

Arizona Department of Health Services

CONCLUSION: The Arizona Department of Health Services (Department) provides and coordinates public health services and programs for the State. Some of the Department’s key responsibilities include regulating some health-related occupations, such as emergency medical care technicians; regulating childcare and healthcare facilities; responding to public health emergencies; and helping control public health epidemics. The Department failed to investigate, or timely investigate or resolve, some long-term care facility complaints and self-reports. In addition, it did not comply with some conflict-of-interest requirements. The Department is also responsible for safeguarding its information technology (IT) systems and data, and some gaps in its IT security processes resulted in an incident and additional IT security weaknesses. Finally, the Department is responsible for more than 30 boards, commissions, committees, councils, subcommittees, teams, and user or work groups that are subject to open meeting law requirements, and the Department did not consistently comply with open meeting law requirements for 3 meetings we reviewed.

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

As the State licensing agency and the State Survey Agency for the federal Centers for Medicare and Medicaid Services (CMS), the Department is required to investigate all complaints and long-term care facility self-reported incidents (self-reports) for the 147 State licensed/CMS certified long-term care facilities in the State. We reviewed 33 complaints and a judgmental sample of 37 self-reports the Department received in calendar years 2017 and 2018 for 5 judgmentally selected long-term care facilities and found that the Department did not investigate or did not timely prioritize, investigate, or resolve some long-term care facility complaints and self-reports. Specifically, we found that as of June 2019, 38 of the 70 complaints and self-reports were still open and uninvestigated. These uninvestigated complaints and self-reports included allegations of abuse and neglect of residents and unsanitary living conditions.



The Department did not meet the 10-working-day time frame for initiating its investigation for **11 of 12 priority B complaints and self-reports**.

Additionally, for the 20 complaints and self-reports that the Department did investigate, we found that the Department did not timely initiate its investigation for 15 of them. For example, 12 of the 20 complaints/self-reports were assigned a priority B (alleges actual harm but does not rise to the level of an immediate and serious threat), and the Department did not timely initiate investigations for 11 of these 12 complaints/self-reports.

Recommendations

- The Department should ensure all long-term care facility complaints and self-reports are prioritized, investigated, and resolved in a timely manner.
- 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.

Department did not comply with some conflict-of-interest requirements

Arizona law requires employees of public agencies and public officers to avoid conflicts of interest that might influence or affect their official conduct and outlines several requirements for doing so. We identified several areas where the Department was not meeting statutory requirements or best practices. For example, although required by statute,

the Department lacked a special disclosure file that memorializes all disclosures and did not require members of the more than 30 Department-supported boards, commissions, and committees to complete disclosure forms. Also, the Department was not requiring employees to annually disclose conflicts, a best practice. These deficiencies increased the risk of Department employees and public officers not disclosing conflicts. However, the Department began addressing these deficiencies in July 2019.

Recommendation

The Department should continue its efforts to develop and implement a new conflict-of-interest disclosure process.

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

To administer its programs, the Department uses many IT systems to store and process large volumes of sensitive and/or confidential data. Various federal and State laws and regulations and the Arizona Department of Administration's Strategic Enterprise Technology Office (ASET) policies specify the Department's responsibility for protecting this data. However, we identified an instance where confidential Department data was not properly protected by the Department and was therefore inappropriately available to the public. Specifically, a security weakness on a Department website allowed a member of the public to view confidential data such as birthdates, identification numbers, and other information as well as copy an authorized user's credentials and use them to log into a Department web application. As of August 2019, the Department reported that it had investigated and reported this incident to ASET, as required.

We also identified the following gaps in the Department's data classification, risk assessment, and IT security awareness training processes:

- Data classification helps to ensure sensitive data is protected from loss, misuse, or inappropriate disclosure. Although the Department reported that it treats all its data as confidential, it has not inventoried its data and documented the classification of that data.
- The Department has not conducted a formal Department-wide IT risk assessment since 2015. A risk assessment is a structured process recommended by credible industry standards and required by ASET policy that at least annually identifies IT risks within an organization—such as weak security practices, outdated systems, or the lack of a plan for restoring IT systems following a disaster.
- The Department requires all employees and contractors to complete basic security awareness training when initially hired and annually thereafter, but is not enforcing this requirement. Specifically, only 20 percent of the Department's 1,128 employees completed both trainings in 2018.

Recommendations

The Department should:

- Develop and implement web application development policies and procedures that incorporate security into the development and modification process.
- Develop and implement revisions to its data classification, risk assessment, and security awareness training policies and procedures to align with ASET requirements and credible industry standards.

Other Department actions needed

As reported in the Sunset Factors, we identified additional areas where the Department should improve:

Open meeting law—The Department is responsible for more than 30 boards, commissions, committees, councils, subcommittees, teams, and user or work groups that are subject to open meeting law requirements. We reviewed 3 meetings for a Department-supported committee and council and found that the Department did not consistently comply with open meeting law requirements.

Recommendation

The Department should develop and implement policies, procedures, training, and an oversight process to help ensure that the boards, commissions, and councils it supports comply with open meeting law requirements.