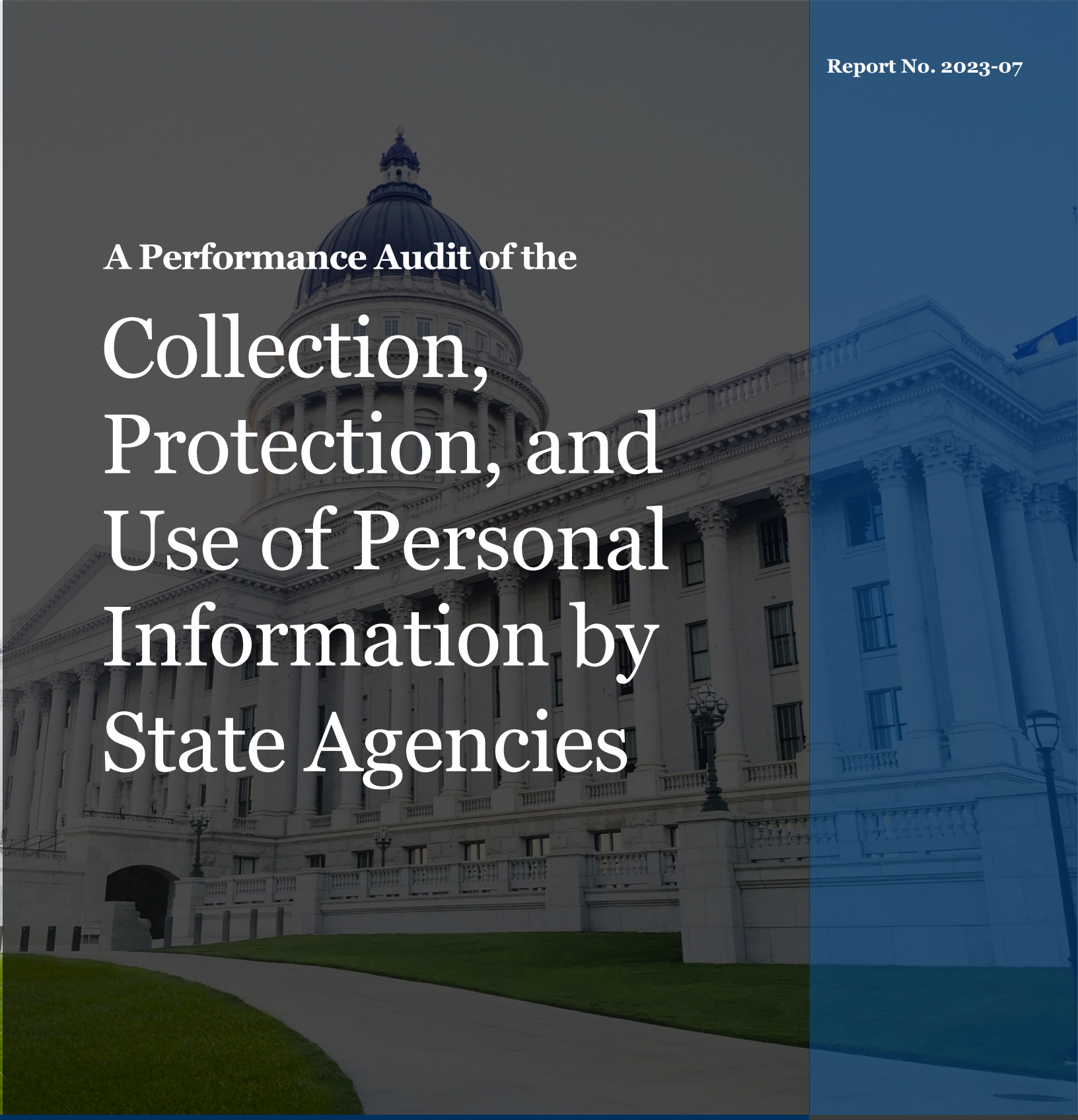
Report No. 2023-07



A Performance Audit of the

Collection, Protection, and Use of Personal Information by State Agencies

Office of the Legislative Auditor General

Report to the **UTAH LEGISLATURE**

LEGISLATIVE AUDITOR GENERAL

LEGISLATIVE
AUDITOR GENERAL

LEGISLATIVE AUDITOR GENERAL

The mission of the Office of the Legislative Auditor General is to serve the Utah Legislature and the citizens of Utah by providing objective and credible information, in-depth analysis, findings, and conclusions that help legislators and other decision makers: Improve Programs, Reduce Costs, and Promote Accountability

Audit Subcommittee

President J. Stuart Adams, Co-Chair
President of the Senate

Senate Evan J. Vickers
Senate Majority Leader

Senator Luz Escamilla
Senate Minority Leader

Speaker Brad R. Wilson, Co-Chair
Speaker of the House

Representative Mike Schultz
House Majority Leader

Representative Angela Romero
House Minority Leader

Audit Staff

Kade R. Minchey, Auditor General, CIA, CFE

Jesse Martinson, Manager, CIA

Zackery King, Audit Supervisor, CPA, CFE

Morgan Hagey, Audit Staff

Office of the Legislative Auditor General

Kade R. Minchey, Legislative Auditor General

W315 House Building State Capitol Complex | Salt Lake City, UT 84114 | Phone: 801.538.1033

Audit Subcommittee of the Legislative Management Committee
President J. Stuart Adams, Co-Chair | Speaker Brad R. Wilson, Co-Chair
Senator Luz Escamilla | Senator Evan J. Vickers
Representative Angela Romero | Representative Mike Schultz

June 13, 2023

TO: THE UTAH STATE LEGISLATURE

Transmitted herewith is our report:

"A Performance Audit of the Collection, Protection, and Use of Personal Information by State Agencies" Report #2023-07

An audit summary is found at the front of the report. The scope and objectives of the audit are included in the audit summary. In addition, each chapter has a corresponding chapter summary found at its beginning.

This audit was requested by Senator Kirk Cullimore, Senator Wayne Harper, Senator Daniel McCay, Senator Mike Kennedy, Senator Curtis Bramble, Senator Jacob Anderegg, Senator Lincoln Fillmore, Senator Keith Grover, and Senator Jerry Stevenson.

We will be happy to meet with appropriate legislative committees, individual legislators, and other state officials to discuss any item contained in the report in order to facilitate the implementation of the recommendations.

Sincerely,

Kade Minchey

Kade R. Minchey, CIA, CFE

Auditor General

kminchey@le.utah.gov

LEGISLATIVE AUDITOR GENERAL

AUDIT SUMMARY
REPORT #2023-07| June 2023

Office of the Legislative Auditor General | Kade R. Minchey, Auditor General

PERFORMANCE AUDIT

COLLECTION, PROTECTION, AND USE OF PERSONAL INFORMATION

AUDIT REQUEST

The Legislative Audit Subcommittee requested an audit to provide assurance that information collected by state agencies are necessary and properly safeguarded.

This audit reviews state agencies' data collection, policies, and the use of data within agencies.

BACKGROUND

For government, data is essential to manage and evaluate statutory programs and to provide services. However, data also introduces risks, both for individuals who provide their personal information, and for businesses and government entities who process and use it.

Data privacy has become a topic of focus in the private sector as society is increasingly digitized. Data privacy is also gaining momentum in the public sectors and more focus is being placed on government agencies and how they handle the personal information of citizens.

KEY FINDINGS

- 1.1 Current data collection and sharing practices by state agencies create data privacy risk. Statutory data privacy guardrails could alleviate the risk.
- 1.2 Without statutory direction, determining data privacy policy falls to agencies. Agencies have varying definitions of data privacy, and some appear to be unfamiliar with data privacy principles.
- 2.1 Office of Vital Records and Statistics data processing of birth registration data shows data privacy weaknesses.
- 2.2 Office of Vital Records and Statistics data sharing and distribution of birth registration needs to be reviewed to ensure it complies with provisions of federal privacy laws.

RECOMMENDATIONS

- 1.1 The Legislature should consider if guardrails are needed to balance the benefits of data and data sharing with data privacy practices in agencies.
- 1.2 The Legislature should consider the merits of passing a data privacy act into statute to provide a data privacy governance structure for state agencies and incorporate data privacy principles into their data processing and sharing practice.
- 1.3 The Legislature should consider defining data privacy in statute for all state agencies.
- 2.1 The Legislature should consider clarifying the collection of birth registration data.
- 2.2 The Legislature should consider the merits of requiring government entities to adopt data privacy principles that include items such as: clear consent, notice, and the disclosure of data collection, use, and sharing.
- 2.3 The Legislature should consider the Office of Vital Records and Statistics data collection and processing practices and whether to establish data privacy policy for state agencies in Utah.

Summary continues on back >>

REPORT SUMMARY

Need for Data Privacy Framework is Growing, Additional Opportunities Exist

As we have probed the data privacy questions raised in this audit, it has become clear that data privacy historically has not been a primary focus for some state level entities. Some entities are collecting personally identifiable information with minimal oversight. In addition, data privacy practices vary across the state. The Legislature should consider the merits of passing a data privacy act into statute.

Data Privacy Questions Exist in the Office of Vital Records and Statistics, Improvements Can Be Made

We conducted an in-depth case study of birth registration data processing carried out by the Office of Vital Records and Statistics. We worked with a consultant to perform a review of these processes according to a privacy program framework. The findings of the consultant along with our audit findings inform our recommendations.

According to our consultant's review and our data privacy analysis, we are concerned that OVRS may not be in compliance with data privacy standards for its birth registration data collection and distribution. Improvements can be made to balance data benefits with data privacy rights of new mothers in this process.

All of our recommendations are to the Legislature because we believe this is a policy decision that is Legislative prerogative to decide.

Inventory of Data Sharing agreements in the Executive Branch

Data sharing is widespread within and between state agencies, and with external entities. About 92 percent of DSAs shown in the chart facilitate the exchange of PII.

Data sharing is beneficial to the functioning of state government, but it also increases data privacy risk for individuals.

For clarity in the chart, only agencies that submitted DSAs to us are graphed. Agreements for specific divisions are counted within the state agencies that administer the respective DSAs. A DSA can be a unique agreement, but several agencies have DSAs they sign with multiple different parties.

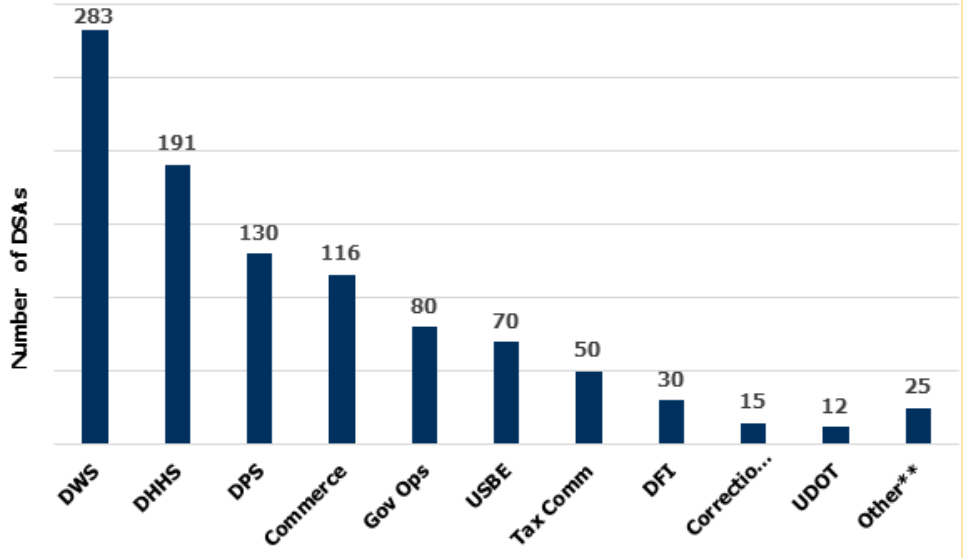


Table of Contents

LEGISLATIVE AUDITOR GENERAL

CHAPTER 1 Summary

Need for Data Privacy Framework is Growing, Additional Opportunities Exist

BACKGROUND

For government agencies, having data is essential for managing and evaluating statutory programs and for providing services. However, having data also introduces risks, both for individuals who provide their personal information, and for businesses and government entities that process and use the data. Data privacy in the private sector has become a focus and it is gaining momentum in the public sectors, with more attention on government agencies and how they handle the personal information of citizens. Agencies' sharing information, which this report does not discourage, is a powerful tool for better service. This report is concerned with privacy guidelines.

FINDING 1.1
State agencies' current data collection and sharing practices create data privacy risk. Statutory data privacy guardrails could alleviate the risk.

RECOMMENDATION 1.1

We recommend the Legislature consider whether statutory guardrails are needed to balance the benefits of data with data privacy practices in state agencies.

FINDING 1.2
Without statutory direction, determining data privacy policy falls to state agencies. Agencies have varying definitions of data privacy, and some appear to be unfamiliar with data privacy principles.

RECOMMENDATION 1.2
We recommend that the Legislature consider the merits of passing a data privacy act into statute to provide state agencies with a data privacy governance structure and to incorporate principles of data privacy into their practices for data processing and sharing.

RECOMMENDATION 1.3
We recommend that the Legislature consider defining data privacy in statute for all state agencies.

CONCLUSION

As we have probed the data privacy questions raised in this audit, it has become clear that historically, data privacy has not been a primary focus for some state-level entities. Some entities collect personally identifiable information with minimal oversight. The Legislature should consider the merits of passing a data privacy act into statute.

Chapter 1
The Need for a Data Privacy Framework Is Growing; Additional Opportunities Exist

1.1 Data Privacy Risk Appears to Exist; Statutory Guardrails Can Balance State Agency Data Processing and Data Privacy Practices

Although Utah has statute and Administrative Rule focused on cybersecurity measures and data protection, it does not have a statutory policy on data privacy to govern state agencies. Creating statutory data privacy policy is one area the Legislature should consider if more balance is needed between state agencies' data collection and sharing activities and their data privacy practices.

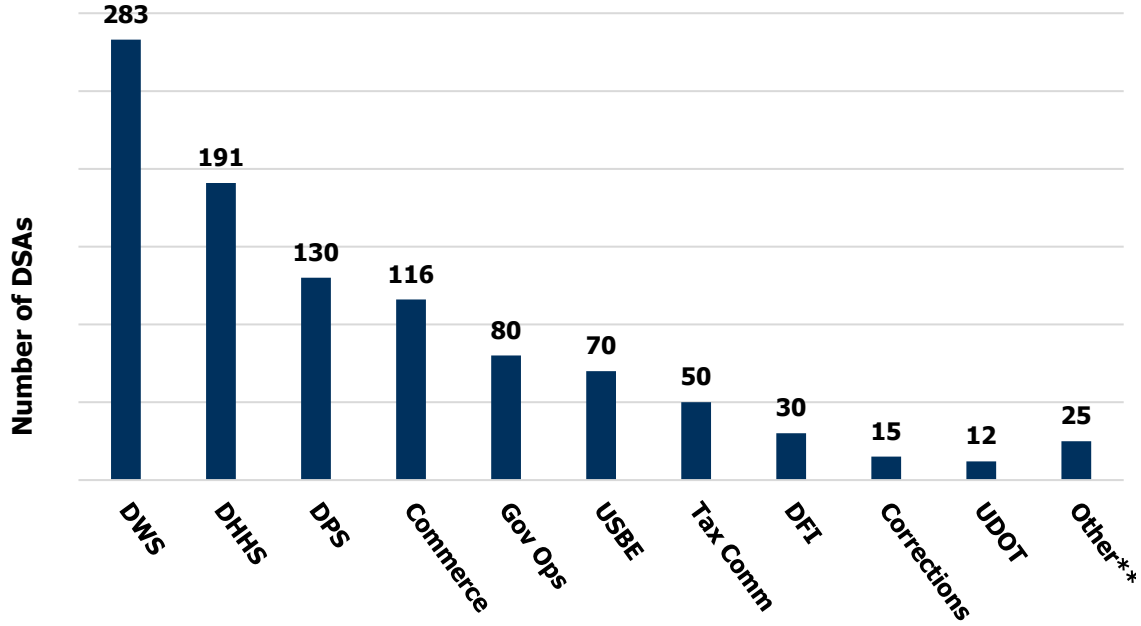
Data Sharing among Agencies and with Third Parties Is Widespread, Increasing Data Privacy Risk in Utah

To understand the breadth and depth of data sharing in Utah agencies, our audit team requested data-sharing agreements (DSAs) from Utah's executive agencies. In reply, we received about one thousand DSAs from forty-one different divisions. Of these, twenty-three divisions within seventeen different agencies provided DSAs that specify how they export data to another state agency or other external entity. Eighteen divisions responded they do not share data.

