STATE OF UTAH
OFFICE OF THE UTAH STATE AUDITOR

TINA M. CANNON
UTAH STATE AUDITOR

Department of Health and Human Services

Management Letter

For the year ended June 30, 2025

Report No. PA-25-01

Office of the Utah State Auditor

Audit Leadership:
Tina M. Cannon, State Auditor
Nora Kurzova, State Privacy Auditor
Mark Meyer, Assistant State Privacy Auditor

UTAH STATE CAPITOL, SUITE 260, SALT LAKE CITY, UT 84114, (801) 538-1025

Table of Contents

State of Utah
Office of the Utah State Auditor

Tina M. Cannon
Utah State Auditor

Management Letter No. PA-25-01

February 2, 2026

Tracy Gruber, Executive Director
Department of Health and Human Services
195 North 1950 West
Salt Lake City, UT 84116

Dear Director Gruber,

The Office of the Utah State Auditor (OSA) operates a hotline program to receive complaints regarding compliance issues or deficiencies involving state or local government agencies, as well as other entities that receive public funds. OSA received a complaint alleging that the Department of Health and Human Services (DHHS), failed to implement adequate incident response procedures and maintains insufficient monitoring mechanisms to efficiently detect and manage such events. According to the complaint, these deficiencies have resulted in under-reporting of incidents and unmitigated exposure to sensitive data, especially data related to children.

Methodology

To assess the credibility of these allegations, we performed the following procedures:

1. Reviewed applicable laws, regulations, and guidance relevant to incident response and data protection responsibilities;
2. Conducted a privacy risk assessment of the most significant DHHS data processing activities as they relate to children;
3. Evaluated DHHS's incident response documentation and internal controls related to cybersecurity and privacy monitoring; and
4. Interviewed selected DHHS employees with focus on the Information Privacy & Security team (IPS), to understand its operational practices and responses to prior data incidents.

Findings Overview

As outlined in our findings, DHHS lacks clearly established incident response roles and pathways, adequate oversight of incident records, adequate employee training, and effective monitoring to detect and manage privacy and security incidents. These weaknesses in oversight, awareness and internal controls allow privacy violations to go undetected or unaddressed for extended periods. We also identify systemic issues in access controls, records dissemination and monitoring across systems and teams handling sensitive records, including mental health and child welfare, as related to two large record repositories: SAFE, used by Division of Child and Family Services (DCFS), and eChart, used by Utah State Hospital (USH).

Our procedures were limited to issues relevant to the specific complaint. Accordingly, we did not conduct a full privacy audit of DHHS' privacy practices or broader cybersecurity framework.

Due to time and scope limitations, and to uphold privacy of the impacted individuals, we did not review actual incident reports. Instead, we interviewed 21 employees, who described the process and provided examples and selected incident related metrics. We also did not review system access logs for the DCFS repository (SAFE) or production data from SAFE or eChart. Had we expanded the scope of our review or performed additional procedures, other concerns may have come to our attention that would have warranted reporting.

Why These Findings Matter

SAFE and eChart systems contain highly personal information about individuals and families in sensitive situations. Mishandling or improper access to this data can result in reputational harm, privacy violations, and long-term consequences such as identity theft, emotional harm, or decisions made based on unethical or illegal motives. Without effective monitoring and safeguards, staff are vulnerable to external pressures, and a single point of failure can compromise entire systems, potentially exposing millions of records to unauthorized access.

We appreciate the courtesy and assistance DHHS personnel extended to us during the course this engagement, and we look forward to a continuing professional relationship.

Sincerely,

Tina M. Cannon

Tina M. Cannon
State Auditor

Findings & Recommendations

Each of the findings below are assigned a risk rating using the following levels: Low, Medium, High and Critical, depending on severity of harm and potential for long term impact.

Background:

SAFE is the Comprehensive Child Welfare Information System (CCWIS) for the State of Utah, Division of Child and Family Services (DCFS). SAFE supports all aspects of child welfare case management, including intake, case notes, case management of in-home and foster care cases, adoption cases, as well as child abuse and neglect cases. SAFE currently contains six million records related to 2,020,726 distinct individuals.

EChart, maintained by the Utah State Hospital (USH), serves as its central repository of records related to patients with mental health needs. Echart currently contains records related to 10,587 individuals.

Finding 1. Inadequate Access Controls in SAFE and eChart Systems

Risk Rating: Critical

Both SAFE and eChart permit access to sensitive records without enforcing or adequately monitoring role-based and least privilege access.

