Department of Government Operations
Division of Technology Services

State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

JENNEY REES
Executive Director

ALAN FULLER
Chief Information Officer

September 30, 2022

Chair and members of the Judiciary Interim Committee,

This report is submitted by the Government Operations Privacy Officer (GOPO), pursuant to Utah Code § 67-1-17. The GOPO is directed to review the privacy practices of state agencies to determine whether the practices adequately protect individual privacy and make recommendations for reform, including recommendations for legislation. Over the past year the GOPO has worked closely with state agencies, the Personal Privacy Oversight Commission, State Privacy Officer, State Archivist, State Chief Information Security Officer (CISO), and the executives of the Department of Government Operations to coordinate privacy practice reviews and establish a consensus on recommendations to be made to ensure adequate protection of an individual's constitutional right of privacy in relation to governmental processing of personal information.

The assessments contained in the report detail the privacy practices that have been reviewed, the determinations made from the reviews, and how the determinations establish support for the proposed legislative amendments that are directed toward the Government Records Access and Management Act (GRAMA) and Utah Code § 63A-12-100 *et seq.*, formerly known as the Public Records Management Act (PRMA). Through the targeted amendments, GRAMA and PRMA may serve as a foundation for standardizing the privacy practices of state agencies, as well as allowing for continued improvement, to ensure adequate protection of the constitutional right of privacy in addition to maintaining records management requirements.

The GOPO welcomes any questions that the Committee might have as well as an opportunity to discuss the reviews and recommendations that have been made in addition to the plans for continuing to improve the privacy practices of state agencies moving forward.

Sincerely,

Christopher D. Bramwell

Government Operations Privacy Officer
Department of Government Operations, Division of Technology Services

utah govops

UTAH DEPARTMENT OF GOVERNMENT OPERATIONS

Division of Technology Services

Government Operations Privacy Officer's Annual Report To The Judiciary Interim Committee 2022

TABLE OF CONTENTS:

Key Terminology & Definitions:

This report uses many words and phrases that may be considered “terms of art” within the information privacy and cybersecurity fields in addition to certain terms that have been defined within Utah Code, and terms for which definitions are included in the proposed legislative amendments that are discussed within, and attached to, this report. This list of key terms and definitions is meant to serve as a helpful aide but is not exhaustive. The endnotes include additional definitions as well as citations to defined terms, etc.

Constitutional right of privacy (or “right to privacy”): for purposes of this report, means a “constitutional … right of privacy in relation to personal data gathered by governmental entities,” as recognized by the Utah Legislature. Utah Code § 63G-3-103(1).

Legal requirements: for purposes of this report, legal requirements are meant to incorporate state and federal laws, rules, regulations, and other obligations that are supported by force of law e.g., contracts and grants.

Personal Identifiable Information (PII): for purposes of this report, personal data or personal information refers to PII and PII is meant to incorporate all similar phrases that refer to information that may identify an individual, whether by itself as a singular data element, or if combined, linked, or is linkable with additional information or data elements. PII includes “personal data” as defined in Utah Code § 67-1-17, which is the Section of Utah Code that establishes the Government Operations Privacy Officer.

Privacy practice: for purposes of this report, has the same meaning as defined in Utah Code § 67-1-17(1)(c)(i) and (ii), “Privacy practice means the acquisition, use, storage, or disposal of personal data. "Privacy practice" includes: a technology use related to personal data; and policies related to the protection, storage, sharing, and retention of personal data.”

Process(ed/ing): for purposes of this report, process, when referring to data or information, is meant to incorporate any and all agency activities or functions that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by entities, programs, and information systems.