Data sharing entails the exchange of data from one state agency to another, or to federal government entities, external entities like universities, and third-party vendors.

DSAs are not inherently wrong or problematic. In some cases, they are essential.

Figure 1.1 DSAs Are Common in State Agencies. Only agencies that responded with DSAs are included in the chart. For clarity, agreements for specific divisions are counted within the state agencies that administer the respective DSAs. A DSA can be a unique agreement; however, several agencies have DSAs they sign with multiple parties.*



Source: Auditor generated from agency self-reported data
** Each agency submitted at least two DSAs*
*** Other – Dept. of Environmental Quality, Dept. of Alcoholic Beverage Services, Public Service Commission, Dept. of Natural Resources, Governor's Office of Economic Opportunity, Salt Lake Community College, and Tooele Technical College.*

Figure 1.1 indicates widespread data sharing among state agencies. About 92 percent of the DSAs shown in Figure 1.1 facilitate the exchange of personally identifiable Information (PII). Data is shared between divisions in the same agency, between different state agencies, with external entities like universities and non-profit organizations, with federal government agencies, and with third-party vendors. Data sharing is done to aid agencies in their statutory duties, administer federal programs, and procure operational services by contract.

About 92 percent of DSAs reported to us facilitate the exchange of PII.

We sampled and analyzed more than one hundred DSAs from those submitted by state agencies to understand their data privacy protections. Our Findings are summarized below.

Data Sharing Agreement Strengths	Data Sharing Agreement Weaknesses
Data security is common.	Data privacy is not explicitly addressed.
Agencies administering federal programs or that receive/distribute federal funds have more well-developed data privacy practices. Federal laws such as HIPAA and FERPA drive this condition.	Not all agencies administer federal programs or funds and therefore do not have federal influence in their DSAs.
Elements of data privacy exist by virtue of overlapping tenets with data security.	Lack of data privacy elements that include data subject involvement or consent.
Facilitate the exchange of meaningful information that enhances the efficiency of program management.	Lack of, or underdeveloped risk management processes to oversee, monitor, and provide accountability.

A data privacy act that requires the incorporation of data privacy principles into data-sharing practices can bring balance to data processing in state agencies.

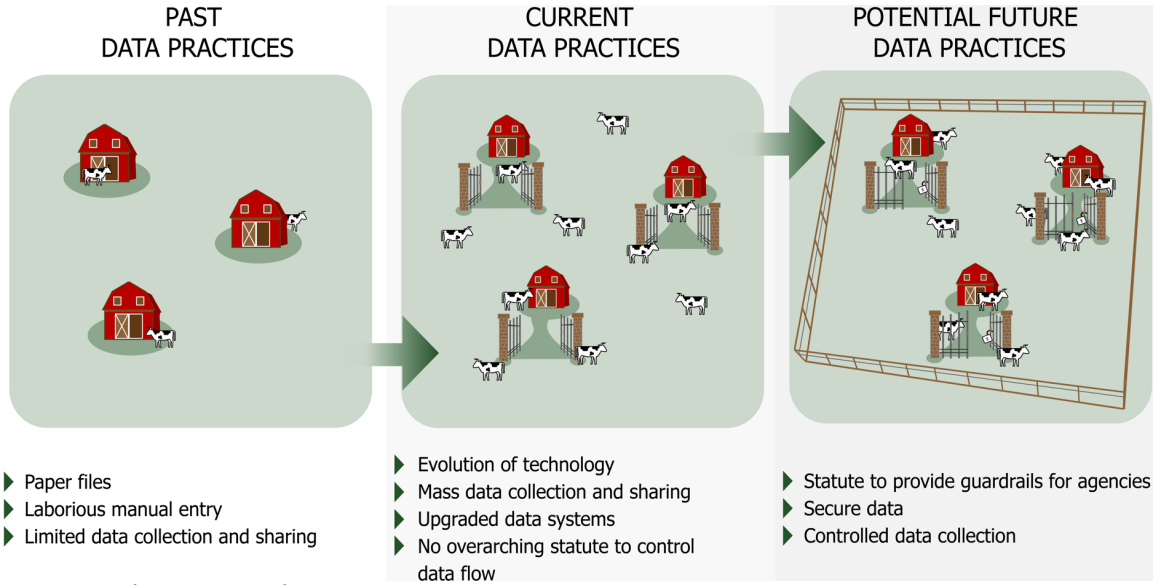
Current Practices Allow for Significant Data Collection and Sharing

Past data practices were siloed in agencies due to paper files and laborious manual entry – data sharing was uncommon. As digital capabilities have increased with technology innovation, agencies have transitioned to current data practices that use computer- and digital-based operations. Significant advances in government operations can result with data sharing. The concern we raise is that data collection via electronic platforms has greatly expanded the volume of PII that agencies process, and we believe the Legislature should consider whether data privacy policy is needed. Data security is a daily concern for agencies; this concern is heightened because the security gates are open due to significant data sharing between agencies and with external entities.

Significant improvement in government operations is possible with data sharing.

Data processing has greatly expanded with technology and digital advancement.

Legislature should consider whether guardrails are needed.



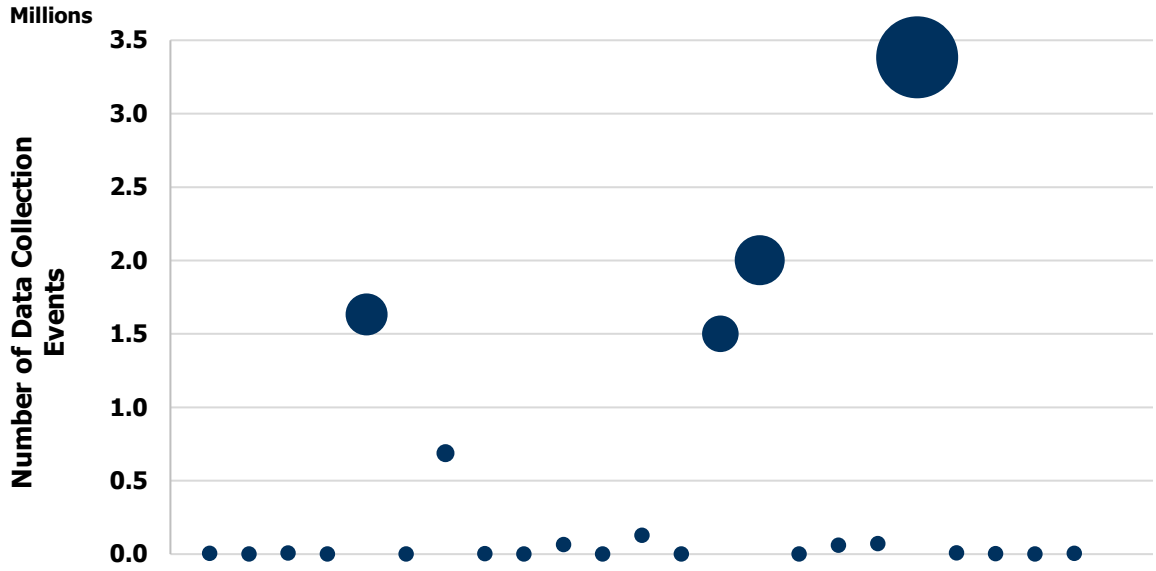
Source: Auditor generated

The profusion of PII and data sharing with current practices has enabled state agencies to address challenges of Utah citizens and provide services more efficiently and effectively. It has also resulted in more focus on privacy rights and data privacy practices within agencies. To alleviate data privacy risks associated with current practices, the Legislature could provide statutory guardrails to incorporate principles of data privacy into agency data-processing activities while allowing agencies to maintain the efficiencies gained with current practices.

As we conducted our fieldwork for this audit, we learned that the chief privacy officer (CPO) in the executive branch was also conducting a data privacy assessment. The CPO provided us with preliminary data from that assessment.

Figure 1.2 plots an estimate of "data collection events," or the number of times state agencies collected data from citizens within one year. Thirty-one agencies were assessed and twenty-three responded. Increased data collection leads to an increase in data privacy risk.

Figure 1.2 Some Agencies' Data Collection Events in the Millions. About 9.6 million data collection events by state agencies took place in calendar year 2022. This graph depicts the magnitude of data collection events, with each bubble representing a different agency.



Source: Chief privacy officer, Department of Government Operations

Out of twenty-three responding agencies, the median number of data collection events was five thousand. Some agencies reported zero[1], but as shown in Figure 1.2, one agency reached nearly 3.4 million collection events. This illustrates the frequency of data exchange from citizens to state agencies.

The most common data collection method for state agencies is web forms, confirming the widespread use of digital media for collecting data.

Methods for collecting data were also assessed by the CPO. Collection methods can include paper forms, PDF or Microsoft Word forms, video recordings, etc. The 9.6 million data collection events in one year, together with the number of DSAs shown in Figure 1.1, indicate the magnitude of data collection and processing performed by state agencies under the current policy framework, suggesting the impact of current data-processing activities on data privacy risk. The reliance on web-based, digital media to conduct state business stands out.

Impact of Data Privacy Risk Is Difficult to Estimate, Utah Examples Show That Impact Can Be High

A lack of data privacy policy in statute and *Administrative Rule* is a key contributing factor to high data privacy risk. The CPO's 2022 report to the Judiciary Interim Committee identifies the state's lack of a comprehensive privacy law that clearly outlines required privacy practices and policies for state agency privacy programs. The CPO also introduced the NIST Privacy Framework

[1] In reply to our inquiry, the CPO stated that many of the agencies reporting zero did so because they did not have enough data to provide an estimate, but in his opinion, they likely do collect PII.

in the report as a tool to show how a framework can be used to assess and identify privacy gaps.

The National Institute of Standards and Technology (NIST) is a widely used source in private and public sectors for cybersecurity standards. In 2020 NIST augmented its cybersecurity standards by producing the *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*. Drawing from its cybersecurity framework, NIST's privacy framework addresses privacy risk and specifies a strategy to systematically manage it.

Privacy controls are a function of the NIST privacy framework. One focus of controls is the "disassociability" of the data to protect individuals' privacy.

An example is aggregating data and/or de-identifying it.

We recommend this practice whenever possible.

The impact, or cost, of data privacy risk is difficult to estimate.

One agency information officer explained that there is not a concrete or reliable way to estimate the cost of a lack of data privacy, but that it is more appropriately measured on an individual basis.

In summary, people can experience adverse impacts to their personal and/or professional lives when their data is processed. Each time a person provides PII to a business or government agency for goods, services, licenses, etc., their potential for problems, or privacy risk, increases from greater exposure of their PII. Data privacy risk also grows each time PII is accessed by a third party, or when it is shared with external entities.

The NIST privacy framework also highlights risks and benefits with data processing. Risks and benefits exist for citizens and consumers who access goods and services, and for the businesses and governmental entities that process PII.

	Citizens/Consumers	Business	Government
Benefits	• Access to goods and services	• Increased profits • Operating efficiency • Increased productivity	• Improved service delivery • Operating efficiency • Research
Risks	• Identity Theft • Loss of privacy • Surveillance • Discrimination	• Data breach/leak • Fines • Litigation • Damaged reputation	• Loss of public trust • Data breach/leak • Cost to repair and reimburse

Source: Auditor summary of NIST Privacy Framework and other sources

Furthermore, there is increased scrutiny of state agencies and how they process citizens' personal data. Recent Utah examples of this spotlight include:

- 2020 reporting on the **Utah Division of Motor Vehicles' sharing of driver license data** of Utah citizens with the University of Utah, and the Legislature's actions in the 2020 General Session.

- 2021 reporting on **hospitals' collection of personal information of new mothers in exchange for birth certificates on behalf of the Office of Vital Records and Statistics,** and the Legislature's subsequent action in its 2022 General Session.

In both cases, Utah citizens expressed concern about the state government's use of their PII. In both cases, the Legislature passed bills to address privacy risks associated with the data processing procedures of state agencies.

Details of our in-depth case study of OVRS's data processing and privacy practices – such as how OVRS collects, manages, and shares its data – is contained in Chapter II.

RECOMMENDATION 1.1

We recommend the Legislature consider whether statutory guardrails are needed to balance the benefits of data with data privacy practices in state agencies.

1.2 Unfamiliarity with Data Privacy Principles at State Agencies, Data Privacy Practices Vary

In a survey to gauge data privacy knowledge and practices at state agencies, we asked a series of questions focused on privacy policies, notices, and how agencies define privacy including: (1) Does your agency have a data privacy policy? (2) Does your agency have a public privacy notice?, and 3) How does your agency define privacy? We received twenty-five responses from twenty-two agencies.

According to agency responses, it appears that compliance with requirements for public privacy notices is low. It also appears that agencies generally do not have strong internal policies for data privacy. There also appears to be confusion between data privacy notices and internal policies that drive data-processing activities. This confusion may be related to the many different defintions agencies provided for data privacy.

What is currently missing in statute and A*dministrative Rule* are policies and regulations focused on state agencies; i.e., how they process the PII they collect and how they manage it internally. Currently, agencies decide how to define privacy, which results in inconsistent data privacy practices.

Agencies do not appear to be complying with statute to have a public privacy notice in a prominent place, at all locations, where PII is collected on their websites.

Agency Compliance with Public Privacy Notice Requirements is Low

In our survey, we asked agencies if they have a public privacy notice for their website data collection activities. After review of their responses and documentation, about 77 percent either do not have a public privacy notice, or rely on the privacy notice from the Utah.gov website. These results appear to indicate that most

agencies do not have a public privacy notice for their data-processing activities. This is concerning with regards to best practices in data privacy; it also may be in violation of **UCA *63G-2-601(2)*** which requires governmental entities to provide notice, in a prominent place, at all locations where personal information is collected.

This result appears to add to the evidence that most state agencies currently do not adequately incorporate data privacy practices into their data-processing activities and overall operations.

Internal Data Privacy Policy for State Agencies Is Lacking

In addition to learning of agency practices with public privacy notices on their websites, we asked about agencies' internal data privacy policies. Importantly, no statute or rule is currently in place requiring agencies to have an internal data privacy policy.

In response to our survey, agencies submitted privacy policies that focus on data security rather than data privacy.

It appears that agencies are lacking adequate internal data privacy policies.

In response to our survey, two agencies provided the policy for public privacy notice for agency websites on Utah.gov. Upon further examination of the other policies that agencies submitted to our team, all but one focus on data security instead of data privacy. Given these findings, it is our opinion that almost none of the responding agencies appear to have an internal data privacy policy to govern their data processing activities.