Per statements of the system owner, SAFE allows 1,222 users broad viewing access to the records within the database. Some of the groups that were granted access other than the DHHS social workers include: Utah Office of Guardian ad Litem, several individuals from the Utah Psychotropic Oversight Panel (UPOP), and the office of Attorney General. Viewing access to records is not restricted based on specifically assigned cases or tasks, and the system does not require justification to be entered before viewing documents outside of a user's workload. Users are expected to determine for themselves what range of viewing access is appropriate and adhere to a confidentiality agreement requiring they only look at records relevant to their work. While their access is logged, it is not actively monitored.

Furthermore, DHHS does not maintain an updated data flow schema indicating which groups have access to or receive data from SAFE. DHHS has taken over 10 weeks to produce a basic (and flawed) overview of the data flows, despite several follow ups and enquiries from the auditors.

Records are scheduled to remain in the system for 100 years, accumulating long-term exposure risk. Retention periods for typical records related to child welfare case management span from 7–10 years,[1] with only very specific vital records (such as adoption records) needing to be archived permanently.

In eChart, 823 DHHS employees have system access to patients' charts. As with SAFE, users of eChart are expected to determine for themselves what range of viewing access is appropriate. Discharged patients' records are soft locked[2] after 60 days; however, users may still access them immediately by submitting a comment, which is logged. Records for 340 active in-house patients remain fully accessible to all with an access privilege, without any requirement for justification. Although the division Privacy Officer reviews access logs monthly through a manual sampling process, there is no automated analysis or real-time monitoring to detect outliers or unauthorized access. By policy,[3] and based on a confidentiality agreement, employees are expected to access only the records relevant to their workload.

While both systems have existing back-end role assignments for users, they allow users to view records beyond their immediate responsibilities without proper oversight or access restrictions. Viewing access decisions rely on user discretion, and there are no automated or proactive mechanisms to flag or prevent inappropriate access. Although access is reviewed for inactivity, SAFE accounts access privileges are only revoked after six months without login (while e-Chart accounts access privileges are revoked after one month without login). Retaining access privileges for inactive users for 6 months reflects overly permissive access rights, especially to a system including sensitive records as SAFE does.

DHHS is aware of intentional breaches of policy and confidentiality agreements occurring, along with known instances where workers access or disclose records to the wrong persons by mistake. The division's Privacy Officers have recorded multiple cases where staff viewed records unnecessarily. The USH Privacy Officer has also documented instances of staff capturing unauthorized photos of patients or facilities, as well as external reports of sensitive data posted online.

In addition, no well-known or secure mechanism for anonymous reporting of inappropriate access is in place for either system, leading to staff or other stakeholders having limited options to report wrongdoing without fear of retaliation from agency leadership or coworkers.

The following are the specific risks identified in our test work:

- Single point of failure: Compromising one account or access point (through means like social engineering, bribery, or abuse of technical tools) can expose entire data repositories, enabling malicious actors to move easily between records without being flagged for looking at inappropriate records.

[1] Prosecuted non-felony criminal case files, Civil case files, Child Protective Services Investigation case files
[2] A record is locked but a procedure that unlocks it is known, immediate, and barrier-less.
[3] (02-03 Code of Ethics and Conduct (III)(C)(1)(a),(b),(c), and (e))

- Uncontrolled disclosure: Protected records can be accessed without authorization, putting the privacy of minors, patients, and other vulnerable groups at risk.
- Under-detection of incidents and breaches: Inadequate monitoring distorts perceptions of compliance; fear of impact on employment decreases willingness to self-report.
- Over-retention: Sensitive data kept indefinitely increases the risk of misuse over time.
- Risk of exposure of children's data: Broad, unchecked access heightens the threat of identity theft, which is especially concerning for children's data, as such stolen information can go undetected for years and is highly valuable on the dark web.

This approach does not align with best practice requirements under recognized industry frameworks, regulations and rules,[4] which promote or require that all access, including viewing, be limited to users with a defined business need and protected by adequate safeguards. While distinguishing between viewing and modifying privileges is a cornerstone of access management, viewing should still be restricted to records directly pertinent to a user's specific role and assigned work. Best practices call for implementing adequate technical safeguards in addition to purely administrative measures, such as policy or agreement that prohibits access without a legitimate need to know. "Need to know" is a general security principle that says people get access to information only when it is actually required to perform a specific role or task, and only to the minimum scope and duration needed.

Given the volume of sensitive information involved and the number of users with broad access, the risk of unauthorized disclosure is pervasive. The potential impact includes compromise of protected data, regulatory violations, and erosion of public trust. The likelihood of deviation from policy within such large group is very likely and the severity of impact is high.