State agency: for purposes of this report, has the same meaning as defined in Utah Code § 67-1-17(1)(d)(i) and (ii), “State agency means the following entities that are under the direct supervision and control of the governor or the lieutenant governor: a department; a commission; a board; a council; an institution; an officer; a corporation; a fund; a division; an office; a committee; an authority; a laboratory; a library; a bureau; a panel; another administrative unit of the state; or an agent of an entity described in Subsections (A) through (Q). "State agency" does not include: the legislative branch; the judicial branch; an executive branch agency within the Office of the Attorney General, the state auditor, the state treasurer, or the State Board of Education; or an independent entity.”

Introduction

In the Government Records Access and Management Act (GRAMA), the Utah Legislature recognized a "**constitutional … right of privacy in relation to personal data**[1] **gathered by governmental entities**." Utah Code § 63G-3-103(1) (emphasis added).

During the 2021 General Session the Legislature passed H.B. 243 Privacy Protection Amendments, codified at Utah Code §§ 67-1-17, 63C-24-101 *et seq.*, and 67-3-13. H.B. 243 created the Government Operations Privacy Officer, the Personal Privacy Oversight Commission (PPOC), and within the State Auditor's Office the State Privacy Officer (SPO). The bill also outlined the parties' respective authorities, responsibilities, and duties. The authority is fairly limited, with a focus on the review and assessment of the privacy practices, providing educational and training materials, and recommending legislation.

The Government Operations Privacy Officer (GOPO) as created in Utah Code § 67-1-17, is mandated to, with respect to personal data[2], review the privacy practices[3] of state agencies[4], determine whether the privacy practices adequately protect individual privacy, provide recommendations to a state agency for privacy practices that require reform, determine the existence of alternative technology or improved practices to protect privacy, and make recommendations for legislation based on the results from the reviews. Further, the GOPO is required to report to the Judiciary Interim Committee annually, on or before October 1.[5] Thus, in conjunction with the constitutional right to privacy recognized in GRAMA, the question that the Legislature has tasked the GOPO to answer and report back on, may be summarized as:

Do The Privacy Practices Of Executive Branch State Agencies Adequately Protect The Constitutional Right Of Individual Privacy In Relation To Personal Data Processed By Executive Branch State Agencies?

Synopsis:

Privacy Practice Assessment

- We assessed the extent of legal requirements that govern state agencies' privacy practices with respect to processing of personal data.

NIST Privacy Framework

- **GV.PO-P5:** Legal, regulatory, and contractual requirements regarding privacy are understood and managed.[6]

Assessment #1 - 2022

KEY FINDINGS:

In Utah, not all state agencies are subject to or governed by a particular or comprehensive state or federal information privacy law, rule, or regulation that clearly establishes requirements for the privacy practices of state agencies with respect to personal data.

KEY DETERMINATIONS:

State agencies are generally subject to GRAMA and Utah Code § 63A-12-100 *et seq*., formerly known as the Public Records Management Act (PRMA), less certain exceptions, and as such, with targeted amendments, GRAMA and PRMA may serve as a foundation for improving privacy practices of state agencies to ensure adequate protection of the constitutional right of privacy in addition to maintaining records management requirements.

RISKS:

Absent explicit requirements that apply to the privacy practices of all state agencies, state agencies are left to decide, in an ad hoc fashion, if and what privacy practices to create and implement. Thereby not allowing for standardized review and assessment of the adequacy of the privacy protections of citizen's personal data.

KEY RECOMMENDATIONS:

The GOPO recommends that the proposed legislative amendments attached to this report as Appendix A, be supported, as they have also received the support of the PPOC, SPO, and the executive leadership of the Department of Government Operations (DGO).