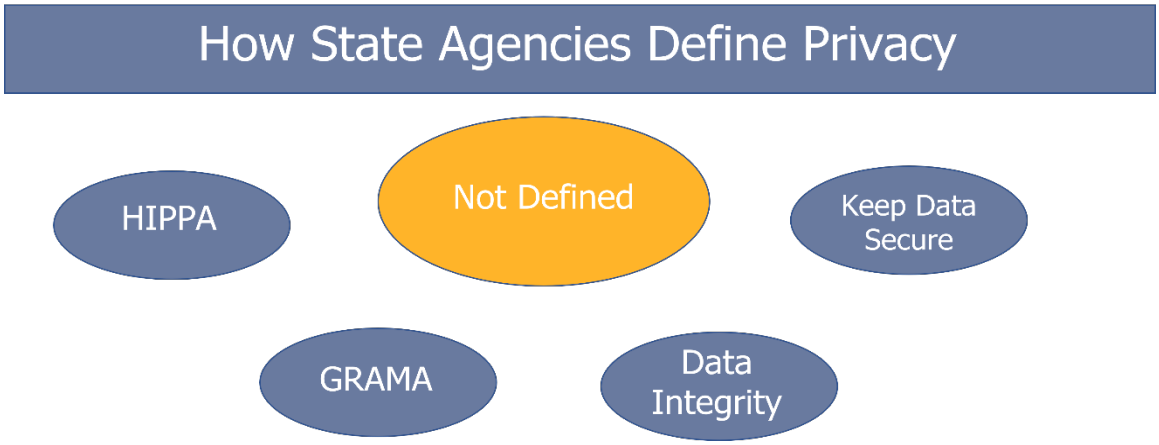
Without a state-driven data privacy act, agencies are left to their own to set internal data privacy policies. For agencies involved with federal programs, stronger data privacy actions are required through federal law. However, our survey results appear to indicate an unfamiliarity with data privacy principles and that data privacy policies are lacking at the agencies. We believe this is improving within agencies with the attention of the chief privacy officer, state privacy officer, and Personal Privacy Oversight Commission. However, these conditions provide further evidence that a data privacy act to set a governance structure for data processing, with data privacy principles, may be a prudent step for the Legislature to consider.

RECOMMENDATION 1.2

We recommend the Legislature consider the merits of passing a data privacy act into statute to provide a data privacy governance structure for state agencies and to incorporate data privacy principles into their data processing and sharing practices.

Statewide Data Privacy Policies Are Uncoordinated; Utah Agencies' Definitions of Data Privacy Are Not Consistent

In our data privacy survey to state agencies, we asked for each agency's definition of data privacy. State agencies have varying working definitions of data privacy that relate to the nature of their data usage. This results in a wide array of definitions being used across the state.



To best manage data privacy in the state, the Legislature could consider implementing a state-wide, comprehensive definition of data privacy akin to the one found in the CPO's privacy plan. This could help guide the management of data, while allowing agencies autonomy to manage their specific data needs.

RECOMMENDATION 1.3

In conjunction with considering a data privacy act, we recommend the Legislature consider defining data privacy in statute for all state entities.

CHAPTER 2 Summary

Data Privacy Questions Exist in the Office of Vital Records and Statistics, Improvements Can Be Made

BACKGROUND

We conducted an in-depth case study of birth registration data processing carried out by the Office of Vital Records and Statistics (OVRS). We worked with a consultant to perform a review of these processes based on a privacy program framework. The findings of the consultant, along with our audit findings, inform our recommendations. All recommendations of this audit are directed to the Legislature because we believe data privacy is a policy decision that is Legislative prerogative to decide.

FINDING 2.1

The processing of birth registration data by the Office of Vital Records and Statistics shows data privacy weaknesses. A consultant review fails OVRS in areas of governance, legal basis, policy and standards, data subject rights and program maintenance.

RECOMMENDATION 2.1

We recommend the Legislature consider clarifying the collection of birth registration data. One clarifying option is to separate essential birth registration information from research questions by creating two separate forms.

RECOMMENDATION 2.2

We recommend the Legislature consider the merits of requiring government entities to adopt data privacy principles that include items such as: clear consent, notice, and the disclosure of data collection, use, and sharing.

FINDING 2.2

Data sharing and distribution of birth registration data by the Office of Vital Records and Statistics needs to be reviewed to ensure compliance with provisions of federal privacy laws. Current processes raise data privacy concerns.

RECOMMENDATION 2.3

We recommend the Legislature consider Office of Vital Records and Statistics data collection and processing practices and whether to establish data privacy policy for state agencies in Utah.

CONCLUSION

According to our consultant's review and our data privacy analysis, we are concerned that OVRS may not be in compliance with data privacy standards for its collection and distribution of birth registration data. Improvements can be made to this process to balance data benefits with data privacy rights of new mothers.

Chapter 2
Data Privacy Questions Exist in the Office of Vital Records and Statistics, Improvements Can Be Made

2.1 The Office of Vital Records and Statistics Can Improve Data Privacy in How It Processes Data

We performed an in-depth data privacy case study of the Office of Vital Records and Statistics (OVRS), an office in the Department of Health and Human Services (DHHS). From birth registration to marriage records and death certificates, OVRS collects vital records data of Utah citizens, daily. These records contain personally identifiable information (PII) and personal health information (PHI). OVRS uses this data to fulfill its statutory duties. The information is also shared with other state agencies and external entities like federal government entities and universities for research purposes. We understand the importance of sharing information and the results that can be obtained. It is also important to ensure that the privacy of information is considered and is consistent with standards we are recommending be considered by the Legislature.

To enhance our in-depth case study, we hired a professional data privacy consultant to analyze OVRS's data practices for birth registration.[2] The graphic below shows eighteen pillars of the consultant's privacy program framework (PPF) which could be considered as a framework to evaluate the strength of data privacy practices in state agencies.

Source: Consultant report

[2] The consultant from Inspire! Privacy and Security LLC, has professional data privacy experience in multiple private sector corporations, including Microsoft and Facebook – Ireland. The consultant's full data privacy report is included in Appendix B.

For our audit, the consultant focused on six selected pillars (depicted in the orange boxes) regarding OVRS's birth registration processes. These include governance, legal basis, policies and standards, third-party risk management, data subject rights, and program maintenance. According to the consultant's final report, OVRS's data processing for birth registration falls short on all six of these data privacy pillars.

DHHS was cooperative in providing us with the necessary information for this case study. The department is actively working on policies to implement data privacy practices throughout its organization. Likewise, at OVRS. Management has shown us actions they have taken to protect PII and PHI. We are encouraged by these efforts. We also believe that more can be done to integrate data privacy practices into OVRS's data-collection and data-sharing practices with birth registration and certificates.

DHHS has shared agency-wide policies it is working on to address data security and incorporate data privacy principles into its divisions.

We are encouraged by this progress and encourage additional attention at OVRS for data processing of birth registration.

Existing Data Privacy Governance May Be Insufficient for the Complexity of OVRS Data Processing Activities

Our consultant's PPF has eleven different tasks by which birth registration governance was evaluated. The consultant failed OVRS in each of the eleven tasks. A basis for analysis was existing Utah statute and rule. In addition, we conducted preliminary audit work on the existing oversight structure that monitors and provides external checks and balances for OVRS's data-processing and data-sharing activities.

Two external bodies at DHHS could provide this type of oversight for OVRS's data processing: the Health Data Committee (HDC) and the Institutional Review Board (IRB). From our inquiries to OVRS management, it appears that neither of these oversight bodies provides an adequate level of accountability for OVRS's data-processing activities for birth registration. Management explained that HDC statute specifically excludes OVRS from its oversight. The IRB is more focused on data requests after the data is collected. Such requests come from external entities like universities for research purposes, as well as internal entities.

As a result, OVRS's only accountability mechanisms for processing birth registration data are internal, or via management approval. In our interactions with OVRS it became evident that internal policies have been inconsistent because they have depended on who the current OVRS director is. An example of a manager-driven policy is the process for data access and data sharing.

Former Data Sharing Practices with Other State Agencies Concerning. OVRS management described a scenario where other state agencies had access to the OVRS databases through a data query, giving them access to all data OVRS collected for birth registration. However, current management has halted this type of data access and has implemented data sharing agreements (DSAs). Implementing DSAs with parameters for data use is a positive step forward. A remaining concern, however, is that this appears to be driven by the current OVRS management, rather than an office policy. Without a robust policy for data sharing and data access, there is the risk of inconsistency and

unaccountability. This type of policy environment also heightens data privacy risk. The Legislature may want to consider creating a state-wide law that would require policies to be adopted to address issues around data sharing and data access.

Additionally, positive steps are being taken within DHHS to create a governance structure. However, additional attention should be paid to creating both internal and external governance apparatuses for OVRS data-collection and data-sharing activities. We encourage DHHS and OVRS to solidify OVRS policies and procedures in data sharing to ensure sound data privacy practices, long-term.

Consultant Review of OVRS's Processing of Birth Registration Data Reveals Data Privacy Weaknesses

Among other duties, a main function of OVRS is to register and certify births in the state of Utah. Statute currently requires hospitals to gather birth certificate data and file birth certificates with the state. Current practice in Utah is to gather additional research questions from new mothers, beyond what is essential to create a birth certificate. The Legislature may want to consider if requiring additional research questions in this process is still desired. In addition to this concern, other data privacy issues arise with the collection of PHI from new mothers, for example, there are weaknesses in notification and disclosure of the purpose of data collection and its use and distribution thereafter.

OVRS reported to us it is not subject to HIPAA for the PHI collected by hospitals when the data are uploaded to its database. This appears to create a gap in the data privacy requirements of birth registration data when OVRS receives it.

The Legislature could consider filling this gap in statute to ensure data privacy requirements are in place long-term.

While statutory provisions appear to allow for current data collection methods, our consultant raised concerns that data requested may exceed statutory limits of the Government Records Access and Management Act (GRAMA). This is because GRAMA requires adherence to federal privacy laws when PHI is requested, and federal privacy laws require entities to obtain consent from data subjects when collecting and using PHI.[3]

OVRS reported that it is not subject to privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA), which would mean any data privacy protections for data it processes are based solely on OVRS policy. Thus, there is a gap in the data-processing lifecycle of birth registration data collected from new mothers. In our discussions with OVRS and DHHS regarding this issue, it was explained that DHHS policies incorporate HIPAA-like policies for data processing. This is encouraging, but it also means the current DHHS administration is the driving force behind this policy approach and we are concerned that a different administration could have a different approach. Therefore, we believe this gap in data privacy law is one the Legislature should consider filling with statutory data privacy requirements.

[3] DHHS reported to us that OVRS is not a covered entity or business associate under HIPAA and therefore is not subject to its provisions. As a result, the PHI collected by hospitals is not considered to be PHI under HIPAA when transferred to OVRS.

When analyzing OVRS's data-collection methods through the lens of data privacy principles, we believe this demonstrates an area where a statewide data privacy policy may be needed. Furthermore, statute allows for the current collection methods in these areas. These issues are analyzed in detail below.

Data Collection Exceeds What Is Necessary for Birth Certificates and Raises Data Privacy Questions. The standard Utah birth certificate contains the following information of a newborn and its parents: (1) child's name, (2) child's sex, (3) the date, time, and place of birth, (4) child's weight, (5) parents' names, dates and places of birth, with the mother's resident city and state, and (6) the city and county of birth. ***UCA*** 26B-8-104(3) currently requires hospitals to gather required birth certificate data and file birth certificates. In hospitals, this data collection starts with a forty-three-question, paper questionnaire called the "Parent's Worksheet to Register Birth Information," which is included as Appendix C. This many questions exceeds the data points needed for a birth certificate, and multiple questions ask about the demographics, health, personal characteristics, etc. of the mother and father of the new baby.

From our discussions with OVRS, if a new mother does not fill out questions marked "Required" on the parent worksheet, birth clerks at hospitals have access to the medical records of new mothers and can fill in missing data before submitting it. Required questions are so marked because of a contract OVRS has entered into with the National Center for Health Statistics (NCHS). This contract obligates OVRS to collect PHI from new mothers and transfer it to NCHS, which uses the data for research purposes and distributes it to external entities for the same use. This contract and the statutory language allowing these methods are discussed in detail later in this chapter.

Data privacy concerns for the parent worksheet center on questions of proper disclosure and consent. However, without statutory policy, it is unclear if current practice should be changed. We recommend the Legislature consider the merits of adding data privacy principles into statute.

Data privacy concerns exist with unclear disclosure and consent rules when filing for a birth certificate. There is a general gap in law and policy in this area making it difficult to determine if current practices should be changed.

In addition, the parent worksheet combines "Required" questions with others that are marked "Optional" and are not necessary to obtain a birth certificate but are included for other purposes. Mixing questions in this manner creates an overly complex presentation of data collection, which can confuse the purposes and need for the data.

OVRS management reported to us they do not know whether birth clerks also fill in "Optional" questions before submitting new birth information to their data system,

which creates a possible control weakness in the data collection process that could enable the collection of PHI without consent.

Data Privacy Weaknesses with Transparency. Transparency is a tenet of data privacy that includes giving notice about the use of PII. Transparency centers on what data is collected, why it is collected, and how it will be used. The chief privacy officer (CPO) explained that giving notice can be considered equivalent to consent for government entities. This puts greater weight on the substance and quality of the notice.

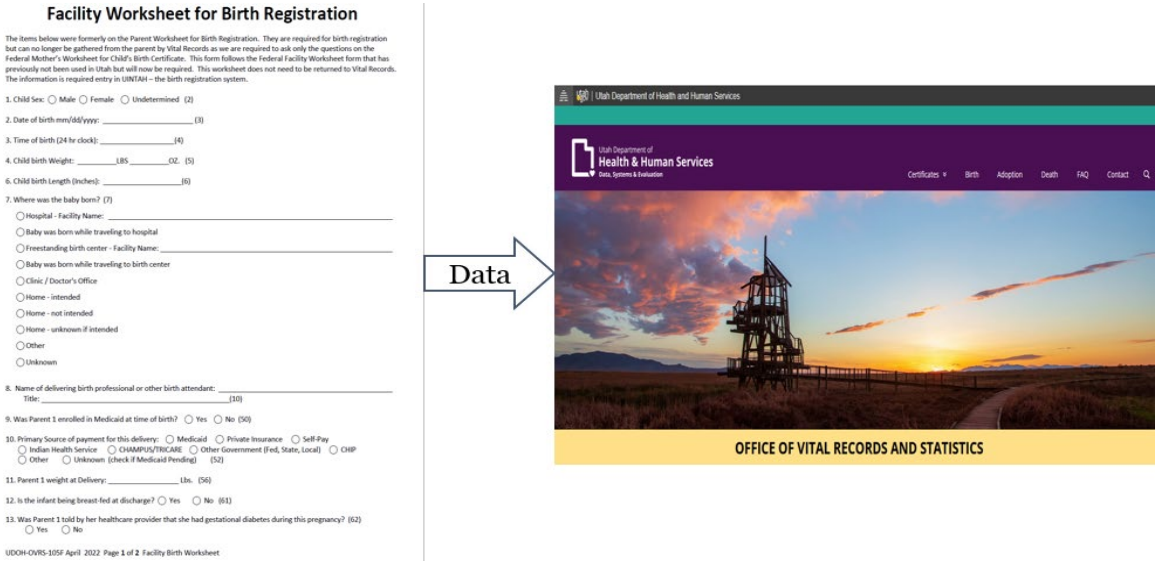
The current notice for the parent worksheet's is weak in these areas, leaving it unclear what parents are consenting to. First, instead of an explicit consent provision, the notice cites multiple Utah statutes which must be looked up separately and are laborious to understand. Second, vague language describes the use of the data. Fore example, instead of saying the data is sent to a federal agency, or to the University of Utah for research and data sharing, statute is quoted with terms such as "medical research program."

In its 2013 privacy framework, the Organisation for Economic Co-operation and Development states, "If…overwhelmed by choices or complex information, individuals will tend to choose what is presented to them. Providing information that is understandable is a key component of transparency." We asked the CPO about the data collection and usage from the parent worksheet, and if its notice is sufficient according to data privacy standards. The CPO replied no, and it is not how he would write a form of this nature.

These concerns are compounded by OVRS's additional data-collection and data-sharing practices after new mothers are discharged from hospitals.

Facility Worksheet May Present Data Privacy Weaknesses by Obtaining Data After the Fact and Sharing It without Informed Consent

Data collection happens not only at the front end of a new birth, but also at the back end, after a new mother is discharged from the hospital. A "Facility Worksheet for Birth Registration" (facility worksheet), see Appendix D, is used to gather this data and neither the worksheet, nor the data collection is disclosed.



Facility Worksheet for Birth Registration

The items below were formerly on the Parent Worksheet for Birth Registration. They are required for birth registration but can no longer be gathered from the parent by Vital Records as we are required to ask only the questions on the Federal Mother's Worksheet for Child's Birth Certificate. This form follows the Federal Facility Worksheet form that has previously not been used in Utah but will now be required. This worksheet does not need to be returned to Vital Records. The information is required entry in UINTAH – the birth registration system.