Risk rating level and rationale: Critical.

Given the type of information in eChart and the volume of records in the SAFE system, the risk rating is elevated to Critical.

Recommendations:

We recommend that DHHS implement more stringent access controls and adequate monitoring metrics by:

1. *Access Privileges Review*

[4] NIST SP 800-53 Rev. 5 (AC-2, AC-3, AC-5, AC-6), HIPAA Privacy Rule 45 CFR § 164.514(d), HIPAA Security Rule 45 CFR § 164.308(a)(4), ISO 27001:2022 Control 5.15 (A.5.15), or Utah Code § 63A-19-401(2)(ii)

Evaluating access controls for alignment with the principles of least privilege and need-to-know. Removing group access for those without a true need to know. Effective practices commonly include requiring documented and verifiable justification for access to sensitive or non-assigned records, with supervisory oversight and periodic review. Time-limited, just-in-time, and emergency access models, with post-access validation, may also reduce risk exposure.

Shortening period after which access is removed if not used to a maximum of 30 days across systems storing sensitive data.

Developing and maintaining an updated schema of data flows and access privileges.

2. *Record Retention and Dissemination Review*

   Bolstering existing technical safeguards to minimize the occurrence of staff sending records to the wrong recipient by mistake or exfiltrating records with ease. This could be done through flags raised when sending out sensitive data, asking the sender to double check the recipient, adding passwords to the most sensitive attachments, or re-evaluating avenues and methods used to disseminate data with the goal of minimizing the chances of sensitive data being disclosed inappropriately.

   Reviewing record retention timelines to minimize needless accumulation of privacy risk.

3. *Monitoring*

   Implementing regular monitoring mechanisms that detect anomalous or unauthorized access behaviors to strengthen accountability. This typically involves analyzing and establishing baseline usage patterns, identifying deviations, and ensuring appropriate escalation of potential concerns in real time.

4. *Auditing*

   Performing regular supervisory reviews of access records and justifications can be enhanced through a combination of automated analysis and regular manual audits. This increases visibility into access activity and potential misuse and anomaly detection and escalates suspected cases for further investigation and appropriate action.

DHHS's Response:

Recommendation 1-1. We recommend that DHHS implement more stringent access controls and adequate monitoring metrics by Access Privileges Review.

Department Response: The Utah Department of Health and Human Services (DHHS or department) partially concurs with this recommendation. While it can't be implemented exactly as proposed, the department is committed to achieving the same outcome. An alternative path has been identified that better aligns with the current system architecture, which will enable more rapid progress on this front.

What: DHHS will evaluate its access controls in SAFE and eChart to determine whether they are aligned with least privilege and need-to-know principles based on its business and mission. To the extent that users' access in SAFE and eChart provide for the opportunity to exceed the least privilege and need-to-know principles, DHHS will review, and where appropriate, adopt additional administrative and technical controls to enforce least privilege and need-to-know principles. DHHS will verify that through the deprovisioning of the single sign-on (SSO) of UtahID that former employees or potential bad actors with access to these users' credentials cannot access these systems regardless of whether the accounts remain in the system. DHHS will further consider the business need to retain accounts for current employees beyond a window of inactivity. To the extent that accounts are not needed beyond a window of inactivity, DHHS will adopt means to remove accounts.

How: DHHS will evaluate roles within SAFE and eChart and define, where not documented, the access and privileges needed for each of these roles based on its business and mission. Afterwards, DHHS will consider access controls from the NIST SP 800-53, the effectiveness of these controls balanced with expense (see e.g. HHS Cybersecurity Performance Goals, CISA Cybersecurity Performance Goals, MITRE, etc.), and then select, as appropriate, access controls consistent with guidance from NIST SP 800-37. DHHS will investigate whether user access to systems are deprovisioned promptly after a window of inactivity. To the extent deficiencies are identified, DHHS will adopt procedures to appropriately deprovision user access and these accounts as soon as reasonably possible after a window of inactivity.

When: In SAFE and eChart, DHHS will conduct reviews of access and privileges, evaluate controls, and, as appropriate, select controls. To the extent additional controls are selected from the NIST SP 800-53, DHHS with its service providers will create plans of action and milestones (POA&Ms) consistent with guidance from NIST SP 800-37 to create and implement these controls by March 31, 2026. DHHS will create and implement the selected controls within the timelines specified in the POA&Ms.

Responsible Staff: Patrick Thomas, Director of Information Privacy and Security; Tonya Myrup, Director of the Division of Child and Family Services; and Dallas Earnshaw, Superintendent of the Utah State Hospital.

