state government.

The Arizona Department of Health Service (ADHS or the Department) serves a critical role in promoting, protecting and improving the health and wellness of all Arizonans as we provide public health services throughout their entire lifecycle. The Department, through approximately 300 programs it administers, serves all 7.1 million Arizonans. Many people may not recognize the impact that public health has on every facet of our daily lives. There are many ways we help improve the lives of all Arizonans, including:

- Protecting the health and lives of all Arizonans by controlling epidemics
- Educating people on healthy habits, such as nutritious eating and getting physical activity
- Assisting people with tobacco cessation and disease self-management
- Ensuring safe food and water
- Testing virtually all newborns for metabolic diseases and serving as the State's only reference laboratory
- Improving access to physical and behavioral health
- Monitoring hospitals, nursing homes, assisted living centers, ambulances, childcare centers and other licensed facilities and professionals
- Documenting every vital event in Arizona including all births, deaths and adoptions

We also operate the Arizona State Hospital (ASH), which provides high acuity, inpatient psychiatric services to our state's most vulnerable residents.

ADHS is proud to be a part of Arizona's strong public health system, providing safe parks, clean air, clean water, safe meals and a healthy environment to raise our families. The work we do adds value to our state and brings health and wellness to all Arizonans. ADHS has been recognized nationally as a leader in public health initiatives and is accredited by the National Public Health Accreditation Board (PHAB).

More information about the Department's objectives and anticipated accomplishments are detailed in the ADHS Fiscal Year 2020 Strategic Plan and the Department's FY18 Annual Report, which is posted online.

We appreciate your report highlighting the important work we do as part of our mission of supporting *Health and Wellness for all Arizonans* and that the Department has met its statutory objective and purpose, and is improving the efficiency with which it has operated. As we have noted in prior communications, we are committed to continuous improvement and will undertake activities that will enhance our processes. However, we are concerned that how your findings are conveyed does not provide adequate context for readers and legislators and could result in misinterpretation of the findings and our overall performance. Because the purpose of the Sunset Review process is to provide overall perspective on the Department's performance to allow legislators to "review the purpose and functions of state agencies to determine whether continuation, revision, consolidation or termination is warranted,"[1] overall context is particularly important in audits that support Sunset Reviews. Therefore, while we will employ strategies that will address the findings, you will see in our response that there are certain findings with which we cannot agree.

For example, in Finding 1, the report makes sweeping statements about public health and safety risks in the context of the auditors' review of 33 complaints and a judgmental sample of 37 self-reports for 5 long-term care facilities that are regulated and funded through an agreement with the federal Centers for Medicare and Medicaid Services (CMS). However, the audit fails to provide context for this analysis and findings. In total, long-term care facilities represent less than 0.5 percent of the total licensees under Department regulation and the sample of 5 facilities represents 0.014% of total licensees under the Department's jurisdiction. The complaints reviewed represent roughly 0.4% of all complaints received by the Department during the two-year period under evaluation. Rather than articulating how the Department performs across this wide range of activities to protect public health and safety and investigating and resolving complaints within its jurisdiction, the audit findings focus on this very narrow non-representative sample. In addition to only

[1] *Handbook on Arizona's Sunset & Sunrise Review*, Fifty-Fourth Legislature, 2019-2020.

representing a small subset of the Department's overall regulatory activity, this sample is even small within the overall long-term care facility regulation framework, which received a total of 4,959 complaints over the two-year period in question.

We would also note that under this federal program overseeing long-term care facilities, the Department performs functions for CMS, who sets the expectations, requirements and funding for the program. The Department is currently in compliance with those requirements as determined CMS. The audit establishes expectations for the Department beyond those that exist in its agreement with CMS or as currently established by the Legislature, including establishing investigation time frames by examining policies in other states without a comprehensive analysis of those other states' requirements and available resources. If the State wants to expand the regulation of this industry beyond the federal requirements, including an evaluation of Arizona's long-term care marketplace and resources needed to meet any additional expectations that are set, the Department would be pleased to participate in those discussions. In summary, we will not detail every individual concern with how the audit articulates its findings. But as a result of these concerns, we cannot agree with Finding 1.