1. Child Sex: ○ Male ○ Female ○ Undetermined (2)
2. Date of birth mm/dd/yyyy: _____ (3)
3. Time of birth (24 hr clock): _____ (4)
4. Child birth Weight: _____LBS _____OZ. (5)
6. Child birth Length (Inches): _____ (6)
7. Where was the baby born? (7)
   - ○ Hospital - Facility Name: _____
   - ○ Baby was born while traveling to hospital
   - ○ Freestanding birth center - Facility Name: _____
   - ○ Baby was born while traveling to birth center
   - ○ Clinic / Doctor's Office
   - ○ Home - intended
   - ○ Home - not intended
   - ○ Home - unknown if intended
   - ○ Other
   - ○ Unknown
8. Name of delivering birth professional or other birth attendant: _____ Title: _____ (10)
9. Was Parent 1 enrolled in Medicaid at time of birth? ○ Yes ○ No (50)
10. Primary Source of payment for this delivery: ○ Medicaid ○ Private Insurance ○ Self-Pay ○ Indian Health Service ○ CHAMPUS/TRICARE ○ Other Government (Fed, State, Local) ○ CHIP ○ Other ○ Unknown (check if Medicaid Pending) (52)
11. Parent 1 weight at Delivery: _____ Lbs. (56)
12. Is the infant being breast-fed at discharge? ○ Yes ○ No (61)
13. Was Parent 1 told by her healthcare provider that she had gestational diabetes during this pregnancy? (62) ○ Yes ○ No

UDOH-OVRS-105F April 2022 Page 1 of 2 Facility Birth Worksheet

Data

Further, the facility worksheet has additional questions regarding the personal health of mothers and babies that are not included in the parent worksheet. For example, it asks when the mother's last menstrual cycle occurred. To obtain the data, it was explained that birth clerks fill out the required information with existing medical records. Our consultant raised concerns about these data-collection and data-sharing processes and believes greater attention to consent provisions will enhance data privacy practices in this area. We recommend the Legislature consider policies regarding these practices.

RECOMMENDATION 2.1

We recommend the Legislature consider clarifying the collection of birth registration data. One clarifying option is to separate essential birth registration information from research questions with two separate forms.

RECOMMENDATION 2.2

We recommend the Legislature consider the merits of requiring government entities adopt data privacy principles that include items such as: clear consent, notice, and the disclosure of data collection, use, and sharing.

2.2 Data Distribution after Collection Is Not Disclosed in a Transparent Way, Raises Data Privacy Red Flags

Our data privacy consultant believes third-party risk is an issue that rises to the top levels of an organization. Senior leadership should regularly provide oversight, governance, and auditing. Testing of third-party risk management and rigorous due diligence, contracting, monitoring, enforcement, and off-boarding processes should be in place. Our consultant report fails OVRS in these areas.

A question we asked in our audit work was why OVRS is collecting so much data, beyond what is needed to register a birth and create a birth certificate.

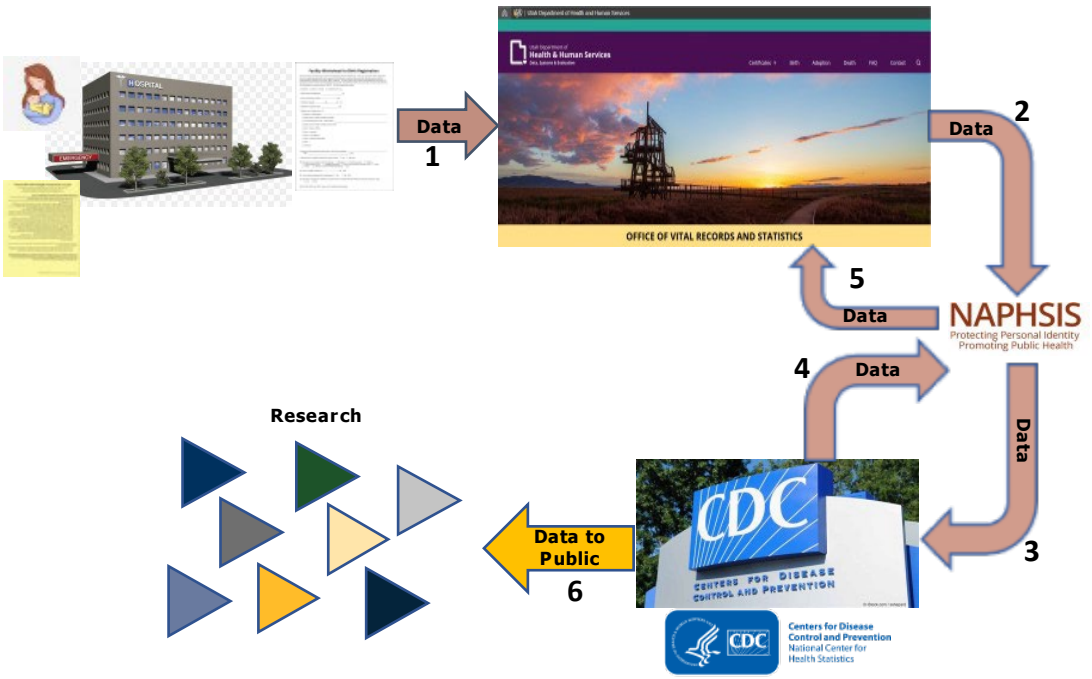
Three main factors contribute to the current data-collection practices: (1) OVRS has a federal contract with the Centers for Disease Control and Prevention (CDC), managed through the NCHS; (2) OVRS has DSAs with other state agencies and external entities that agree to data collection for research and administrative purposes; and (3) statute allows for the data gathering, in some cases requiring it.

OVRS should review how it can be more transparent in disclosing these contracts and DSAs. The Legislature should also consider requiring disclosures that are more transparent.

Contract with CDC Requires Multiple Data Elements from OVRS, but the Contract Is Negotiable

Understanding the contract OVRS has signed with the NCHS is crucial to understanding OVRS's collection of birth information. Since the facility worksheet is not disclosed to new mothers, not only are new mothers' data collected without their knowledge or consent, but the data is obligated contractually by OVRS without their knowledge and consent as well.

Additionally, in our review of statute there are opportunities to clarify code sections relating to how PHI is collected and shared. It appears that the Legislature can provide clarity in data-collection policies by addressing this discrepancy as well if it deems it necessary.



Data flow map of PII and PHI of new mothers: (1) Data is collected through the parent and facility worksheets and uploaded by hospitals to OVRS; (2) OVRS uploads Utah birth records two times per week into the National Association of Public Health Statistics and Information Systems (NAPHSIS) database. (3) NCHS accesses the data from NAPHSIS and participates in coding it to allow for analysis at the national level; (4) coded data are returned to NAPHSIS, and (5) coded data are then sent to OVRS. The data are also made publicly available by NCHS after being deidentified.

In summary, a contract with NCHS obligates the collection of new mothers' PHI, beyond birth certificate data elements needed. Because of this contract, OVRS is required to collect the PHI data and submit it to NCHS.

The Legislature Can Weigh in Policy-Wise on the VSCP Contract. The contract between OVRS and NCHS is referred to as the Vital Statistics Cooperative Program (VSCP). The latest version of the VSCP contract was signed in February 2022 and the contract is amended every five years. All states, territories, New York City, and Washington, DC have similar contracts, which obligate them to gather medical data about parents and newborns and share the data with the CDC. No jurisdiction currently opts out of the contract.

Furthermore, OVRS is compensated monthly for the data it provides. This revenue represents an estimated 25 percent of the OVRS budget. The contract exceeds $3 million for the five-year period. If 80 to 85 percent of the data required by the contract is not collected and sent to NCHS, OVRS can lose funds.

As we researched the VSCP contract, both NCHS and OVRS expressed that the contract is voluntary, and its terms can be changed. (There are fifty-eight data points currently required, as shown in Appendix E. These data points are then used for public health research at the federal level.) The current contract which runs through May 2027, establishes that the state retains ownership of the data. Instead of a binding federal law or regulation, the method NCHS uses to obtain the data it needs is through purchasing the data via the VSCP contract.

OVRS Aids External Entities with Marketing and Research

Although the current practice at OVRS is legal and within statutory boundaries, its activities on behalf of certain external entities raise data privacy concerns. Our consultant flagged these activities because they are carried out without informed consent from new mothers. That said, our audit found no evidence to suggest that OVRS is selling PII to third parties.

OVRS management described situations with two different entities that have approached the office to obtain vital records data to either market services to new mothers or solicit them to participate in research. One example is the my529 educational savings plan, which is a quasi-governmental agency as defined in ***UCA*** 53B-8a-103. Currently, new parents receive a mail advertisement from my529 that markets its investment products several months after the birth of their baby. OVRS explained that my529 desired vital records data so it could carry out these marketing activities, but that mailing information is not given to my529. Instead, my529 provides its brochure, OVRS provides the mailing label, and both are sent to State Mail to be processed for mailing. A similar procedure is in place with Brigham Young University to solicit research participants. However, we recommend the Legislature consider whether policy should be created to require informed consent provisions for these data processing activities.

Collection and Transmission of PII Are Written into Statute without Consideration of Data Privacy

It is a statutory requirement to register and certify a new birth within ten days of the birth. If the new mother is not married at the time of the birth, a voluntary declaration of paternity form is required to be filled out with the "declarant" father's information. In conjunction with these requirements, ***UCA 26B-8-105*** requires the collection of social security numbers of parents for each live birth in the state. It requires the state registrar to transfer this PII to the Office of Recovery Services (ORS) "as soon as practicable."

In speaking with OVRS management, establishing paternity is one task ORS is required to do to obtain federal funding. Since OVRS has the statutory duty to collect the information ORS needs, and has the data, both divisions have a DSA to provide ORS access to OVRS data systems for a fee.

Data privacy concerns arise with the collection of PII and OVRS's DSA to provide access to another agency without consent or disclosure of the intended use of that data, and this practice is written into statute.

This arrangement demonstrates how data sharing can improve the efficiency of state agencies in their administration of government programs. However, it is also an example of the imbalance of reaping the benefits of data, at the expense of data privacy. With a data privacy act and a more integrated data privacy program for state agencies, situations such as these can receive greater attention and balance can be obtained.

RECOMMENDATION 2.3

We recommend the Legislature consider Office of Vital Records and Statistics data collection and processing practices and whether to establish data privacy policy for state agencies in Utah.

Complete List of Audit Recommendations

Complete List of Audit Recommendations

This report made the following seven recommendations. The numbering convention assigned to each recommendation consists of its chapter followed by a period and recommendation number within that chapter.

Recommendation 1.1

We recommend the Legislature consider whether statutory guardrails are needed to balance the benefits of data with data privacy practices in state agencies.

Recommendation 1.2

We recommend that the Legislature consider the merits of passing a data privacy act into statute to provide state agencies with a data privacy governance structure and to incorporate principles of data privacy into their practices for data processing and sharing.

Recommendation 1.3

We recommend that the Legislature consider defining data privacy in statute for all state agencies.

Recommendation 2.1

We recommend the Legislature consider clarifying the collection of birth registration data. One clarifying option is to separate essential birth registration information from research questions by creating two separate forms.

Recommendation 2.2

We recommend the Legislature consider the merits of requiring government entities to adopt data privacy principles that include items such as: clear consent, notice, and the disclosure of data collection, use, and sharing.

Recommendation 2.3

We recommend the Legislature consider Office of Vital Records and Statistics data collection and processing practices and whether to establish data privacy policy for state agencies in Utah.

Appendix/Appendices

A. Data Privacy Principles

The Organization for Economic Co-operation and Development (OECD), which the United States participates in, developed and promulgated privacy guidelines in 1980. A reason cited for these guidelines was the onset and proliferation of computer technology, how it enhances data processing capabilities, and the raised level of data privacy risk – or the increased threat to privacy – resulting from it.

In 2013, the OECD revised and updated its privacy guidelines in a report titled, The OECD Privacy Framework. The framework provides a comprehensive analysis of the challenges to individual rights of privacy with exponential increases in data processing. It does this while striking a balance with the benefits of data to society and the public good derived from it. It also outlines the OECD's eight data privacy principles that act as guidelines for private and public entities as they process personal data.

OECD Data Privacy Principles

Collection Limitation	There should be **limits to the collection** of personal data and any such data should be **obtained by lawful** and **fair means** and, where appropriate, with the **knowledge or consent** of the data subject.
Data Quality	Personal data **should be relevant** to the purposes for which they are to be used, and to the extent necessary for those purposes, **should be accurate, complete and kept up-to-date.**
Purpose Specification	The **purposes for collection** of personal data should be **specified at the time of** data **collection** and the **subsequent use limited to** the fulfilment of **those purposes or** such **others as are not incompatible with those purposes** and as are **specified on each occasion of change of purpose.**
Use Limitation	**Personal data should not be** disclosed, made available or otherwise **used beyond collection purposes except**: (a) with the **consent** of the data subject; or (b) by the **authority of law.**
Security Safeguards	**Personal data should be protected by reasonable security safeguards against** such risks as **loss or unauthorized access, destruction, use, modification or disclosure of data.**
Openness	There should be a general **policy of openness** about developments, practices and policies **with respect to personal data. Means should be readily available** of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and residence of the data controller.
Individual Participation	**Individuals should have the right:** (a) **to obtain confirmation** of processed data relating to them; (b) **to receive communication** of data relating to them: (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form this readily intelligible to them; (c) **to be given reasons if a request** for data **is denied**, and **be able to challenge** such denial; and (d) **to challenge data relating to them** and, **if the challenge is successful** to **have the data erased, rectified, completed, or amended.**
Accountability	A **data controller should be accountable for complying** with measures which give effect to the principles stated above.

Utah's Government Operations Privacy Officer has created a proposed Privacy Plan for the state which includes a set of privacy principles, as well.

Proposed Privacy Principles for Executive Branch Agencies by Government Operations Privacy Officer*

1. Individual Participation
2. Lawful, fair, and Responsible Use
3. Data Minimization
4. Transparency and Accountability
5. Security
6. Due Diligence

*As of January 2023

B. Inspire! Privacy and Security Full Report

CY23 Utah Office of Vital Records and Statistics Audit Report

Prepared for:

The Utah Office of Legislative Audit ("OLAG")

May 2023

CONTACT INFORMATION

Inspire! Privacy and Security LLC • 536 North 500 East, Nephi, Utah USA 84648 • 801-512-4445 • ask@inspireprivacyandsecurity.com

TABLE OF CONTENTS

[Table of Contents]

SCOPE OF WORK

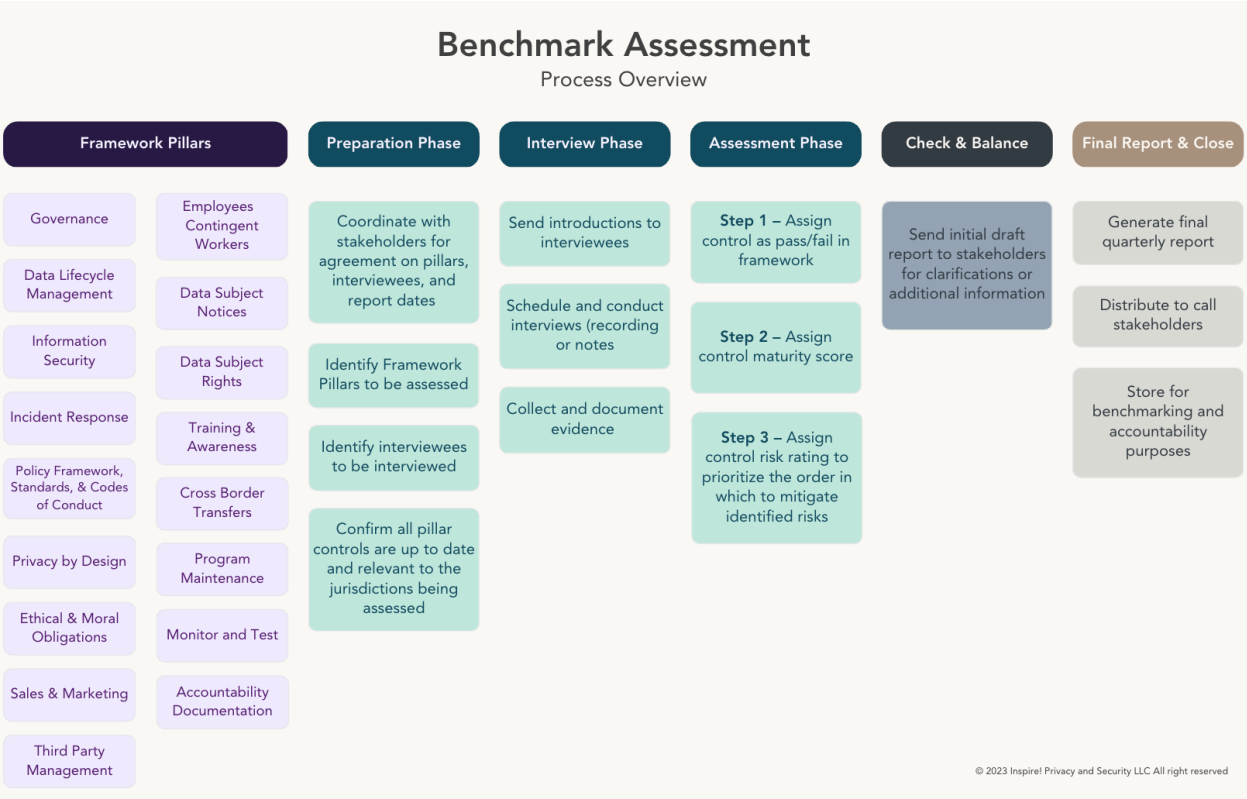
Inspire! Privacy and Security, LLC has been asked to test OVRS's compliance with applicable privacy and data protection laws, regulations, and other requirements, assess the risks associated with any identified gaps, then provide advice about how to mitigate the risks by working toward compliance. A global standard has been used which has been measured against current global privacy and data protection laws, regulations, and industry standards. The Inspire! global privacy and data protection framework used has been provided to OLAG for the purpose of continuing their work to make recommendations to OVRS to improve the maturity level of their current privacy program, and to comply with applicable privacy and data protection laws. The Inspire! team has completed its CY23 Audit and is now providing this final report.