Current State of Legal Requirements with Respect to the Privacy of Personal Information Collected by State Agencies

A review of the privacy practices of state agencies must account for any applicable legal requirements. In Utah, not all state agencies are subject to or governed by a particular or comprehensive state or federal information privacy law, rule, or regulation that clearly and concisely establishes requirements for the privacy practices of state agencies with respect to personal data. There are sections of Utah Code that may address a specific state agency or program with respect to privacy and personal data that it collects for specified purposes. And there are specific laws and regulations that may apply to a particular industry or entity with respect to privacy of specific elements of personal data. As such, given the number of state agencies, the number of government services being provided, and number of interactions with individuals, and thus, the processing of personal data, together with the disparate breadth and scope of applicable law, a one-by-one review and analysis of each privacy practice of each state agency would seemingly never be completed. However, state agencies are generally subject to GRAMA and Utah Code § 63A-12-100 *et seq.*, formerly known as the Public Records Management Act (PRMA), less certain exceptions, and as such, with targeted amendments, GRAMA and PRMA may serve as a foundation for standardizing the privacy practices of state agencies to ensure adequate protection of the constitutional right of privacy in addition to maintaining records management requirements.

There are some issues that must be addressed within both GRAMA and PRMA for them to serve as an adequate foundation for state agencies' privacy practices. First, although GRAMA contains the legislature's recognition of a constitutional right of privacy in relation to personal data processed by a government entity as well as several other provisions that relate to privacy, it appears that GRAMA is rarely, if ever, considered a privacy protecting law as opposed to it being a law governing management of, and access to, government records. Similar in this respect to GRAMA, PRMA also has a limited connection to privacy due to the close inter-working relationship between PRMA and GRAMA. As such, legislative amendments to clarify and enhance the privacy focus of both laws are being proposed and will be discussed in more detail elsewhere in this report.

Second, even though GRAMA and PRMA are understood to subject state agencies to records management and access requirements, it appears as though state agencies are not fully compliant with every requirement. Further, it appears that many of the provisions that could be considered as relating to privacy, receive far less attention–compliance–from the agencies and their legal counsel. Thus, for GRAMA and PRMA to serve as an adequate privacy foundation, compliance with currently existing requirements must also be improved. Addressing these issues will be done through proposed legislative amendments.

Though there is no overarching comprehensive privacy law that has established standard privacy practice requirements across state agencies, state agencies are subject to GRAMA and PRMA, which, through minimal amendment, can serve as a foundation for standardizing state agencies' privacy practices. As such, it is recommended that the proposed legislative amendments attached to this report as Appendix A, be supported, as they have also received the support of the PPOC, SPO, and DGO executive leadership.

Synopsis:

Privacy Practice Assessment

- We assessed whether the privacy practices of state agencies could be reviewed in a standardized manner that would allow for clear reportable metrics, ongoing observations, and improvement of privacy maturity.

NIST Privacy Framework

- **ID.DE-P4:**
  Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.

Assessment #2 - 2022

KEY FINDINGS:

No overarching privacy law has established standard privacy practice requirements across state agencies, as such, a baseline determination of the maturity and adequacy of a state agency's privacy practices must be determined against established standards and best practices.

State agencies have adopted the NIST Cybersecurity Framework to assess security control maturity. The NIST Privacy Framework correlates with the Cybersecurity Framework and could be used to assess privacy practice maturity.

KEY DETERMINATIONS:

State agencies' privacy practices should be reviewed against accepted best practices and national standards. This allows for a standardized review that can be used across state agencies such that there can be appropriate comparisons made with measurable and observable metrics that can be tracked over time.

RISKS:

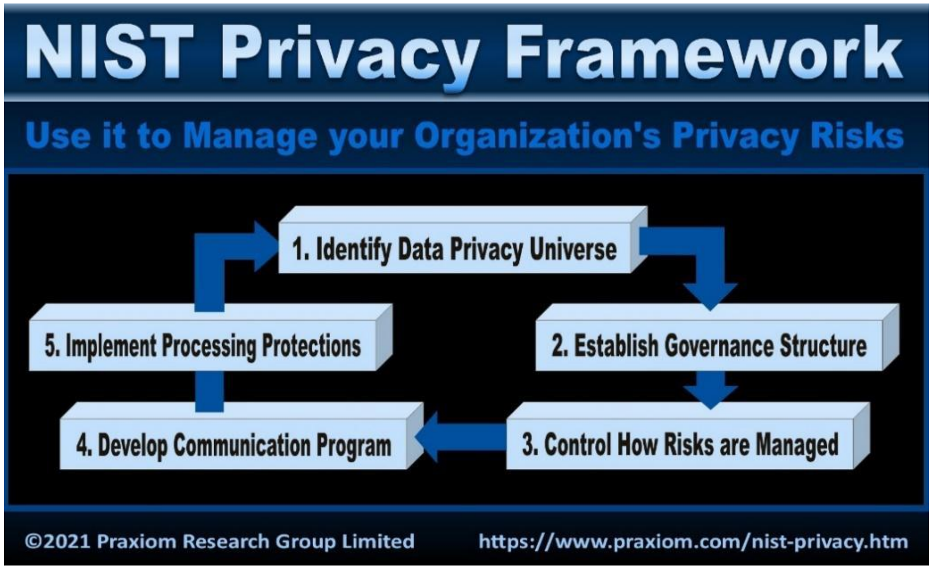
Not adopting or assessing privacy practices against an industry recognized privacy framework may result in difficulty creating and maintaining longitudinal privacy practice maturity metrics that are standardized across all state agencies.

KEY RECOMMENDATIONS:

Adoption of the NIST Privacy Framework by state agencies should be proposed to the executive state agencies' cabinet security council.

NIST Privacy Framework

Privacy practices should be reviewed against accepted best practices and national standards. This allows for standardized reviews that can be used across state agencies such that there can be appropriate comparisons made with measurable and observable metrics that can be tracked over time in addition to providing state agencies with a mechanism to identify and manage privacy risks. As there is no overarching privacy law that has established standard privacy practice requirements across state agencies, a baseline determination of the maturity and adequacy of a state agency's privacy practices must be determined against established standards. There is a certain amount of overlap between the concepts of security and privacy. The cybersecurity standards that the state adheres to are the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST SP 800-53 Rev. 5). The NIST Privacy Framework can be correlated with the NIST Cybersecurity Framework. As such, the NIST Privacy Framework is being used by the GOPO as an initial standard for the review and assessment of the privacy practices of state agencies because it is an accepted national standard, it allows for standardized reviews across state agencies, and it fits well with the standards that the state uses for its cybersecurity framework.


NIST Privacy Framework
Use it to Manage your Organization's Privacy Risks
1. Identify Data Privacy Universe
2. Establish Governance Structure
3. Control How Risks are Managed
4. Develop Communication Program
5. Implement Processing Protections
©2021 Praxiom Research Group Limited
https://www.praxiom.com/nist-privacy.htm

The NIST Privacy Framework is utilized internally by an entity to map legal requirements back to a categorized list of recognized privacy practices and controls, which enables privacy professionals to more easily identify gaps, set benchmarks, measure maturity, and prioritize privacy practices that require improvement. Correlating the NIST Privacy Framework with the NIST Cybersecurity Framework that the state has already adopted and implemented will allow for collection of reliable standard metrics that can be used to monitor and compare the maturity of the privacy practices of a state agency by all relevant stakeholders. To ensure that the privacy practices of state agencies adequately protect individual privacy rights, the GOPO recommends that adoption of the NIST Privacy Framework by state agencies be proposed to the Cabinet Security Council.

Synopsis:

Privacy Practice Assessment

- We assessed whether state agencies have established standard privacy risk assessment and risk management processes.

NIST Privacy Framework

- **GV.RM-P1:**
  Risk management processes are established, managed, and agreed to by organizational stakeholders.

Assessment #3 - 2022

KEY FINDINGS:

No standardized privacy risk assessment or privacy risk management processes have been adopted that apply uniformly across all state agencies.

Ad hoc privacy risk management processes have been implemented by agencies with applicable federal regulatory or contractual requirements.