The Department also cannot agree with Finding 3. We take seriously our obligation to protect critical, sensitive and confidential data. ADOA-ASET is the Arizona office responsible for setting the technology, security, privacy, and communication strategies, policies, and procedures for the state of Arizona. ASET's guiding principles include *Driving best-in-class, enterprise-wide security standards through the office of the state Chief Information Security Officer (CISO) in an effort to ensure that all cyber security initiatives are secure and compliant.* To this end, ASET provides leadership, standards and governance across all of state government, leveraging its experts to set expectations and monitor enterprise security controls and state agency activities. The report misrepresents our IT security processes, including using inaccurate terminology to describe activities in the report (e.g., use of the term "breach", which did not occur, but was implied to have occurred in the report). The incident referenced in the audit involved a multistep, complicated process in which an individual would have needed specific knowledge to access the information. Contrary to what is reported in the audit, ADHS's web application development policies and procedures are aligned with ASET and credible industry standards.

In addition, the audit reports that the Department has not conducted a formal Department-wide IT risk assessment since 2015. This misleading statement fails to explain that ASET conducted a state-wide risk assessment several years ago and determined that Arizona

could greatly reduce IT risks by implementing enterprise controls. The Department and other states agencies have focused on implementing these controls over the past few years, including the establishment of RiskSense, a tool used for IT vulnerability management and risk scoring. The RiskSense platform includes the assignment of a safety score which is used to evaluate and monitor each agency's risk exposure. Governor Ducey and ASET set a goal for each state agency to maintain a score of 725 or above; the Department currently exceeds this goal. In addition, the score is updated at least twice a month and Department leadership reviews its performance weekly and allocates resources as needed to address identified issues. Now that these controls have been implemented, the Department plans to return to performing annual risk assessment. The Department believes ASET provides sufficient and appropriate leadership on IT security issues and will continue to work collaboratively with ASET to maintain its agency's information security. It will also implement recommendations that will continue to enhance its procedures.

As discussed above, the wording and issue framing of the audit causes us concern in several instances; we have noted others in our detailed response. Again, we appreciate your recommendations and will implement them, where there is agreement, but we do not believe the audit findings provide a full picture of our overall performance.

We appreciate your partnership and look forward to continuing to advance *Health and Wellness for all Arizonans.*

Sincerely,

Cara M. Christ, MD
Director

Attachment

Finding 1: Department's failure to investigate, or timely investigate or resolve, some long-term care facility complaints and self-reports may put residents at risk

Recommendation 1: To help ensure all long-term care facility complaints and self-reports are prioritized, investigated, and resolved in a timely manner, the Department should:

Recommendation 1a: Continue with its efforts to allocate new or reallocate existing staff to prioritize, investigate, and resolve long-term care facility complaints and self-reports on a full-time basis.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The Department is currently assigning two additional staff to handle complaints. The ADHS will focus these staff to respond to high priority complaints. However, retention and training remain an issue to keep highly qualified staff at the Department. The Department recognizes however, that it would require significantly more staff to timely investigate all long-term care complaints. Based on estimates and similar work, The Department believes an additional 44 staff and an additional $3.3M of appropriation and GF allocation will be needed to timely adjudicate the nearly 2,500 complaints received annually. Additionally, the Department leadership is utilizing the Arizona Management System and has assigned this project as a breakthrough for the agency to increase the number of high priority complaints investigated on time.

Recommendation 1b: Develop and implement a time frame for completing investigations and closing long-term care facility complaints and self-reports.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The Department is currently revising its policies and procedures to account for this recommendation. The Department anticipates completion of this effort by April 2020.