Current Status: Both Division of Child and Family Services (DCFS) and the Utah State Hospital (USH) have reviewed jobs types in SAFE and eChart, respectively, to ensure that these job types have appropriate access privileges in these systems based on the minimum necessary rule. DCFS has updated its process to review accounts after 90 days of inactivity for deprovisioning. USH has reviewed its process to review accounts after 30 days of inactivity for deprovisioning and has decided that this is an appropriate timeline given its business needs. DHHS has a draft of its access control (AC) policy that will replace its current AC related policies that better align with the AC controls in NIST SP 800-53 rev. 5. This AC policy is ready to be reviewed by the DHHS Policy Committee and will be finalized by March 31, 2026.

Recommendation 1-2. We recommend that DHHS implement more stringent access controls and adequate monitoring metrics by Record Retention and Dissemination Review.

Department Response: The department concurs with this recommendation.

What: The department will implement strategies to reduce and mitigate occurrences of staff accidently sending information to the incorrect recipient(s) and will evaluate Child and Family Service retention schedules.

How: The Office of Information Privacy and Security (IPS) will evaluate and implement strategies to reduce occurrences of staff accidently sending information to the wrong recipient(s) via email. IPS and the Division of Child and Family Services' (DCFS) will also coordinate a review of DCFS' retention schedules and amend them, if appropriate, to make sure data is kept only for the amount of time needed.

When: By June 30, 2026

Responsible Staff: Patrick Thomas, Director of Information Privacy and Security; Tonya Myrup, Director, Division of Child and Family Services, and Dallas Earnshaw, Director of Utah State Hospital

Current Status: IPS is evaluating ways in which it can reduce occurrences of staff accidently sending information to the wrong recipients. As part of this strategy, it has identified additional training and better implementation of Virtru as strategies. To implement the training strategy, IPS has assigned a security officer to be primarily responsible for building out its training program consistent with the SANS Institute's Security Awareness Maturity Model. Also, during the DHHS All Staff Monthly Meeting on October 8, 2025, DHHS's Office of Information Privacy and Security (IPS) provided privacy training. This training included guidance from HHS on best practices to avoid sending information to incorrect recipients and how to better use secure messaging tools like Virtru. DCFS has worked with IPS to review its retention schedules as part of its record series. These tasks are on track to be completed by the June 30, 2026 deadline.

Recommendation 1-3. We recommend that DHHS implement more stringent access controls and adequate monitoring metrics by Monitoring.

Department Response: The department concurs with this recommendation. DHHS inherits controls for monitoring anomalous or unauthorized access from DTS through active monitoring tools. The department will consider flagging anomalous and unauthorized access through these active monitoring tools.

What: Typically, real-time monitoring of systems are achieved through active monitoring tools. DTS provides active monitoring tools to DHHS through its service level agreement (SLA). Because of this, DHHS will review SAFE and eChart to identify the feasibility of flagging anomalous or unauthorized access within these systems with existing active monitoring tools. To the extent controls are reasonably practical, DHHS will develop POA&Ms to create and adopt these controls.

How: DHHS will review the eChart and SAFE to determine whether these systems are configurable to adopt compensating controls to achieve similar outcomes to monitoring anomalous or unauthorized access. If the systems are not configurable to achieve these functions, DHHS will consider the feasibility of developing these compensating controls. After this feasibility analysis, DHHS will identify reasonable controls within NIST SP 800-53 and create POA&Ms to create and implement them.

When: DHHS will conduct a feasibility analysis, select mitigating controls, if applicable, and create POA&Ms to implement selected controls by March 31, 2026.

Responsible Staff: Patrick Thomas, Director of Information Privacy and Security, Tonya Myrup, Division of Child and Family Services Director, and Dallas Earnshaw, Director of Utah State Hospital.

Current Status: DCFS and USH have worked with Utah Division of Technology Services (DTS) to better provide monitoring of system access logs in SAFE and eCHART. Prior to the audit both systems had system logging and both DCFS and USH periodically monitored these logs. DCFS has inputted SAFE's access logs into a business intelligence (BI) tool that it reviews daily to detect anomalous activities. USH is working with DTS to create a tool in eCHART that flags anomalous activities that can be reviewed daily. These tasks of selecting controls and POA&Ms have largely been achieved. The remaining steps are to fine tune the BI tool and build out the eCHART functionality.

Recommendation 1-4. We recommend that DHHS implement more stringent access controls and adequate monitoring metrics by Auditing.