RISKS:

Lack of standardized privacy risk assessment and management processes may result in unmitigated threats or risks to the constitutional privacy rights of individuals.

KEY RECOMMENDATIONS:

The GOPO should coordinate with state agencies to implement standardized privacy risk assessment and management processes that include inventory, threshold, assessment, and remediation.

Standardized Risk Assessment and Management Processes

The State's chief information security officer (CISO) recognized the importance of standardized risk assessment and management processes, and by way of a third-party governance, risk, and compliance software that assesses, manages, and provides insights related to application security—RSA Archer—implemented a standardized cybersecurity risk management process for state agency applications managed by DTS. Based on the recommendation from the GOPO that adequate privacy protection of PII requires state agencies to implement standardized privacy risk assessments and management processes, the CISO provided funding and support to expand RSA Archer by purchasing the RSA Data Governance and Privacy Program Management modules to account for privacy as well as cybersecurity. The GOPO is currently coordinating with state agencies to implement the privacy modules in a standardized format that will be designed to:

- Help state agencies identify and inventory PII.
- Help state agencies inventory PII processing activities.
- Help state agencies assess the privacy impacts and risks posed by PII processing activities.
- Enable state agencies to group processing activities for the purposes of performing privacy impact assessments.
- Enable state agencies to implement plans of action and milestones to manage and mitigate risks identified during assessments.
- Enable state agencies to view longitudinal metrics related to privacy practice maturity that can be presented from data stored in the RSA Archer system.

RSA Archer will be able to provide quantifiable and consumable metrics of the maturity of a state agency's privacy practices that can be refined appropriately depending on the nature of the audience. Such that the legislature can have access to the requisite information it finds desirable, as can the executives and leadership of a particular state agency, division, or program as appropriate. This will also allow for not only compliance with the requirement that the GOPO is to compile, maintain, and make public on the governor's website information about the privacy practices of state agencies, but will provide readily consumable, measurable, comparable, standardized, and therefore useful metrics and information.[7] Thereby facilitating greater transparency as well as greater understanding and involvement of stakeholders and the general public in addition to improving privacy protections of PII by giving state agencies the ability to monitor, address, and manage privacy risks.

Assessment #4 - 2022

Synopsis:

Privacy Practice Assessment

- We assessed whether state agencies have identified and inventoried all PII that they process.

NIST Privacy Framework

- **ID.IM-P1:** Systems/products/services that process data are inventoried.

KEY FINDINGS:

There is no requirement that a state agency identify and inventory all PII that it processes.

There is no standard definition of PII that state agencies can work from in determining whether a record is or contains PII.

KEY DETERMINATIONS:

State agencies should be required to identify inventory its record series that contain PII and to report that PII inventory to the GOPO. A standard definition of PII should be established for state agencies to determine what PII they process and where PII resides.

RISKS:

Lack of a complete PII inventory means that all PII processing may not be known or identified, and as such, there may be PII processes that are not assessed to determine and manage privacy related risks, resulting in unmitigated privacy risks.

KEY RECOMMENDATIONS:

The GOPO recommends that targeted amendments be made within GRAMA and PRMA to define PII and require identifying and inventorying records that are or contain PII.

Defining, Identifying, and Inventorying Personal Identifiable Information (PII)

A privacy framework is implemented in steps or phases. Several initial steps need to be taken to create a viable foundation for the privacy framework which can then be built upon and enhanced as appropriate over time. A core element of implementing a privacy framework is to identify what PII a state agency processes, which includes *where* the PII is processed—otherwise stated as having a PII inventory. This is a foundational necessity for adequate privacy protection. Where state agencies do not have a requirement to identify and inventory all PII they process, most state agencies have not done so, and thus they are not adequately protecting the privacy of PII. Proposed legislative amendments to GRAMA and PRMA seek to address this issue by requiring state agencies to denote each record series, record, or information within a record that is or contains PII, and report that PII Inventory to the GOPO.