Recommendation 1c: Regularly update its policies and procedures to reflect changes in its current long-term care facility complaint and self-report investigation and resolution practices and CMS requirements.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The Department is currently revising its policies and procedures to account for this recommendation. The Department anticipates completion of this effort by April 2020.

Recommendation 1d: Develop and implement additional bi-monthly management reports to monitor whether and how quickly its long-term care facility complaints and self-reports are being prioritized, investigated, and resolved.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The Department has developed the necessary management reports and is currently refining and implementing the new monitoring tools.

Recommendation 1e: Ensure that any complaints and self-reports that are investigated during an annual survey or outside of the annual survey are initiated and investigated according to the time frames required by the assigned priority level.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The Department is currently assigning two additional staff to handle complaints. The Department will focus these staff to respond to high priority complaints. The Department recognizes however, that it would require significantly more staff to timely investigate all long-term care complaints. Based on estimates, the Department believes an additional 44 staff will be needed and an additional $3.3M of appropriation and GF allocation to timely adjudicate the nearly 2,500 complaints received annually.

Recommendation 2: The Legislature should consider forming a task force to study and propose policy options for addressing the Department's timely investigation and processing of long-term care facility complaints and self-reports to help ensure resident health and safety. Options to consider include establishing requirements for investigating all complaints and self-reports, appropriate time frames for conducting investigations of and closing out long-term care facility complaints and self-reports, and reporting performance metrics to the Legislature. Task force members should include appropriate stakeholders, such as legislators, Department representatives, Arizona Department of Economic Security representatives, industry members (i.e., long-term care facility owners or licensed administrators), patient advocates, and if appropriate, a federal CMS representative. Legislation forming the task force should identify task force membership, its overall purpose and expected outcomes, and deadlines for reporting recommendations to the Legislature.

Department Response: The finding of the Auditor General is Choose an item.

Response explanation:

Finding 2: Department did not comply with some conflict-of-interest requirements

Recommendation 3: The Department should continue its efforts to develop and implement a new conflict-of-interest disclosure process and form that will help it comply with the State's conflict-of-interest requirements and best practices, such as having public officials and employees annually disclose whether or not they have any substantial financial and/or decision-making conflicts, and train employees on how the State's conflict-of-interest requirements relate to their unique program, function, or responsibilities.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will complete development, and implement the conflict of interest disclosure process, by April 1, 2020.

Finding 3: Some gaps in Department IT security processes resulted in a security incident and additional IT security weaknesses

Recommendation 4: The Department should develop and implement web application development policies and procedures that incorporate security into the development and modification process, including requirements for gathering security requirements, using up-to-date secure coding standards, performing threat modeling during development, reviewing source code, and performing security testing before releasing a web application to the live environment.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: ADHS' web application development practices align with ASET's policies and credible industry standards; however, our procedures could be enhanced. ADHS will review and update its web application development procedures to ensure that security is fully incorporated and implement any additional areas mentioned that aren't currently being performed (such as threat modeling).

Recommendation 5: The Department should require staff who are responsible for developing web applications to regularly receive role-based training on how to develop and maintain secure web applications.

Department Response: The finding of the Auditor General is not agreed to and the recommendation will not be implemented.

Response explanation: Staff responsible for developing web applications receive ASET Secure Coding training. Developers that are not FTE's are required to have this knowledge and interviews include this type of questioning.

Recommendation 6: The Department should develop and implement revised data classification policies and procedures that provide guidance on how to classify its data; require developing a data classification inventory that is updated regularly; specify requirements for protecting data based on its level of risk; and establish processes for handling confidential data, such as ensuring that only approved devices process confidential data.

Department Response: The finding of the Auditor General is not agreed to and the recommendation will not be implemented.