Department Response: DHHS concurs with this recommendation.

What: DHHS will review its current audit controls for SAFE and eChart and identify additional technical and administrative controls to perform this function, if appropriate and necessary. Current examples of auditing practices at the Utah State Hospital (USH) include: monthly auditing of access by an employee to records outside of the employee's assigned work unit; requiring justification for access of records outside of an employee's work unit; and requiring submitted justifications for access to records for patients who were discharged more than 60 days ago.

As appropriate, DHHS will adopt additional AU controls from the NIST SP 800-53 and create POA&Ms to create and implement them.

How: DHHS will conduct a feasibility analysis of adopting additional technical and administrative AU controls. Based on this feasibility analysis, DHHS will, as appropriate, adopt additional AU controls from the NIST SP 800-53 and create POA&Ms to create and implement them consistent with NIST SP 800-37.

When: DHHS will conduct a feasibility analysis, select mitigating controls, if applicable, and create POA&Ms to implement selected controls by March 31, 2026.

Responsible Staff: Patrick Thomas, Director of Information Privacy and Security, Tonya Myrup, Division of Child and Family Services Director, and Dallas Earnshaw, Director of Utah State Hospital.

Current Status: Both DCFS and USH are enhancing their auditing controls in SAFE and eCHART by using the monitoring tools described above. DCFS is currently auditing access logs in its BI tool daily. Once the tool is developed in USH, USH will have the ability to audit its access logs daily. The selection of controls and Plans of action and milestones (POA&Ms) have already been completed. DCFS needs to fine tune its BI tool and USH needs to work with DTS to finish its monitoring tools. DHHS is in the process of updating its audit and accountability (AU) policy to align this policy with the AU controls in NIST SP 800-53 rev. 5. The AU policy is ready to be reviewed by the Policy Committee at DHHS which will be finalized by the March 31, 2026 deadline.

Finding 2. Lack of Monitoring and Quality Control related to the DCFS's GRAMA Team

Risk Rating: High

From January 1 to June 10, 2025, the 11-person Division of Child and Family Services' (DCFS) "GRAMA team" received 2,195 record requests—an average of 20 requests per workday. In total, the team released 49,638 pages of documents during that period. Individual requests take between one and 12 months to complete by the team, despite the primary timeline for responding to Government Records Access and Management Act (GRAMA) requests being just 10 days.[5] Furthermore, processing delays have driven a sharp increase in GRAMA appeals—from 34 in Fiscal Year (FY) 2023 to 57 in FY 2024, and 162 in FY 2025, with 80% of the 2025 appeals related to delays in record provision.[6]

DCFS GRAMA requests involve highly sensitive information, with some including audio recordings that need to be reviewed, details on child abuse, child removals, and family investigations. Despite the nature and volume of the work, the team operates without a designated quality control role. There are no consistent secondary reviews, peer checks, or oversight processes to verify outgoing records. Staff are expected to identify and report their own errors while managing large caseloads. According to the division's privacy officer and the team supervisor, mistakes—such as sending data to the wrong recipient are sometimes detected only after the information has been released or reported to the entity by an external stakeholder. There is no structured process in place to audit past responses or identify systemic issues.

[5] Utah Code: 63G-2-204 4 b

[6] Related to the extraordinary circumstances extension under *Utah Code* 63G-2-401 1b

Utah Code § 63G-2-204 mandates timely resolution of records requests, including expedited procedures and provisions for delays. The GRAMA Basic Checklist, developed internally, requires diligent review of records and accuracy.

Despite awareness of the workload imbalance, management did not make changes to staffing or process as of time of the initiation of this audit.

Without internal controls to catch such issues, errors go unnoticed, increasing the risk of noncompliance, poor service delivery, and data handling failures. Incidents and breaches are not adequately recorded, with the entity being able to provide only "estimated numbers" of incidents and breaches for the last 3 years, upon request of the auditors.

A functional and secure anonymous reporting channel does not exist, limiting staff or other stakeholders' ability to raise concerns about missteps or privacy risks through protected means without fear of retaliation from leadership.

Risk rating and rationale: High

The likelihood of mistakes made within an under-resourced group is likely and the severity of potential impact is high.

Recommendations:

1. *Resources.*

   We recommend that DCFS management assess whether current staffing and resources are sufficient to effectively manage workloads and maintain quality standards. Consideration should be given to ensuring adequate tiered oversight and review capacity before DCFS releases records.

2. *Process*

   We recommend that in addition to reviewing the resources, the DCFS management re-evaluate current processes for handling, transcribing, and redacting audio recordings, as well as the storage and distribution of sensitive documents, to identify opportunities for reducing complexity and minimizing potential exposure points and to add tiered review where needed.