State agencies are responsible for providing a multitude of services and functions which often requires the collection and use of an individual's personal information—PII—which may then subject the agencies to various state and federal laws and regulations that apply to the particular information gathered. Indeed, across the spectrum of applicable laws and regulations, state agencies are subject to numerous variations of terminology and definitions–which include varying data elements–for what may be understood as constituting personal identifying information. As such, it is not enough to merely direct state agencies to identify and inventory the PII they process, state agencies must also be told what data elements constitute PII for the purposes of identifying and inventorying PII.

Currently there is no specific federal or state law, regulation, rule, standard, or policy that provides all state agencies with a single definition of personal identifiable information that state agencies can work from to determine whether a record is or contains PII. There are many definitions of PII and similar terms and phrases within Utah code—such as "personal data," "identifying information," "confidential information," and "protected health information,"—that may apply to particular agencies in specific situations and circumstances. The wide degree of variation in such definitions, including what data variables are to be considered as identifiable, does not lend itself to being used by state agencies to make a standardized determination which would then facilitate a state agency to be able to maintain an accurate inventory of its PII. Adequate protection of privacy rights necessitates that state agencies have a definition or parameters to reference to determine whether data is considered personally identifiable information. As such, a recommended definition of PII has been proposed as an amendment to GRAMA.

Given the complexity of identifying all data variables that a state agency should consider as being identifiable of an individual, and thus as PII, which may depend on potential situations and circumstances in addition to the proposed definition includes a rulemaking requirement which will allow for broad input on the matter from the agencies that will be impacted, subject matter experts, stakeholders and the general public. This will allow for both completeness and transparency.

Synopsis:

Privacy Practice Assessment

- We assessed the adequacy of privacy governance in state agencies, including whether there are sufficient knowledgeable and trained personnel to implement and monitor a state agency’s privacy practices.

NIST Privacy Framework

- **GV.PO-P3:** Roles and responsibilities for the workforce are established with respect to privacy.
- **GV.AT-P3:** Privacy personnel understand their roles and responsibilities.

Assessment #5 - 2022

KEY FINDINGS:

There is no requirement that state employees be trained on specific privacy practices or have demonstrable privacy related knowledge, skills, or expertise–with the exception of certain agencies governed by federal regulation.

There is no requirement that state agencies designate an individual to act as a privacy officer who is responsible for managing, implementing, or administering privacy practices.

RISKS:

Implementation, management, and administration of a transparent and accountable privacy program requires that privacy professionals within agencies possess the privacy related knowledge, skills, and abilities (KSAs) required to perform those functions. The lack of said employees with privacy KSAs is a critical gap in the governance structure of state agencies and results in privacy practices being implemented in an ad hoc manner and to varying maturity levels across state agencies.

KEY RECOMMENDATIONS:

Each state agency should designate one or more privacy officers that are responsible for implementing, managing, and administering agency privacy practices.

The GOPO should provide standardized privacy training to designated privacy officers as well as a standard privacy training for all state employees.

Privacy Governance and the Need for Trained Knowledgeable Privacy Professionals

Another core element of a privacy framework and is thus essential for adequate privacy protections and practices, is a proper governance structure, which is critical to creating, implementing, and maintaining a privacy program that is both auditable and transparent. Adequate privacy governance structure is established through having trained, knowledgeable, privacy professionals with clear role designations and responsibilities. Under PRMA state agencies are required to appoint records officers to work with the Division of Archives and Records Services (DARS) in managing its records.[8] However, records officers are not privacy professionals, and given the substantial size and complexity of addressing the privacy practice needs of state agencies, the lack of knowledgeable privacy professionals poses a significant risk to individuals' right of privacy. This inadequacy may be addressed by requiring state agencies to appoint a privacy officer, akin to the requirement to appoint a records officer, with specific responsibilities and obligations. Legislative amendments to GRAMA and PRMA to address this issue have been proposed.