This report contains, (1) an overall maturity score for each area of focus, based on (2) findings regarding the controls used to conduct the assessment, (3) risks associated with continued non-compliance, and (4) recommended next steps designed to improve the maturity score and lower the organization's risk profile. Please note: The recommendations made in this report focus on (1) prioritizing high risk gaps (2) improving the overall maturity level, and (3) limited budget, time, and resources.

[Table of Contents]

PROCESS OVERVIEW

The following diagram illustrates the general process that was used for this audit. Key individuals were interviewed by asking questions associated with each of the categories listed below and the associated predetermined global privacy program framework controls. Notes were captured and reviewed and approved by the individuals who were interviewed. Evidence was provided in support of statements made as needed and are stored by OLAG. A determination was made for each control to assign a maturity ranking and the risk to the data subject which resulted in this final report.



Assessment Phase

Step 1 - Control Initial Assessment

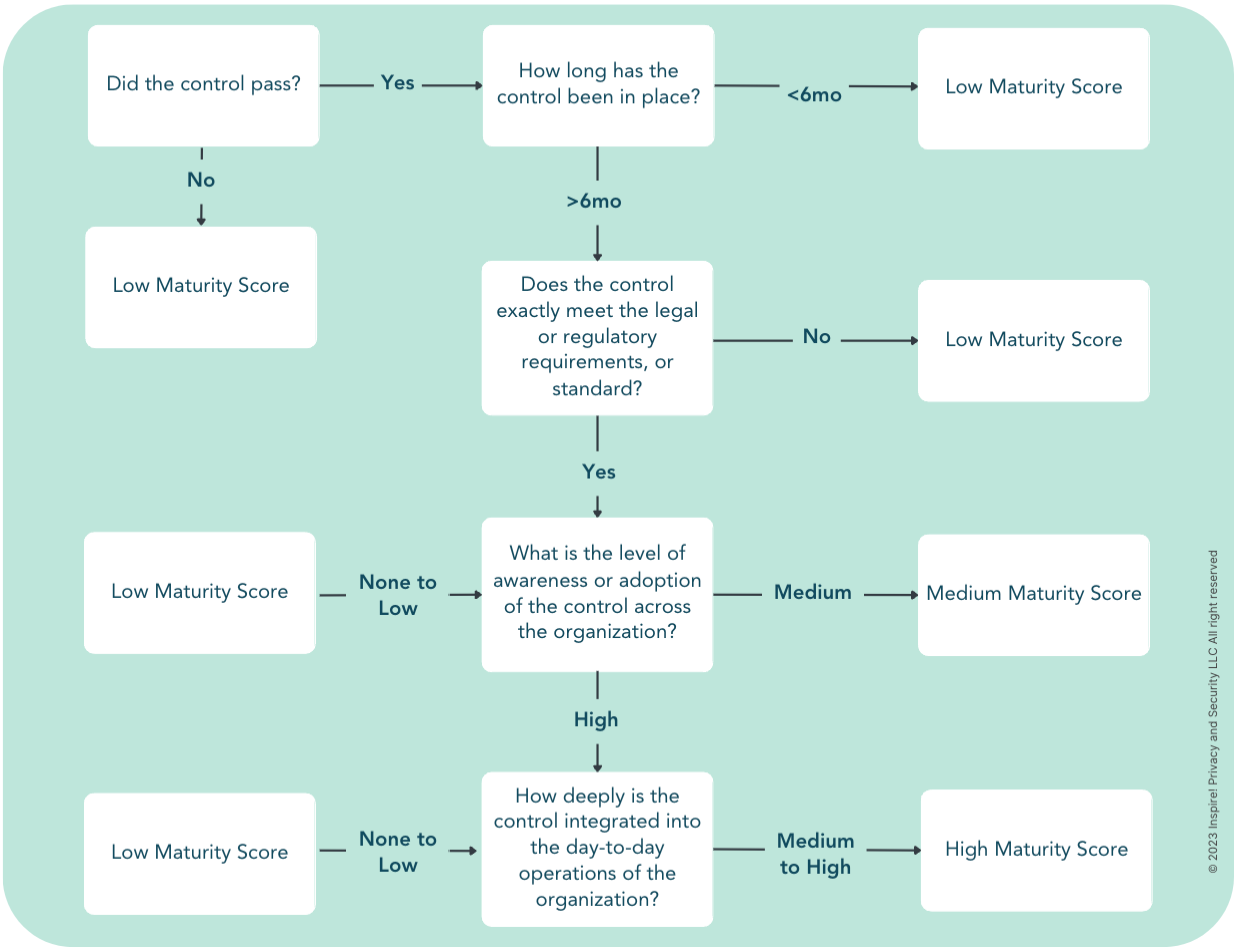
Once the Framework Pillars are agreed upon, and the Preparation and Interview Phases are complete, the Assessment Phase is completed by deciding whether each control is “passed” or “failed” and assigning a “maturity ranking.”

Step 2 - Maturity Ranking (Low, Medium, High)

The following diagram illustrates the decision tree used in this second step of the Assessment Phase for determining the maturity ranking of each control. For example, for the first control in the Governance Pillar if an individual has been assigned with responsibility for privacy at the executive level the control is marked

"passed." However, if very few people in the organization understand there is a "privacy officer," the maturity rating for this control is medium to low based on the process described in the following table:

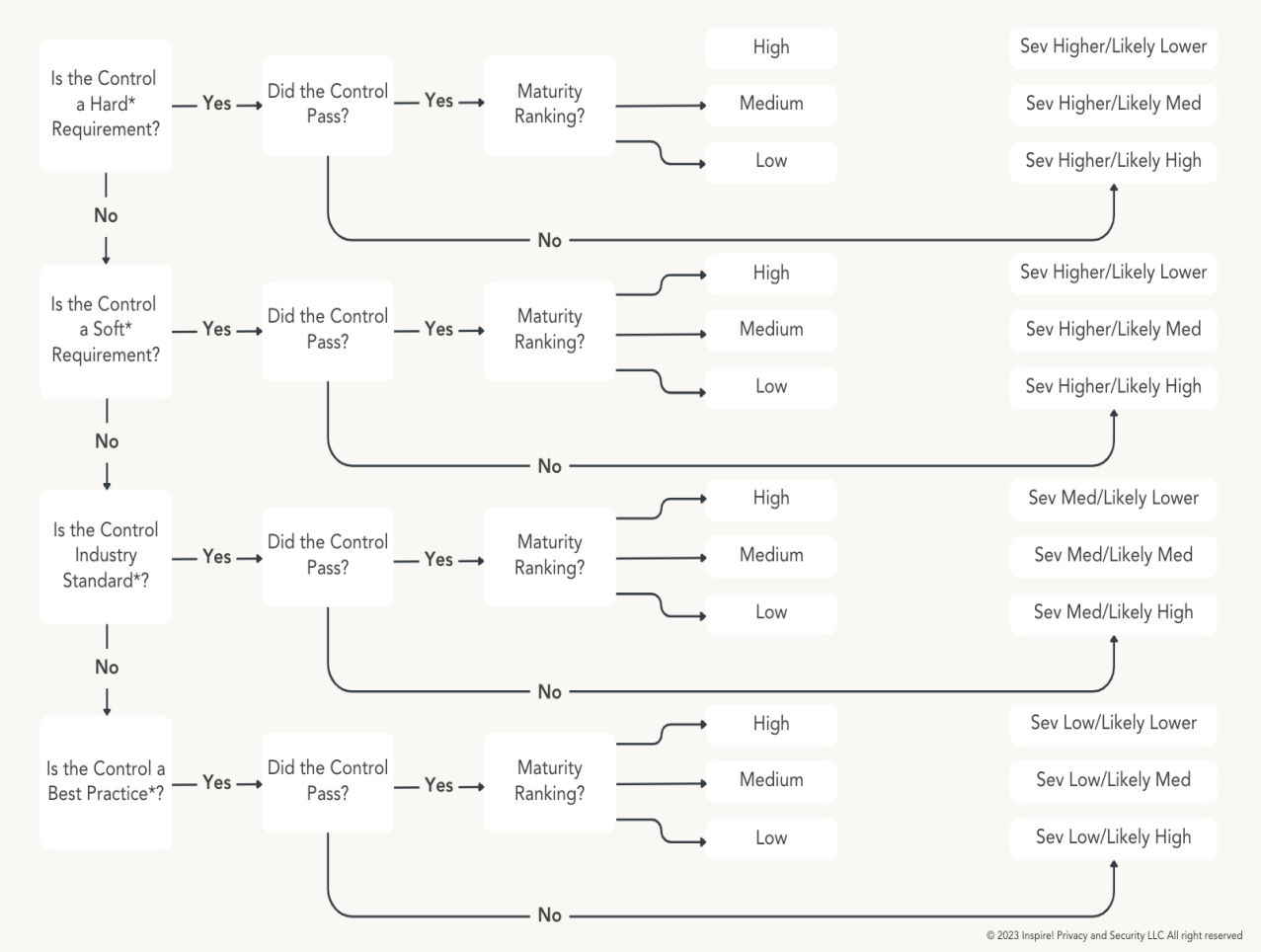
Maturity Ranking Formula



Step 3 - Risk Assessment

The third step in the Assessment Phase requires an assessment regarding the level of risk introduced to the individual data subject by the processing described in each control. Whether a control has "passed" and then its maturity ranking will be foundational for the analysis regarding the likelihood and severity of risk associated with each control. Controls are also assigned a status as "hard," "soft" or "best practice." Whether a control is a hard or soft requirement, or a best practice is determined by the laws, regulations or standards associated with the control and the jurisdictions impacted by the control. This assessment formula is described in the following table:

Risk Assessment Formula



*Hard Requirement = Statutory Requirement, Soft Requirement = Regulatory Requirement, Industry Standard = aligns with specific standard (eg. ISO, NIST, SOC2), and Best Practice is control regulators have come to expect and will be requested during a regulatory inquiry or investigation

Risk Rating Score

Once the risk assessment formula is applied to each control, a risk rating score is assigned to each control based on the following table:

Together these four tables, outline the process that was followed for this audit, which is designed to recommend a structured, well-supported, incremental approach to lowering risk and improving the maturity of your global privacy and data protection program, and then in each subsequent year benchmarking and showing tangible, measurable progress, which will in and of itself lower the risk profile of the organization.

[Table of Contents]

EXECUTIVE SUMMARY (TL; DR)

OVRS has an overall low maturity level ranking for its agency-specific privacy program/practices. This ranking is a result of work that needs to be accomplished to comply with hard, statutory requirements in some significantly high-risk areas such as the collection and sharing of non-required (secondary purpose) birth registration data without consent of the individual data subject.

More specifically, OVRS has a low maturity level ranking in the areas of Data Governance, Legal Basis/Authority, Policy Framework, Standards and Codes of Conduct, Third-Party Risk Management for affiliated and unaffiliated third-parties, Data Subject Rights, and Program Maintenance.

In addition, OVRS current privacy program/practices introduce substantial, if not catastrophic risk that is very likely to result in risks to the rights and freedoms (which is very likely in some cases to result in actual harm) of individual data subjects.

[Table of Contents]

AUDIT SCORES AND RISK RATINGS

Global Privacy and Data Protection Program Category	# of Applicable Hard Requirements (Total/Passed)	# of Applicable Soft Requirements (Total/Passed)	# of Applicable Industry Standard/Best Practices (Total/Passed)	Overall Risk Rating Score (1-5) *
Data Governance	7/0	1/0	3/0	5 (Very Likely/Substantial)
Legal Basis	16/0	0/0	0/0	5 (Very Likely/Substantial)
Policy Framework, Standards and Codes of Conduct	2/0	0/0	3/3	4 (Very Likely/Light)
Third-Party Risk Management (Affiliated and Unaffiliated)	16/0	0/0	3/0	5 (Very Likely/Substantial)
Data Subject Rights	4/0	0/0	9/0	4 (Possible/Substantial)
Program Maintenance	0/0	0/0	0/0	3 (Possible/Moderate)

*Please see the Inspire! Privacy Program Framework stored by OLAG for details.

[Table of Contents]

HIGH PRIORITY FINDINGS AND RECOMMENDATIONS

DATA GOVERNANCE

Data governance is an organizational measure that is recognized as an industry wide as a best practice from a compliance perspective. Several aspects are increasingly required by law and regulation. Regulators expect to see a data governance and oversight focus in compliant organizations, and industry standards require evidence of a solid data governance and oversight program. An ideal governance and oversight plan

has a privacy officer, security officer and a support structure such as a data governance committee with strategic and tactical policies and oversight responsibilities. Evidence of governance and oversight is focused on development and maintenance of privacy and data protection organizational measures that have been operationalized and enforced. An ideal privacy and data protection governance program includes one or more assigned privacy and data protection roles known as a network of "privacy champs" supporting the privacy and security officers and data governance committee.

In the state of Utah, The Government Records Access and Management Act ("GRAMA") is the closest thing to a privacy law for public sector agencies associated with Data Governance. For example, GRAMA specifically requires each agency to appoint a Records Officer responsible for compliance with GRAMA, including annual certification of compliance, coordination with the State Records Committee and other records division such as the State Archives, etc. Records are the physical medium relied on by agencies to fulfill their mandate. Each record (whether hard-copy or electronic) contains data, which in turn, often contains personal information. And while GRAMA is not specifically a privacy law, the law has substantial privacy implications and impacts how personal information is processed from a Data Governance and Data Lifecycle perspective, including collection, access and sharing.

Finding #1 – The Office Vital Statistics and Records has not appointed a Records Officer as required by GRAMA.

RECOMMENDATION

Appoint an OVRS Records Officer.

Finding #2 – OVRS has not classified its records as required by GRAMA, which in turn will identify those documents that can be shared, are subject to other state and federal laws and regulations and determine whether and when to engage other stakeholders such as oversight committees.

RECOMMENDATION

Classify all OVRS Records.

Finding #3 – Sharing of OVRS Records is subject to audit and oversight by other stakeholders within the government hierarchy as outlined by GRAMA.