3. *Auditing*

   We recommend that DCFS management strengthen supervisory and audit activities related to record provision, including periodic tiered reviews and retrospective checks, and ensure that results are regularly communicated to leadership for continued process improvement.

DHHS's Response:

Recommendation 2-1. We recommend that DCFS management assess whether current staffing and resources are sufficient to effectively manage workloads and maintain quality standards. Consideration should be given to ensuring adequate tiered oversight and review capacity before DCFS releases records.

Department Response: DHHS concurs with this recommendation.

What: A few months prior to the audit, on March 5, 2025, DCFS and DHHS executive leadership met to address staffing shortages within the GRAMA team. The GRAMA team had been experiencing high turnover and multiple absences due to FMLA, which complicated accurate personnel assessment. The Division of Continuous Quality and Improvement (CQI) was engaged to evaluate the current GRAMA structure, including processes, training, and communication, to identify opportunities for efficiency, streamlining, and overall improvements. Their recommendations encompassed resources and staffing necessary for the GRAMA team to more efficiently and effectively manage workload, timeliness of request processing, and quality standards.

How: CQI completed its evaluation in June 2025 and made a total of 20 recommendations to DCFS and DHHS leadership. After approval and prioritization, DCFS began implementing the recommendations with support from CQI. These included restructuring the DCFS GRAMA team to redistribute job responsibilities, allowing managers to focus on supervisory duties, and quality assurance activities. DCFS has hired an additional GRAMA manager and is in the process of hiring an additional 6 full-time employees to support fulfilling records requests accurately and timely.

DCFS has increased GRAMA staffing and continues to implement other recommendations from CQI, including an improved tracker, workflow, and training. Redistributed responsibilities and clarified roles will allow for the team managers to include quality assurance checks as a routine process in their day-to-day supervisory tasks and training of staff. All of these recommendations will collectively support manageable workloads and help DCFS maintain quality standards.

When: This recommendation has been completed.

Responsible Staff: N/A

Current Status: This recommendation was completed as of the initial response.

Recommendation 2-2. We recommend that in addition to reviewing the resources, the DCFS management re-evaluate current processes for handling, transcribing, and redacting audio recordings, as well as the storage and distribution of sensitive documents, to identify opportunities for reducing complexity and minimizing potential exposure points and to add tiered review where needed.

Department Response: DHHS concurs with this recommendation.

What: As referenced in the response to 2-1, CQI has conducted an operational improvement project with the DCFS GRAMA team. CQI's review resulted in recommendations made in the categories of structure, process and systems, training and resources, communication, and culture. One of the primary aims of these recommendations is to create greater consistency in processing across GRAMA specialists and to ensure all staffare following efficient and secure procedures.

How: There are several CQI recommendations that are in process of implementation that contribute to this audit's recommendation. First, DCFS has developed a standard operating procedure (SOP) for the GRAMA process for all staffto reference and follow. This includes the workflows for processing, storage of requests in a new tracker, and the tools used for redaction, including audio files. Second, redistributed roles and responsibilities removed many competing priorities for GRAMA specialists' time and focus. These adjustments allow for focused attention on redaction and remove many interruptions that in the past may have created delays or mistakes. Third, DCFS has shifted from individual case loads to instead having a central team queue where staffpull a case at a time. The imbalance of individual workloads was creating problems in processing, consistency, and bottlenecks. This adjustment allows specialists to focus on the single case currently assigned to them and completing it accurately. This includes their processing of audio-visual files, which are more complicated to redact and require dedicated focus to ensure accuracy.

When:

SOP development – December 31, 2025

Redistributed roles and responsibilities - Completed

Central team queue - Completed

Responsible Staff: Charri Brummer, DCFS Assistant Director; Steven Sullivan, DCFS Support Services Administrator

Current Status: DCFS has partnered with the DHHS Division of Continuous Quality and Improvement (CQI) to identify ways to improve its GRAMA team's productivity. Based on CQI's feedback, DCFS has implemented the following: increased GRAMA staffing and supervision; explored automated tools to improve efficiency and accuracy; adopted a standard operating procedure; implemented an improved tracker, workflow, and training; redistributed responsibilities; and clarified roles to provide for quality assurance checks.