Response explanation: ADHS has a Data Classification policy that is consistent with State of Arizona policy. Data is classified at the system level. ASET is in the process of working with an agency to pilot a third party tool that will categorize and classify data so we will review the results of this pilot to see if this is something feasible to implement in the future. We are working on implementing the State Data Governance Organization policy to formalize data roles and provide associated training for data owners, data stewards, and data custodians.

Recommendation 7: The Department should conduct a formal Department-wide risk assessment at least annually, as required in its risk assessment policy and procedures, to evaluate, document, and prioritize the areas in the Department's IT environment with the highest security risks.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The last risk assessment the Department had performed was when Behavioral Health Services (BHS) was part of the Department and BHS funded a third party to perform this. Several years ago the state did a risk assessment and determined that the State could greatly reduce IT risks by implementing enterprise controls. The Department has focused on these implementations the last couple of years. One of the controls that was implemented was RiskSense for vulnerability management and risk scoring on a state-wide basis.

Recommendation 8: The Department should develop and implement a revision to its risk assessment policy and procedures to include categorizing the Department's information based on the likelihood of risk and magnitude of harm as required by ASET policy.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The Department Information Security Program policy is consistent with the State policy. The Department will work to enhance our procedures and standards regarding the categorization of information.

Recommendation 9: The Department should develop and implement revised security awareness training policies and procedures that include a process for ensuring employees and contractors comply with annual basic security awareness and HIPAA training requirements and acceptable use attestations; specify the role-based training that is required based on employees' and contractors' responsibilities; explain how it will implement its security awareness program; describe the topic areas that its security awareness training classes should cover; and specify how it will communicate security awareness training throughout the year

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The Department has a mature security awareness and HIPAA training program which require initial and ongoing (annual) Security Awareness and HIPAA training per policy. However, the Department hasn't always obtained 100% compliance. The Department will work to improve its compliance on these trainings. We utilize the State Security Awareness computer based training which contains the required content. Security Awareness training and acceptable use attestations were recently completed in June of 2019. HIPAA training for 2019 has been taken historically in the month of December each year, and is scheduled for December of 2019.

Recommendation 10: The Department should continue with its plans to develop and implement role-based training.

Department Response: The finding of the Auditor General is not agreed to, but the recommendation will be implemented.

Response explanation: The Department intends to develop and implement a more formal role-based training program. The state of Arizona has conducted role-based training for IT leaders, Information Security personnel, System Administrators, and Developers over the years and the Department has participated in these trainings. These types of training are not logged into the State's current Learning Management System because that system lacks the capabilities of logging third party training.

Sunset Factor 2: The extent to which the Department has met its statutory objective and purpose and the efficiency with which it has operated.

Recommendation 11: The Department should continue using the electronic grants management system, and ensure that for all future grant evaluations conducted using this system, its grant evaluations clearly indicate whether grant applicants complied with all evaluation criteria and that all evaluation factors are included in the grant solicitation.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will implement the recommendation by April1, 2020.

Sunset Factor 5: The extent to which the Department has encouraged input from the public before adopting its rules and the extent to which it has informed the public as to its actions and their expected impact on the public.

Recommendation 12: The Department should develop and implement policies, procedures, and training to help guide the boards, commissions, and councils it supports; and its staff members' compliance with open meeting law requirements.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department has begun to implement this recommendation (training is now being done through the State Ombudsman's Office as suggested on the Attorney General's web site) and will have the recommendation fully implemented by April1, 2020.

Recommendation 13: The Department should develop and implement an oversight process to ensure that the boards, commissions, and councils it supports comply with open meeting law requirements.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will implement this recommendation by April1, 2020.

Recommendation 14: The Department should update its website to include a conspicuously posted statement indicating the location for all electronic and physical postings of public meeting notices and a complete and accurate listing of all the entities that are subject to open meeting law along with information about their purposes and where to locate information about these entities' public meetings, such as agendas and minutes.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department has begun to implement this recommendation (statement now posted on ADHS' Administrative Rules' web site) and will have the recommendation fully implemented by April1, 2020.