RECOMMENDATION

Work with the CPO and the PPOC to develop a mature and compliant sharing policy and process that is fully operationalized.

[Table of Contents]

LEGAL BASIS

The processing of personal information either requires the participation of the individual the data identifies (data subject), or some lawful and fair basis for the processing. Your agency can rely on several different legal bases for your processing. They are (i) consent, (ii) contractual necessity, (iii) legal obligation, (iv) vital interest, (v) public interest, or (vi) legitimate interest, or (vii) some other statutory legal authorization.

The requirements associated with each legal basis will vary based on the jurisdiction, your role, the category or type of data, and other factors. Each legal basis will also have associated restrictions and characteristics. For example, the type of consent that can be relied on (whether express or explicit) will vary based on whether the data is personal information or sensitive personal information. Consent must be clear and conspicuous, as well as specific to each type of processing, and it must be as easy to withdraw consent as it was to give it.

Another good example is the legal basis of Legitimate Interest. Historically, Legitimate Interest has been used by organizations as a "catch-all" when no other type of legal basis is possible, or to authorize processing that may or may not have been authorized by the data subject. Today Legitimate Interest can only be relied upon by an organization when the interests of the organization outweigh the risks to the rights and freedoms the processing introduces to the data subject, and on balance the analysis is skewed in favor of the data subject. The data subject must also be given the right to restrict or object to the processing. In other words, it is very hard to meet the bar for a valid legal basis to process personal information based on an organization's Legitimate Interest, and it is becoming increasingly difficult due to updated regulations and guidelines as well as specific, newer sectoral laws.

In summary your agency must conduct a legal analysis, and document that analysis for accountability purposes, regarding the legal basis for your processing associated with each category of data and each purpose for its use. The source of the data, how it was collected, who it is transferred to, and other factors must be considered. This will form the basis for compliant notice to data subjects and the basis for your compliance efforts.

Finding #1 – OVRS has not provided a legal analysis for the legal authority for its processing activities and there is no notice to data subjects regarding its legal authority to collect, use and share personal information with other agencies.

RECOMMENDATION

Work with the Legislature and Attorney General's Office to identify (based on legal analysis) the legal authority for processing of each data element and the purpose for which the data can be used including sharing with other agencies.

Finding #2 – In order to share OVRS data with other agencies for a myriad of purposes each transfer of personal information requires legal authority for the transfer. Given the number of requests for OVRS Data a state-wide Privacy Act governing public sector use of personal information is recommended.

RECOMMENDATION

OVRS should work with the legislature, the Chief Privacy Officer and the Utah Privacy Protection and Oversight Committee to develop laws, regulations, and other requirements to legally process the non-required personal information in the form of a public sector Privacy Act.

Finding #3 – OVRS has specific statutes such as the Utah Vital Statistics Act as the legal authority to process very specific data elements of personal information for very specific purposes if certain policies and procedures are followed. OVRS is processing data that is not required by the Vital Statistics Act (or other laws) so its legal authority to process this non-required personal information is in question. Based on the legal analysis recommended above, specific legal authority must be established for the processing of non-required personal information.

RECOMMENDATION

OVRS should work with the legislature, the Chief Privacy Officer and the Utah Privacy Protection and Oversight Committee to update existing, associated laws, regulations, policies, processes, and notices, etc..

[Table of Contents]

POLICY FRAMEWORK, STANDARDS AND CODES OF CONDUCT

A policy framework is the most effective tool for the critical development, implementation, refreshing, monitoring, testing, enforcing, retiring of policies and processes, and communicating with impacted individuals in a seamless manner with minimum impact to the organization's ways of working.

Development and maintenance of a policy framework that reflects the way your organization works will provide a valuable tool for managing your data privacy and information security programs. The framework will also play a critical role in verifying and demonstrating compliance with applicable laws and regulations to meet your accountability obligations in an elegant way.

A solid global policy framework focused on privacy and data protection is the tool that will create a vision for experienced or novice privacy professionals or others simply trying to comply with privacy and security program policies designed to comply with applicable laws and regulations. It is also the breadcrumbs regulators will follow as they conduct an inquiry or investigation, and it will be the backbone for your efforts to certify to an external standard and provide a solid foundation for the organization's obligations associated with accountability. By conducting research, assessing available resources, and developing a plan for your policy framework that addresses each aspect associated with your global privacy program this practice will help ensure your program's success.

While OVRS is not required to have a policy framework, or comply with any standards or codes of conduct, this is the most efficient and effective way to comply with policy requirements associated with the processing of personal information. More particularly, the processing by OVRS of non-required Health Data from hospital workers to collect birth registration data is subject to HIPAA and other Health Data laws with privacy and data protection laws and employee training, acknowledgement, acceptance, and enforcement is required. A process is necessary to comply with these types of requirements.

Finding #1 – OVRS was unable to provide evidence of a privacy policy or process documents specific to privacy requirements the agency is subject to.

RECOMMENDATION

Work with the Legislature, Attorney General's Office, the CPO and/or the PPOC to develop a legally compliant privacy policy and process documents associated with the processing of personal information.

Finding #2 – OVRS was unable to provide evidence of a employee and contingent worker training specific to the agency's processing of personal information, including sensitive personal information which also includes Health Data.

RECOMMENDATION

Work with the Legislature, Attorney General's Office, the CPO and/or the PPOC to develop a legally compliant employee privacy training, acknowledgements, and agreements to comply with OVRS policies and processes, including enforcement that is specific to the processing of OVRS data.

Finding #3 - While OVRS is not required to have a policy framework, or comply with any standards or codes of conduct, this is the most efficient and effective way to comply with policy requirements associated with the processing of personal information.

RECOMMENDATION

Work with the Legislature, Attorney General's Office, the CPO and/or the PPOC to develop a legally compliant OVRS Policy Framework.

[Table of Contents]

THIRD-PARTY RISK MANAGEMENT (AFFILIATED AND UNAFFILIATED)

Third-party risk management requires organizations that rely on third parties to assist with the processing of personal information to put a formal process in place to manage associated risks and to assume the associated liabilities, including due diligence, contracts, maintenance, auditing, and enforcement. This applies to third parties that use the personal information they receive from the organization for their own benefit (otherwise known as a "sale"), or for any reason beyond support of the organization to provide a product or service as a service provider.

A compliant risk management process requires policies, resources, budget, and a formal process as follows:

Finding #1 – The processing of managing data sharing with third parties is complicated and will vary based on the types of third parties the agency is sharing personal information with. This requires a formal, fully developed, funded, resources and well-researched process, that is constantly monitored and refined. OVRS does not have this type of a process, which is required to fully comply with the sharing requirements of its enabling statutes and other laws like GRAMA or HIPAA or other Health Data laws.

RECOMMENDATION

Work with the Legislature, Attorney General's Office, the CPO and/or the PPOC to develop a legally compliant privacy policy and process documents associated with the processing of personal information by both affiliated and non-affiliated third parties, including other agencies, vendors, and IT support.

Finding #2 – The processing of managing data sharing with third parties is complicated and will vary based on the types of third parties the agency is sharing personal information with. This requires a formal, fully developed, funded, resources and well-researched process, that is constantly monitored and refined. OVRS does not have this type of a process, which is required to fully comply with the sharing requirements of its enabling statutes and other laws like GRAMA or HIPAA or other Health Data laws. This includes requirements for contracts and other associated documentation.

RECOMMENDATION

Work with the Legislature, Attorney General's Office, the CPO and/or the PPOC to develop a legally compliant data sharing agreement templates, including a maintenance process.

Finding #3 - The processing of managing data sharing with third parties is complicated and will vary based on the types of third parties the agency is sharing personal information with. This requires a formal, fully developed, funded, resources and well-researched process, that is constantly monitored and refined. OVRS does not have this type of a process, which is required to fully comply with the sharing requirements of its enabling statutes and other laws like GRAMA or HIPAA or other Health Data laws. This includes transfer/sharing technical measures, operational measure, as well as procedural measures.

RECOMMENDATION

Work with the Legislature, Attorney General's Office, the CPO and/or the PPOC to develop a legally compliant data sharing policies and processes that are fully operationalized.

[Table of Contents]

DATA SUBJECT RIGHTS

Data subjects around the world have many statutory rights which may vary by country or region, or even by sector. These rights include the right to: (1) notice and information about their own personal information, (2) access to their own personal information, (3) rectification or accuracy, (4) erasure and to be forgotten, (5) restriction or objection, (6) no profiling or automated decision-making, (7) data portability, and (8) no marketing. Except for the right not to be marketed to, these rights are not absolute and must be balanced with other rights and obligations, such as your organization's obligation to keep data in the event of a legal obligation. These requests must also be verified before acting. These rights may also include the right to withdraw consent if your organization has relied on consent as a legal basis for processing personal information. As a result, organizations are required by law to design, implement, maintain, monitor, and test, and maintain accountability documented associated with a formal process for your agency's policies and processes for data subjects' rights.

Finding #1 – As a public sector agency, OVRS is responsible for complying with Fair Information Privacy Practices as required under the Federal Privacy Act (which OVRS is required to comply with in the context of transfers to CDC), HIPAA also requires specific data subject's rights as well as other Health Data laws. As a result, OVRS is required to have policies and processes associated with data subject rights.

RECOMMENDATION

Work with the Legislature and Attorney General's Office to identify all relevant legislative statutory, regulatory, contractual requirements and develop policies and processes to provide the data subjects rights explicitly identified each OVRS information system at the data element level.

Finding #2 – As a public sector agency, OVRS is responsible for complying with Fair Information Privacy Practices as required under the Federal Privacy Act (which OVRS is required to comply with in the context of transfers to CDC), HIPAA also requires specific data subject's rights as well as other Health Data laws. As a result, OVRS is required to have policies and processes associated with data subject rights. This includes ensuring the requestor is the authorized data subject.

RECOMMENDATION

Develop and maintain procedures to verify identity of requestor or complainant (Verified Consumer Request (VCR) and an appeals process.

Finding #3 - As a public sector agency, OVRS is responsible for complying with Fair Information Privacy Practices as required under the Federal Privacy Act (which OVRS is required to comply with in the context of transfers to CDC), HIPAA also requires specific data subject's rights as well as other Health Data laws. As a result, OVRS is required to have policies and processes associated with data subject rights. This includes demonstrating compliance of the formal the OVRS data subject's rights policies and processes.

RECOMMENDATION

Develop and maintain a tracking system to demonstrate compliance.

[Table of Contents]

PROGRAM MAINTENANCE

The requirement to implement and maintain global privacy and data protection is implied and expressed. It is implied because the only way to ensure current and future compliance is to identify on-going privacy compliance requirements, become integrated into the relevant privacy and data protection communities and trade organizations, track updated, new and upcoming laws and regulations, seek legal opinions regarding relevant application of privacy and data protection laws, including its intersection with information security laws and regulations and document decisions associated with the interpretation and application of relevant privacy and data protection laws. These activities are also expressly required in several major omnibus laws globally.

Finding #1 – OVRS has narrow requirement to develop and maintain certain aspects of a privacy program. For example, GRAMA requires a program to comply, HIPAA and other Health Data laws require a program, and the list goes on, and other applicable federal laws and Fair Information Privacy Practices require OVRS to develop and maintain a privacy program.

RECOMMENDATION

Work with the Legislature, Attorney General's Office, the CPO and/or the PPOC to develop and maintain an agency-wide privacy program that is operationalized and maintained as the primary vehicle to demonstrate compliance with all requirements identified in this audit.

C. "New Parent Worksheet"

Parent's Worksheet to Register Birth Information

The information you provide on this worksheet will be used to register your child's birth.
Once registered you can order a copy of your child's birth certificate.
You can also apply for a Social Security card for your child on this worksheet.

How information from the Parent's Worksheet is used

The birth certificate is a legal document used to prove your child's age, citizenship, and parentage throughout their life.

- ***It is important that you provide readable, complete, and accurate information.***
- *Items marked "REQUIRED" are required by law [UCA § 26-2-4(1), UCA § 26-2-22(4), UCA § 78B-15-101 et seq., Utah Uniform Parentage Act].*
- *UCA § 26-2-4(2) mandates the Office of Vital Records to require "as a minimum the data recommended by the federal agency responsible for national vital statistics". This includes both items from this worksheet and information from the birthing center (as defined in UCA §26-21-2(6)) pursuant to UCA §26-2-5(3) & (4). To see items recommended for the standard birth certificate and for data in the birth record see https://www.cdc.gov/nchs/nvss/revisions-of-the-us-standard-certificates-and-reports.htm.*
- *Utah law requires births to be registered with the State Registrar within 10 days (UCA §26-21-5(2)). The law allows for registration within the first year but the State Registrar may require additional evidence in support of the facts of birth and an explanation of why the birth was not registered within the required ten days. After one year evidence of the facts of birth is required and the birth certificate is marked "Delayed".*
- State laws regulate the release of identifying information from any vital record including this birth registration worksheet to ensure the confidentiality of the parents and their child (UCA §26-2-22). This law states that birth information may be released to persons with a direct, tangible, and legitimate interest as defined in the law which includes (1) the subject of the record, an immediate family member, the guardian, the legal representative, or a child placing agency; (2) the request involves a personal property right of the subject of the record, (3) the request is for the official purpose of a public health authority or a state, local, or federal government agency, (4) the request is for a drug use intervention or suicide prevention effort or a statistical or medical research program, (5) the request is a certified copy of an order of a court. For additional information see UCA §26-2-22.
- Information shared under the law is the least necessary to meet the needs of the recipient and will not include identifying information unless absolutely necessary to fulfill the need.
- Information obtained for birth registration in accordance with the law is retained indefinitely.
- Failure to provide the some of the required data elements, may result in a birth certificate that does not meet the requirements for RealID and could result in the subject of the record being denied a drivers license, passport, or enrollment in school.

In addition to legal information, there is "OPTIONAL" information requested on the parent worksheet. This information will not appear on the birth certificate.

- *Some of the items marked "OPTIONAL" are used to better process your child's birth registration. If the information does not pertain, you may leave it blank. Some of the items marked "OPTIONAL" are requested for use by public health and medical researchers to study and improve the health of mothers and newborn infants.*

Items marked "OPTIONAL" are not required. By filling out optional information, you are giving your permission for that information to be used as allowed by UCA §26-2-22. If you do not want your information used, please leave that item blank. Optional information will be de-identified before 6 years or you can request the optional information be de-identified sooner by contacting the State Office of Vital Records and Statistics.

THIS WORKSHEET IS NOT AN APPLICATION FOR A BIRTH CERTIFICATE

How do I get a certified copy of a Birth Certificate?

- If you provide your email address on this worksheet you will receive an email when your child's birth has been registered.
- Once the birth is registered, you can order the certificate online at **silver.health.utah.gov** and pay the fee.
- The footprint card or registration form you receive from the hospital or midwife is not an official birth certificate.

Correcting mistakes, adding, or changing information on the birth certificate

Please make sure your information is registered correctly the first time by filling out the required items on this worksheet clearly and completely.

- Non-standard English characters and diacritical marks are not accepted by the Social Security Administration. Because of this diacritical marks may not show up on your child's social security card. This is not an issue that Vital Records can fix.
- Utah allows ISO basic Latin alphabet. A special process is required to include accents, tildes, graves, umlauts, and cedillas in your child's name. Ask your birth clerk or midwife for more information.
- Ask for a copy of the information that has been entered into the birth registration system so that you can check for accuracy.
- If you find mistakes, have them corrected before you leave the location where you gave birth.
- Changes to the information after registration can be done by filing an amendment with the Office of Vital Records and Statistics.
- Changes made to the birth certificate after registration will show as amendments to the original record, so it is important to be sure the information is accurate before it is registered with the State Registrar by the hospital or midwife.

How do I get my child's Social Security Card?

- To order a Social Security Card for your child, be sure to check "Yes" on item #3 and sign the worksheet.
- The card will be mailed in 2-3 weeks to the address listed as the mailing address in #16.
- *List the names of ALL persons who live at the address on or in the mailbox for the SSA card to be delivered.*
- A Social Security Card cannot be mailed to "general delivery" or out of the country.