Additionally, DCFS centralized the queue for redaction assignment, which has been very successful and created greater efficiency. These combined efforts have decreased the GRAMA backlog from between 9-12 months to 5.5 months. Moreover, at the time DCFS implemented the process improvements, the oldest open request was from February 2024. As of January 29, 2026, the oldest open request is from July 2025. While DCFS is making progress in addressing the challenges with the many GRAMA requests it receives, it continues to make process and system improvements to reduce complexity and minimize exposure points. The additional activities include developing an automated system, SharePoint. In addition, IPS and DCFS have met with companies offering AI for redaction purposes and are continuing to explore cost and benefit.

DCFS has amended the GRAMA request form to include an option to receive recorded interviews in an audio format or as a transcript, which may result in a fee to cover the cost of additional redaction time.

Recommendation 2-3. We recommend that DCFS management strengthen supervisory and audit activities related to record provision, including periodic tiered reviews and retrospective checks, and ensure that results are regularly communicated to leadership for continued process improvement.

Department Response: DHHS concurs with this recommendation.

What: DCFS had identified weaknesses in its supervisory structure and management of this team. The decision to hire an additional team manager and to split the team into more manageable sizes (6-7 direct reports rather than 10-12) will significantly increase the amount of time able to be spent on direct staff supervision, quality assurance reviews, and subsequent training. The findings of CQI supported their conclusions and identified opportunities to build quality assurance (QA) more consistently into the team's process.

How: Redistributed responsibilities now allow more time for the team managers to include QA reviews of each GRAMA specialist, and minimum QA levels are being established (i.e. X% of a specialist's cases must be reviewed per month). This will help managers to better identify patterns of mistakes from specific staff and correct them with the staff in a more timely, and proactive, manner. If patterns emerge across multiple staff, the managers will evaluate if procedural changes or more training is needed for the team. Third, DCFS is building a structured training program for new employees that includes tools, practice, and a graduated transition from training with QA and real-time feedback from their manager as they begin real redaction work. This will ensure that all staff receive the same information and are trained up to DCFS' standards before processing real requests.

When:

Redistributed responsibilities - Completed.

Establish QA minimum levels - December 31, 2025

Create a structured training program - March 1, 2026

Responsible Staff: Charri Brummer, Assistant Director; Steven Sullivan, Support Services Administrator

Current Status: DCFS added an additional GRAMA supervisor to improve coaching and quality assurance.

The two GRAMA supervisors are now meeting individually with new GRAMA specialists to review their Quality Assurance (QA) results and provide immediate feedback. We have established minimum QA requirements for new GRAMA specialists with a standard frequency that progresses from intensive oversight to periodic ongoing reviews based on the accuracy of their redactions.

We are actively collaborating with the Professional Development Team to create a comprehensive training program for new GRAMA employees. The estimated date for completion is March 2026. The new training will feature:

- Self-paced learning modules (slide decks).
- Shadowing and direct practice opportunities.
- Direct mentoring and performance evaluation conducted by a supervisor.

In partnership with the Office of Innovation (OOI), DCFS is also establishing a standardized timeline and performance measures (including QAs) for experienced GRAMA employees. The SOP manual is being used regularly, along with the temporary new employee training and QA measures. The two GRAMA supervisors are providing regular updates to the GRAMA administrator who is providing feedback and additional support to the teams as needed.

Finding 3. Inadequate Incident Response Preparedness

Risk Rating: High

Main incident response policy (04-14, Incident Response Procedures) lacks logically defined severity tiers, assigned roles, escalation procedures, and criteria for assessing impact and likelihood. The division into “serious” and “non-serious” incidents as currently presented in the policy is not effective. While an incident response program exists on paper, there are gaps in how the entity operationalized it, manifested by low awareness of its existence and confusion amongst employees. This limits the organization’s ability to coordinate an effective response.

Nine out of 21 interviewed staff were unaware of which policies exist, their contents, and—in some cases—where to find them, even though they held roles in or adjacent to incident response. The 2025 DHHS Privacy & Security Awareness training provides general guidance but does not explain specific responsibilities, escalation pathways, or practical examples of incident types. Staff struggled to articulate their responsibilities in privacy matters and were unable to identify the correct chain of command and accountability in incident response. Ten of the 21 interviewees, most of them in management positions, expressed confusion about the protocol, including who holds ultimate responsibility for each part of the incident response process.