If you do not receive the card, apply for a replacement from the Social Security Administration at SSA.gov or call 1-866-851-5275.

Name of Parent giving birth: _____ Room Number: _____

PLEASE PRINT CLEARLY

Please leave this worksheet with the birth clerk, midwife, or other birth center personnel for birth registration.
Please fill in circles completely. ● Items not marked OPTIONAL are required.
Parent 1 gave birth to the child. Parent 2 did not give birth to the child.
(Numbers at the ends of the lines are for data entry use.)

1. REQUIRED
What will be your baby's legal name (as you wish it to appear on the birth certificate)? 1

Child First Name(s): _____

Middle Name(s): _____

Last Name(s): _____ Suffix (Jr. Sr. etc): _____

2. OPTIONAL
When labor *started,* where did the parent *plan* to give birth? 8

This information is NOT provided to insurance companies or other state agencies. There are NO legal or insurance consequences to parents based on where they intended to give birth.

◯ Home - Midwife Name: _____ ◯ No midwife

◯ Freestanding birth center - Midwife Name: _____ ◯ No midwife

Facility Name: _____

◯ Hospital

◯ Labor never started. Parent 1 had a C-section without labor.

3. REQUIRED
Do you want a Social Security Number issued for your baby? 11

◯ No

◯ **YES** Provide my child's information to the Social Security Administration for purposes of issuing a social security card to my child.

Parental signature required: X _____

To order a Social Security Card for your child, be sure to check "Yes" above and sign. The Social Security card will be mailed in 2-3 weeks. To ensure delivery, add your baby's name to the names listed on the mailbox. Post offices will forward if a forwarding address is filed with them. If you need the card mailed in care of someone else, please fill out item #17. If the card is returned undeliverable parents will need to apply to SSA for a replacement card. Hospitals and Vital Records cannot process a second request. A Social Security Card cannot be mailed out of the country except under certain circumstances. Diacritical marks such as accents are not accepted by the Social Security Administration and will not appear on the Social Security card.

4. OPTIONAL
What would Parent 1 like to be known as on the child's birth certificate? (If not indicated, default is Mother) 12

◯ Mother ◯ Father ◯ Parent (female) ◯ Parent(male)

5. REQUIRED
Was Parent 1 married when the child was conceived, at the time of birth, or within the last 300 days (about 10 months)? 14,16,17

◯ Yes, to the biological father (skip to #6)
◯ Yes, but not to the biological father (please see below)
◯ No (please see below)

If not married to the biological father, do you wish to legally acknowledge him on the birth certificate?
◯ Yes (please see below) ◯ No (Skip to #6)

The **Voluntary Declaration of Paternity (VDP) form** is the legal form parents who are not married **must** sign in order to legally acknowledge the biological father of the child and list him on the birth certificate. If currently married, but not to the biological father: the **current spouse, the biological father, and Parent 1 must** sign the VDP. If married within the last 300 days: the **ex-spouse, the biological father, and Parent 1 must** sign the VDP. When this Parental Worksheet is given to the birth clerk or midwife the VDP form will be prepared for parents to sign.

6. OPTIONAL
Was the child delivered by a gestational surrogate? 18

◯ Yes ◯ No

7. REQUIRED
What is Parent 1's current legal name? 19

First Name(s): _____

Middle Name(s): _____

Last Name(s): _____ Suffix (Jr. Sr. etc): _____

8. REQUIRED
What was Parent 1's name prior to first marriage? 20
Name as it appears on the current birth certificate. Not a name prior to adoption or other court-ordered name change. Print clearly using upper and lower case characters and spacing as needed.

The name listed below will appear on the child's birth certificate.

First Name(s): _____

Middle Name(s): _____

Last Name(s) (Maiden/Surnames): _____ Suffix (Jr. Sr. etc): _____

9. REQUIRED
What is Parent 1's date of birth? 21

mm/dd/yyyy: _____

10. OPTIONAL 22
Please provide a phone number where we can reach you if we have questions about any of the information provided.

Parent 1 Phone Number: _____

11. REQUIRED
What is Parent 1's. Social Security Number? 23
SSN is required by Federal Law, 42 USC 405(c) Section 205(c) Social Security Act

12. REQUIRED
In what State, U.S. Territory, or foreign country was Parent 1 born? 24

State: _____ or U.S. Territory: _____
Spell out name of U.S. State

OR, if not born in the US or US Territories, what Foreign country: _____

13. REQUIRED
Where does Parent 1 usually live - that is - where is your household/residence located? 26

Complete number and street: _____

Apartment /Unit/Space number: _____ City/Town or Location: _____

U.S. State: _____ Zip Code: _____ County: _____

Foreign Country if not in U. S: _____

14. REQUIRED
Is this household Inside city limits? 27

◯ Yes ◯ No ◯ I don't know

15. OPTIONAL
Parent Email Address - You will receive an immediate email confirming the birth registration from Vital Records allowing you to order and purchase your child's birth certificate. 28

Parent #1 Email: _____ **Print Clearly**

16. REQUIRED
What is your mailing address? (See #17 if your child's SS card is to be mailed to in care of address) 29

◯ Same as residence

Complete number and street: _____

Apartment /Unit/Space number: _____ PO Box: _____

City/Town or Location: _____ U.S. State: _____

Zip Code: _____ County: _____

Foreign Country if not in U. S: _____

23. REQUIRED
What is Parent 2's Social Security Number? 41

SSN is required by Federal Law, 42 USC 405(c) Section 205(c) Social Security Act

24. REQUIRED
In what State, U.S. Territory, or foreign country was Parent 2 born? 42

State: _____ or U.S. Territory: _____
Spell out name of U.S. State

OR, if not born in the US or US Territories, what Foreign country: _____

25. OPTIONAL
Parent Email Address - You will receive an immediate email confirming the birth registration from Vital Records allowing you to order and purchase your child's birth certificate. 46

Parent #2 Email:_____ **Print Clearly**

26. REQUIRED
Is this child to be relinquished or placed for adoption? 48

◯ Yes ◯ No If 'Yes', please list the name of the agency and/or attorney or "private adoption":

_____

27. REQUIRED
Did Parent 1 receive WIC (Women, Infants and Children) food for themselves during this Pregnancy? 51

◯ Yes ◯ No ◯ I Don't know

28. OPTIONAL
Does anyone in the family (biological parents, siblings, aunts, uncles, grandparents, cousins) have a hearing loss (not caused by loud noise, illness, or ear infection) they were born with or which developed in childhood? 53

◯ Yes ◯ No ◯ I don't know

29. REQUIRED
What is Parent 1's height? 54

_____ Feet _____ Inches

30. REQUIRED
What was Parent 1's weight before you were pregnant with this child? 55

_____Lbs.

31. REQUIRED
Did Parent 1 Smoke? 57

◯ Yes ◯ No
If 'yes', how many cigarettes per day did you smoke on an average day during each of the following time periods?
(20 cigarettes per pack)
Three months before pregnancy # _____ Second three months of pregnancy # _____
First three months of pregnancy # _____ Third trimester of pregnancy # _____

32. OPTIONAL
Was Parent 1 transferred to a hospital *within 24 hours after delivering* at a home or birth center? 75

◯ Yes, transferred after delivering **at *home***
Midwife Name: _____
◯ Midwife attended, name unknown
◯ No midwife
◯ Unknown if midwife attended
◯ Yes, transferred after delivering **at *freestanding birth center***
Midwife Name: _____
Facility Name: _____
◯ No, Parent 1 did not transfer to a hospital *within 24 hours after delivering* at a home or birth center.
◯ Unknown if Parent 1 transferred to a hospital *within 24 hours after delivering* at a home or birth center.

33. OPTIONAL
During the month before pregnancy, how many times per week did Parent 1 take a multivitamin, prenatal vitamin or folic acid vitamin? 80

◯ Did not take vitamins ◯ 1 to 3 times per week ◯ 4 to 6 times per week ◯ Every Day ◯ Unknown
If Parent 1 did not take vitamins, what were the reasons - choose all that apply.
◯ Wasn't planning to get pregnant
◯ Didn't want to take vitamins
◯ Didn't think vitamins were needed
◯ Vitamins were too expensive
◯ Experienced side effects after taking (please tell us what you experienced) _____
◯ Other - specify reasons: _____
◯ Unknown

34. REQUIRED
Is Parent 1 of Hispanic Origin? 84

◯ Yes (mark all that apply below) ◯ No, not of Hispanic origin
◯ Yes, Mexican, Mexican American, Chicana(o)
◯ Yes, Puerto Rican
◯ Yes, Cuban
◯ Yes, other Hispanic origin - Specify: _____
(e.g. Spaniard, Salvadoran, Dominican, Colombian)

35. REQUIRED
What is the race of Parent 1? (Please check one or more races to indicate what you consider yourself to be). 85

- ◯ White
- ◯ Black or African American
- ◯ American Indian or Alaska Native - Specify tribe: _____
- ◯ Asian Indian
- ◯ Chinese
- ◯ Filipino
- ◯ Japanese
- ◯ Korean
- ◯ Vietnamese
- ◯ Other Asian - Specify: _____
- ◯ Native Hawaiian
- ◯ Guamanian or Chamorro
- ◯ Samoan
- ◯ Tongan (OPTIONAL)
- ◯ Other Pacific Islander - Specify: _____
- ◯ Other - Specify: _____
- ◯ Unknown (OPTIONAL)

36. REQUIRED
What is the highest level of schooling that Parent 1 will have completed at the time of delivery? 86

- ◯ 8th grade or less
- ◯ 9th-12th grade no diploma
- ◯ High School Graduate or GED completed
- ◯ Some college credit, but no degree
- ◯ Associate Degree (e.g. AA, AS)
- ◯ Bachelor's Degree (e.g. BA, AB, BS)
- ◯ Master's Degree (MA MS, MEng, Med, MSW, MBA)
- ◯ Doctorate (e.g. PhD, EdD) or Professional degree (e.g. MD, DDs, DVM, LLB, JD)

37. REQUIRED
Is Parent 2 of Hispanic origin? 87

- ◯ Yes (mark all that apply below)
- ◯ No, not of Hispanic origin
- ◯ Yes, Mexican, Mexican American, Chicana(o)
- ◯ Yes, Puerto Rican
- ◯ Yes, Cuban
- ◯ Yes, other Hispanic orgin - Specify: _____
  (e.g. Spaniard, Salvadoran, Dominican, Colombian)

38. REQUIRED
What is the race of Parent 2? (Please check one or more races to indicate what you consider yourself to be). 88

◯ White
◯ Black or African American
◯ American Indian or Alaska Native - Specify tribe: _____
◯ Asian Indian
◯ Chinese
◯ Filipino
◯ Japanese
◯ Korean
◯ Vietnamese
◯ Other Asian - Specify: _____
◯ Native Hawaiian
◯ Guamanian or Chamorro
◯ Samoan
◯ Tongan (OPTIONAL)
◯ Other Pacific Islander - Specify: _____
◯ Other - Specify: _____
◯ Unknown (OPTIONAL)

39. REQUIRED
What is the highest level of schooling that Parent 2 will have completed at the time of delivery? 89

◯ 8th grade or less
◯ 9th-12th grade no diploma
◯ High School Graduate or GED completed
◯ Some college credit, but no degree
◯ Associate Degree (e.g. AA, AS)
◯ Bachelor's Degree (e.g. BA, AB, BS)
◯ Master's Degree (MA MS, MEng, Med, MSW, MBA)
◯ Doctorate (e.g. PhD, EdD) or Professional degree (e.g. MD, DDs, DVM, LLB, JD)
◯ Unknown (OPTIONAL)

40. REQUIRED
Did this pregnancy result from infertility treatment? 90

◯ Yes (please answer questions below) ◯ No
If yes, did this pregnancy result from fertility-enhancing drugs, artificial insemination, or intrauterine insemination?
◯ Yes ◯ No
If yes, did this pregnancy result from assisted reproductive technology (e.g. in-vitro fertilization (IVF), gamete intrafallopian transfer (GIFT)?
◯ Yes ◯ No

REQUIRED
Parent 1 Signature
I certify that the personal information provided on this worksheet is correct to the best of my knowledge.
X _____

OPTIONAL
Parent 2 Signature
I certify that the personal information provided on this worksheet is correct to the best of my knowledge.
X _____

It is not necessary to fill out this form for each child of a multiple birth. Complete the form below for additional children born at the same time.

Parent's Name: _____ Room Number: _____

SFN of Baby A: _____

TWIN B / TRIPLET B/ QUADRUPLET B

41. OPTIONAL
What will be your baby #2's legal name (as you wish it to appear on the birth certificate)? 93

Child First Name(s): _____

Middle Name(s): _____

Last Name(s): _____ Suffix (Jr. Sr. etc): _____

TRIPLET C/ QUADRUPLET C

42. OPTIONAL
What will be your baby #3's legal name (as you wish it to appear on the birth certificate)? 94

Child First Name(s): _____

Middle Name(s): _____

Last Name(s): _____ Suffix (Jr. Sr. etc): _____

QUADRUPLET D

43. OPTIONAL
What will be your baby #4's legal name (as you wish it to appear on the birth certificate)? 95

Child First Name(s): _____

Middle Name(s): _____

Last Name(s): _____ Suffix (Jr. Sr. etc): _____

D. OVRS's Facility Worksheet for Birth Registration

Facility Worksheet for Birth Registration

The items below were formerly on the Parent Worksheet for Birth Registration. They are required for birth registration but can no longer be gathered from the parent by Vital Records as we are required to ask only the questions on the Federal Mother's Worksheet for Child's Birth Certificate. This form follows the Federal Facility Worksheet form that has previously not been used in Utah but will now be required. This worksheet does not need to be returned to Vital Records. The information is required entry in UINTAH – the birth registration system.

1. Child Sex: ◯ Male ◯ Female ◯ Undetermined (2)

2. Date of birth mm/dd/yyyy: _____(3)

3. Time of birth (24 hr clock): _____(4)

4. Child birth Weight: _____LBS _____OZ. (5)

6. Child birth Length (Inches): _____(6)

7. Where was the baby born? (7)

- ◯ Hospital - Facility Name: _____
- ◯ Baby was born while traveling to hospital
- ◯ Freestanding birth center - Facility Name: _____
- ◯ Baby was born while traveling to birth center
- ◯ Clinic / Doctor's Office
- ◯ Home - intended
- ◯ Home - not intended
- ◯ Home - unknown if intended
- ◯ Other
- ◯ Unknown

8. Name of delivering birth professional or other birth attendant: _____
Title: _____(10)

9. Was Parent 1 enrolled in Medicaid at time of birth? ◯ Yes ◯ No (50)

10. Primary Source of payment for this delivery: ◯ Medicaid ◯ Private Insurance ◯ Self-Pay
◯ Indian Health Service ◯ CHAMPUS/TRICARE ◯ Other Government (Fed, State, Local) ◯ CHIP
◯ Other ◯ Unknown (check if Medicaid Pending) (52)

11. Parent 1 weight at Delivery: _____Lbs. (56)

12. Is the infant being breast-fed at discharge? ◯ Yes ◯ No (61)

13. Was Parent 1 told by her healthcare provider that she had gestational diabetes during this pregnancy? (62)
◯ Yes ◯ No

14. Date of last menses (last period) mm/dd/yy: _____(64)

15. Number of previous births now living: #_____(65) (Do not include this child)

16. Date of last live birth (do not include this child) mm/yyyy: _____ (66)

17. Number of previous live births now deceased: #_____ (67)

18. Total number of pregnancies not resulting in live birth: #_____(68)

19. Date of last pregnancy not resulting in a live birth: _____ (69)

20. Total number of stillbirths: _____(70)
Losses at 20+ weeks or greater born without signs of life. (Do not include induced terminations - any weeks)

21. Date of first prenatal care visit mm/dd/yyyy: _____ (72)

22. Number of prenatal visits this pregnancy: # _____ (73)

24. Did Parent 1 transfer to a hospital *during labor, but before delivery* from an attempted home or birth center birth? (75)
This information is NOT provided to insurance companies or other state agencies. There are NO legal or insurance consequences to parents based on where they intend to give birth.

◯ Yes, transferred from attempted birth *at home* Midwife Name: _____

◯ Midwife attended, name unknown

◯ Unknown if midwife attended ◯ No midwife

◯ Yes, transferred from attempted birth *at freestanding birth center* - Midwife Name: _____

Facility Name: _____

◯ No, Parent 1 did not transfer to a hospital *during labor* from an attempted home or birth center birth.

◯ Unknown if Parent 1 transferred to a hospital *during labor* from an attempted home or birth center birth.

E. CDC Birth Edits Specifications for US Standard Birth Certificate

Birth Edit Specifications for the 2003 Revision of the U.S. Standard Certificate of Birth

Updated 6/2021

Note: This document replaces Instruction Manual Part 3a, "Classification and Coding Instructions for Live Birth Records" and "Birth Edit Specifications for the 2003 Proposed Revision of the U.S. Standard Certificate of Birth," 7/2012 update

4/2004; 3/2005; 7/2012; Updated 6//2021

TABLE OF CONTENTS

U.S. STANDARD CERTIFICATE OF LIVE BIRTH

4/2004; 3/2005; 7/2012; Updated 6//2021

Item 51	APGAR SCORE
Items 52,53	PLURALITY, SET ORDER
Item 54	ABNORMAL CONDITIONS OF THE NEWBORN
Item 55	CONGENITAL ANOMALIES OF THE NEWBORN
Item 56	WAS INFANT TRANSFERRED WITHIN 24 HOURS OF DELIVERY? IF YES, NAME OF FACILITY TO WHICH INFANT TRANSFERRED
Item 57	IS INFANT LIVING AT THE TIME OF REPORT?
Item 58	IS INFANT BEING BREASTFED?

PLACEHOLDER FIELDS

FILE PROCESSING ITEMS

STATE OF BIRTH
CERTIFICATE NUMBER
VOID FLAG
AUXILIARY STATE FILE NUMBER

APPENDICES

APPENDIX A	COUNTRY CODES
APPENDIX B	STATE, TERRITORY, AND CANADIAN PROVINCE CODES
APPENDIX C	CITY AND COUNTY CODES
APPENDIX D	HISPANIC ORIGIN LOOK-UP TABLE
APPENDIX E	RACE CODES

4/2004; 3/2005; 7/2012; Updated 6//2021

Agency Response

State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

Department of Government Operations
Executive Director's Office

MARVIN DODGE
Executive Director

CHRISTOPHER HUGHES
Deputy Director

MARILEE P. RICHINS
Deputy Director

June 5, 2023

Kade R. Minchey CIA, CFE
Auditor General Office of the Legislative Auditor General
P.O Box 145315
Salt Lake City, UT 84114-5315

Dear Mr. Minchey,

Thank you for the opportunity to respond to the findings and recommendations in A Performance Audit of the Collection, Protection, and Use of Personal Information by State Agencies (23-07).

The Department of Government Operations (DGO) concurs with all applicable findings and recommendations in the audit. DGO is a recently formed department that consists of a merging of multiple previously independent state agencies. As part of the consolidation, during the 2023 general session, DGO received funding for a Director of Information Privacy and Security position that will lead the efforts for DGO to create and implement an information privacy and security program. This program will be based on the privacy program components identified in the strategic privacy plan that is being created by the Chief Privacy Officer (CPO) pursuant to Executive Order 2023-06. The strategic privacy plan will account for privacy risk management practices that state agencies should implement as part of a privacy program. These practices relate directly to the scope of this audit including collection, use, sharing, and protection of personal information.

We agree with the recommendations in the audit as well as the analysis and recommendations of the CPO in the 2022 privacy report to the Judiciary Interim Committee. For DGO, a comprehensive privacy act would not only benefit our own privacy program, but also enable us to better identify opportunities to standardize and operationalize privacy services that will increase privacy program maturity and efficiency of privacy programs for all agencies.

We appreciate the professionalism of you and your staff during this audit and for the guidance and recommendations you have provided for improvement. We believe our combined efforts will result in improvements that will benefit DGO and the agencies we serve.

Sincerely,

Marvin L. Dodge
Executive Director

Department of Government Operations
Chief Privacy Officer, State of Utah

State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

MARVIN DODGE
Executive Director

CHRISTOPHER BRAMWELL
Chief Privacy Officer

June 5, 2023

Kade R. Minchey CIA, CFE
Auditor General Office of the Legislative Auditor General
P.O Box 145315
Salt Lake City, UT 84114-5315

Dear Mr. Minchey,

We have reviewed your Exposure Draft of *A Performance Audit of the Collection, Protection, and Use of Personal Information by State Agencies, Report No. 2023-07*. The audit identified two findings that are generally applicable to all state agencies and provided three recommendations to the legislature. As the State of Utah Chief Privacy Officer (CPO), appointed by Governor Spencer J. Cox, I have the authority and responsibility to, among others, assess privacy practices of state agencies and to make recommendations, including legislative, to the Judiciary Interim Committee. It is encouraging to see that the findings and recommendations from your audit and the internal assessment data and recommendations of the CPO are aligned.

Below, you will find an acknowledgement and response to each of the findings. We appreciate the efforts of the Office of the Legislative Auditor General. Auditing privacy in Utah is an incredible undertaking. We are confident that these findings provide support for the many efforts underway to assess and improve privacy practices of state agencies to provide for appropriate protection of individual Utahn's privacy rights.

PO Box 141002 , Salt Lake City, UT 84114-1002 ♦ telephone 801-957-7171 ♦ https://govops.utah.gov/

CHAPTER 1

Finding 1.1 State agencies' current data collection and sharing practices create data privacy risk. Statutory data privacy guardrails could alleviate the risk.

We agree that this audit finding is valid. The finding aligns with similar assessments made under the authority of the CPO. These assessments also identified the need for clearly defined legislative requirements addressing privacy risk management processes, policies, and procedures for agencies to ensure the protection of the privacy rights of individuals.

Finding 1.2 Without statutory direction, determining data privacy policy falls to state agencies. Agencies have varying definitions of data privacy, and some appear to be unfamiliar with data privacy principles.

We agree that this audit finding is valid. The CPO has identified that many state agencies do not have comprehensive privacy policies that account for the processes and practices that would be essential aspects of a standard privacy program. On April 21, 2023, Governor Cox issued Executive Order 2023-06, which directs the CPO to propose a strategic privacy plan that identifies privacy policies and practices that are generally required of state agencies pursuant to law or that are recommended pursuant to accepted privacy standards and best practices. However, without statutory direction, enforcement of an agency's creation and implementation of the policies and practices identified in the plan is limited.

Recommendation 1.1 We recommend that the Legislature consider whether guardrails are needed to balance the benefits of data and data sharing with agencies' data privacy practices.

We agree with this recommendation. The current patchwork of privacy related laws, rules, and policies cause unnecessary confusion among state agencies and the public. Generally applicable guardrails, in the form of comprehensive legislation, that balance the benefits of data and data sharing with data privacy practices of agencies would ameliorate the risk that such confusion can cause.

Recommendation 1.2 We recommend that the Legislature consider the merits of passing a data privacy act into statute to provide state agencies with a data privacy governance structure and to incorporate principles of data privacy into their practices for data processing and sharing.

We agree with this recommendation. The CPO identified in the 2022 report to the Judicial Interim Committee that Utah lacks comprehensive privacy laws that are applicable to all state agencies. It is the opinion of the CPO that the existing privacy laws and rules that are applicable to state agencies are fragmented, lack consistency, and create confusion for agencies. The following list includes foundational components/topics that the CPO recommends be considered for any comprehensive privacy legislation.

PO Box 141002 , Salt Lake City, UT 84114-1002 ♦ telephone 801-957-7171 ♦ https://govops.utah.gov/

- **Data Protection Principles:** Privacy legislation should establish fundamental principles that guide the processing of personal data. These principles typically include concepts such as lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.
- **Consent and Individual Rights:** The legislation should address the requirement for informed and freely given consent from individuals when their personal data is collected and processed. It should also recognize individuals' rights, such as the right to access, rectify, delete, and restrict the processing of their personal data.
- **Data Breach Notification:** Legislation should mandate agencies to promptly notify individuals and relevant authorities in the event of a data breach that poses a risk to individuals' rights and freedoms. It should outline the requirements for timely reporting, the information to be provided, and any necessary mitigation measures.
- **Purpose Specification and Limitation:** Privacy legislation should emphasize that personal data should only be collected for specified, explicit, and legitimate purposes. It should restrict further processing that is incompatible with the original purpose unless additional consent is obtained.
- **Data Minimization and Storage Limitation:** The legislation should encourage the collection of only necessary personal data and impose limitations on the retention of data. Agencies should be required to securely dispose of personal data when it is no longer needed for its intended purpose.
- **Data Transfer and International Cooperation:** Privacy legislation should address the transfer of personal data to third countries, ensuring adequate protection for individuals' data when it crosses borders.
- **Accountability and Governance:** The legislation should emphasize the accountability of agencies handling personal data. It should require them to implement appropriate technical and organizational measures to protect personal data, conduct privacy impact assessments, and appoint data privacy officers where necessary.
- **Enforcement and Remedies:** Privacy legislation should establish effective enforcement mechanisms and should also provide individuals with avenues for seeking remedies and lodging complaints with regulatory authorities.
- **Privacy by Design and Default:** The legislation should promote the integration of privacy considerations throughout the design and development of systems, products, and services. Privacy-enhancing technologies and practices should be encouraged to ensure privacy is the default setting.
- **Transparent Information Practices:** Agencies should be required to provide clear and easily understandable information to individuals about their data processing practices, including purposes, legal basis, retention periods, and rights.

Recommendation 1.3 We recommend that the Legislature consider defining data privacy in statute for all state agencies.

We agree with this recommendation. The current lack of comprehensive privacy laws along with the lack of a standard taxonomy and lexicon that is applicable to all state agencies increases

the complexity for agencies of knowing what their privacy obligations are and may result in increased risks to privacy. The CPO has included in the strategic privacy plan a standard set of definitions and lexicon for use as part of the plan and is recommending that the executive branch adopt a standard set definitions and lexicon as part of its overall data management strategy.

CHAPTER 2.

The CPO was not directly involved in the audit of the Office of Vital Records and Statistics within the Department of Health and Human Services, which is presented as Chapter 2 of the audit. As such, the CPO does not comment on the findings, which were made in conjunction with the reviews of the consultant–and the consultant's full report was not provided for consideration with the Exposure Draft. However, the CPO is charged with assessing privacy practices of state agencies and making recommendations for improvement, which includes making recommendations to the Legislature, and thus the input of the CPO is pertinent.

Generally speaking, the CPO is supportive of the recommendations presented in the audit. Agencies may be subject to a number of various legal sources that place obligations on personal information that a state agency collects (law, regulation, rule, contract, etc.). As such, clarification of the requirements and parameters that are placed on a particular agency are often an excellent way of reducing risk. Clear and understandable privacy obligations provided by the Legislature will reduce risk to an individual's right of privacy as well as protect the state from potential liability presented by deficient privacy practices of state agencies.

Data privacy is an issue that is garnering more and more attention within the private sector and is now, rightfully, gaining more attention in the public sector. Data is necessary for state agencies to carry out their mandates, but privacy rights must be protected as well. Balancing these two competing priorities is a difficult but necessary task and it will take all parties working together to appropriately make and carry forward such balance. As CPO I look forward to working with OLAG, the Legislature, executive branch agencies, and the public to continue improving privacy protections for individuals' personal information.

Sincerely,

Christopher Bramwell

Christopher D. Bramwell
Chief Privacy Officer, State of Utah

PO Box 141002 , Salt Lake City, UT 84114-1002 ♦ telephone 801-957-7171 ♦ https://govops.utah.gov/

State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

Department of Health & Human Services

TRACY S. GRUBER
Executive Director

NATE CHECKETTS
Deputy Director

DR. MICHELLE HOFMANN
Executive Medical Director

DAVID LITVACK
Deputy Director

NATE WINTERS
Deputy Director

June 5, 2023

Kade R. Minchey CIA, CFE, Auditor General
Office of the Legislative Auditor General Utah State Capitol Complex
Rebecca Lockhart House Building, Suite W315
P.O. Box 145315
Salt Lake City, UT 84114-5315

Dear Mr. Minchey,

Thank you for the opportunity to respond to the recommendations in *A Performance Audit of the Collection, Protection, and Use of Personal Information by State Agencies* (Report #2023-07). On behalf of the Utah Department of Health and Human Services (DHHS), I want to express my appreciation to the Office of Legislative Auditor General and its professionalism in working with our staff in the Office of Vital Records and Statistics (OVRS) to ensure our department is collecting, protectings and utilizing the data it collects within the bounds of the law and in accordance with the expectations of the Utah Legislature.

Our department takes its responsibility to protect the privacy of the individuals served by DHHS seriously. The recommendations contained in this report will ensure we continue to make progress on that commitment. While this audit focuses on privacy across all state agencies, Chapter 2 focuses specifically on the information collected by OVRS. As a result, the following responses submitted by DHHS apply exclusively to Chapter 2. We concur with the recommendations made in Chapter 2 of this report

On behalf of DHHS and OVRS, I want to express our strong commitment to implementing the recommendations included in this report. While our responses only apply to Chapter 2, we acknowledge the recommendations contained throughout this report apply to all state agencies including DHHS. We look forward to working with the state's Chief Privacy Office to implement the recommendation made throughout this report. We will ensure that updates are provided to your office on a quarterly basis to demonstrate this commitment and ensure accountability for implementation.

Sincerely,

Tracy S. Gruber
Executive Director

Recommendation 2.1 We recommend the Legislature consider clarifying the collection of birth registration data. One clarifying option being the separation of essential birth registration information from research questions into two separate forms.

Department Response: DHHS concurs that the Legislature further clarify the collection of birth registration data to distinguish required data elements from optional data elements. After the 2022 General Session, OVRS did make modifications to the mother's worksheet in an effort to distinguish required from optional elements. However, OVRS acknowledges that further clarification by the Legislature may be needed.

How: OVRS will review options for further clarifying the birth registration worksheet as recommended by the auditors and make any necessary updates to the form.

When: Form will be updated no later than November 31, 2023.

Contact: Linda Wininger, lindaw@utah.gov

Recommendation 2.2 We recommend the Legislature consider the merits of requiring government entities adopt data privacy principles that include items such as: clear consent, notice, and the disclosure of data collection, use, and sharing.

Department Response: DHHS concurs with this recommendation and agrees that further guidance is needed with respect to consent, notice and the use of data to those submitting private data to OVRS. DHHS will modify its practices to comply with any statutory changes and implement appropriate rules to align with any new policies adopted by the Utah Legislature.

While DHHS concurs with the recommendation, in the interim, DHHS' Office of Information Privacy and Security (IPS) and OVRS will review OVRS policies and procedures with respect to ensuring clear consent, notice to individuals with respect to collection and disclosure when private data is collected, is used, or shared.

How: IPS and OVRS will review practices around clear consent, notice to individuals with respect to collection and disclosure when privacy data is collected, is used, or shared in order to identify opportunities for improving privacy practices in OVRS.

When: IPS and OVRS will complete their review prior to September 30, 2023.

Contact: Kyle Lunt, kylelunt@utah.gov

Recommendation 2.3 We recommend the Legislature consider Office of Vital Records and Statistics data collection and processing practices and whether to establish data privacy policy for state agencies in Utah.

Department Response: DHHS concurs with this recommendation and OVRS will cooperate with the Legislature in adopting any new policies related to data collection and use of the data. Should the legislature pass new policies on data privacy, the Department of Health and Human Services (DHHS) will modify its practices to comply with the new regulations. DHHS and OVRS will continue to follow department-wide privacy and security policies to ensure appropriate oversight.

State Headquarters: 195 North 1950 West, Salt Lake City, Utah 84116
telephone: (801) 538-4001 | email: dhhs@utah.gov | web: dhhs.utah.gov

How: OVRS will review its practices, including those established by DHHS policies and procedures to evaluate whether modifications are needed to its data collection and processing practices, including its data privacy policy.

When: OVRS will complete their review prior to September 30, 2023.

Contact: Kyle Lunt, kylelunt@utah.gov