Staff across both centralized and decentralized roles of the Information Privacy and Security team maintain their own incident records in personal files, rather than using a dedicated centralized repository, and some use the terms “incident” and “breach” interchangeably. DHHS does not record breaches and incidents appropriately. It's important to clearly define what constitutes a breach, as a breach—not just any incident—triggers specific regulatory obligations, including mandatory reporting and strict timelines. For example, a breach may require notification within five days to the Cyber Center, the Office of the Attorney General,[7] the media or national consumer credit authorities, depending on the number of affected individuals.[8]

Onboarding and refresher training lack sufficient detail on incident response, leaving staff unclear about their roles and obligations. Supporting materials like the IR Program Binder are not integrated into systematic training. As a result, confusion persists, and privacy and incident response responsibilities remain fragmented and poorly communicated across the organization.

Incident response procedures are on a four-year review cycle and table-top exercises[9] are not conducted. Specific timelines for action are not outlined in the incident response documents.

Nationally recognized industry standards[10] as well as Utah Cyber Center guidance and the DTS Cybersecurity Incident Response Plan[11] require a documented incident response process with clear role definitions, classification criteria, regular review and adequate training. Employees must understand their responsibilities, escalation procedures, and reporting expectations. Regular training and centralized, well-known documentation and processes are essential for effective response.

Staff may fail to identify, report, or escalate incidents efficiently and consistently. Misclassification and delays increase exposure and reduce the effectiveness of containment. The organization’s ability to manage privacy or security incidents is significantly weakened.

Risk Rating and Rationale: High

The likelihood of deviation from a desirable and effective process is likely in the face of inconsistent and poorly known guidelines and the severity of impact is high due to sensitivity and volume of records the entity handles.

Recommendations:

[7] Utah Code section 63A-19-405.
[8] Utah Code section 63A-19-406
[9] Simulated scenario-based discussion used to test and evaluate response plans, procedures, and coordination among different stakeholders.
[10] Such as NIST SP 800-61 Rev. 6, ISO/IEC 27035
[11] Utah DTS *Cybersecurity Incident Response* https://privacy.utah.gov/incident-response, Utah Cyber Center https://cybercenter.utah.gov,

We recommend that DHHS regularly reviews and revises Policy 04-14 and related guidelines (e.g., via an annual update), including the Incident Response Program, to establish more frequent and systematic review and communication that supports timely and effective incident handling. The program should also include tabletop exercises and the incorporation of lessons learned into their annual incident response activities.

At a minimum, management should evaluate the following:

1. *Roles and Responsibilities*
   Defining roles, decision-making authority, and escalation paths for incident response, including responsibility for breach determination and reporting. Training staff on the scope of their roles.

2. *Classification*
   Implementing a consistent, entity wide method for classifying and recording incidents and breaches, with predefined response tiers triggered by the type of breach, its impact, and the sensitivity of the affected data. This will support effective prioritization and resource allocation.

3. *Notification and Resolution Timelines:*
   Defining, codifying and routinely reviewing expected response timelines to ensure alignment with legal requirements, public expectations, and effective communication practices.

DHHS's Response:

Recommendation 3-1. We recommend that DHHS regularly reviews and revises Policy 04-14 and related guidelines (e.g., via an annual update), including the Incident Response Program, to establish more frequent and systematic review and communication that supports timely and effective incident handling. The program should also include tabletop exercises and the incorporation of lessons learned into their annual response activities.

At a minimum, management should evaluate the following: 1) Roles and responsibilities, 2) Classification, and 3) Notification and Resolution Timelines

Department Response: The department concurs with this recommendation.

What: The department will update its incident response policy and other documentation with clear descriptions of staff roles and responsibilities, classifications of incidents and breaches, and notification and resolution timelines that comply with the department's obligations under federal and state laws.

How: The Office of Information Privacy and Security (IPS) will review and update the department's incident response policy, create additional reference material, if appropriate, and train staff involved on the updated incident response policy and procedure.

When: By March 31, 2026

Responsible Staff: Patrick Thomas, Director of the Office of Information Privacy and Security; Kyle Lunt, Director, Division of Data, Systems & Evaluation

Current Status: DHHS has a preliminary draft of its incident response (IR) policy that will replace its IR policy originally drafted by Deloitte. This policy will better align with the IR controls in the NIST SP 800-53 rev. 5. DHHS has attended training from CISA and plans to update its IR plan to incorporate guidance from CISA's Cybersecurity Incident & Vulnerability Response Playbooks and NIST SP 800-61 rev. 2.

Additionally, DHHS is in the process of drafting a breach determination standard operating procedure to formalize its breach determination team's membership, voting, roles, and responsibilities. It expects to have created these documents by March 31, 2026. DHHS will then undergo its policy review and approval process for the IR policy. DHHS conducts IR tabletop exercises every other week with its central privacy and security staff and will conduct a department-wide IR tabletop exercise in the summer 2026 based on guidance from CISA.