It is proposed that PRMA be amended to require the chief administrative officer of each state agency to designate a privacy officer who will work with the GOPO to implement privacy practices in alignment with best practices and the NIST Privacy Framework as well as implement and manage the state agency's privacy program. The privacy officer is ultimately responsible for ensuring that privacy interests are protected and that PII is managed responsibly within the agency. To ensure that the agency effectively carries out the privacy related functions described in law and State policies, the privacy officer must have agency-wide responsibility and accountability for the agency's privacy program with direct access to state agency leadership.

Certified Information Privacy Personnel Within State Agencies

Adequate privacy protection requires comprehensive privacy governance which in turn requires state agencies to have personnel in specific roles with pertinent knowledge and understanding. The GOPO is providing all state agencies the opportunity to have at least one employee trained and certified as a Certified Information Privacy Manager (CIPM), through the International Association of Privacy Professionals (IAPP). Having trained personnel will help to support each state agency's privacy maturity efforts and better prepare agencies for future privacy practice assessments and implementations. Each employee who participates receives two full days of instructor-led training as well as textbooks, participant guides, sample test questions, and exam vouchers. This training and certification will ensure each state agency has someone with the knowledge, skills, and abilities to facilitate:

- creating an agency privacy vision and structuring the agency privacy team
- developing, implementing, and managing an agency privacy program framework
- communicating to agency stakeholders
- measuring privacy performance

The first CIPM training occurred in June 2022, and a second CIPM training is scheduled to occur in November of 2022. Thirty government employees completed the first training, representing 16 different state agencies or divisions, and 6 non-state agencies. It is anticipated that an additional 10 more state agencies will participate in the Nov 2022 CIPM training. Proper designation of privacy officers and having trained employees is a metric that will be measured on an ongoing basis. This metric will be captured within the RSA Archer platform, discussed above, and thus can be reported to various audiences as appropriate.

Initial state agencies that participated in the June training include:	
Department of Agriculture and Food	Department of Health and Human Services - ORS
Department of Commerce	Department of Public Safety
Department of Environmental Quality	Department of Transportation
Department of Financial Institutions	Department of Veteran and Military Affairs
Department of Government Operations	Department of Workforce Services
Department of Health and Human Services	Governor's Office of Economic Opportunity
Department of Health and Human Services - State Hospital	Utah Labor Commission
Department of Health and Human Services - DCFS	Utah State Tax Commission

State Agency Privacy Council

Many state agencies will be implementing privacy programs from inception and, at least initially, will do so with a dearth of experienced personnel. To provide additional support to state agencies in implementing and improving privacy practices, the GOPO has established a state agency privacy council that includes a privacy representative of each state agency and the state archivist and is chaired by the GOPO. The privacy council meets monthly and provides an opportunity for the GOPO to provide the privacy representatives with additional training. The meeting also provides an opportunity for agency representatives to pose questions and work through issues in a congenial atmosphere as part of a privacy team. The privacy council will routinely review state agencies’ privacy practices and policies to identify common opportunities for improvement. The privacy council works to strengthen state agency’s privacy practices to ensure that the practices adequately reflect the laws, policies, goals, and values of the State. The privacy council is also a forum in which training and education materials prepared by the PPOC–as required by Utah Code § 63C-23-202–may be disseminated to state agencies.

State Agency Privacy Awareness Training to All Employees

All State employees must annually complete the statewide security training. The GOPO reviewed the security training and found that it did not adequately instruct employees with respect to privacy obligations, risks, and overall importance. The GOPO, working with the requisite personnel within DGO/DTS, determined that given the interconnected relationship of security and privacy, the security training could feasibly be updated to effectively provide both privacy and security training in one module without being overly-long or unduly burdensome. The privacy training will increase employees' overall awareness of the value that personal data represents and thus the risks associated through mismanagement, loss, or theft of such data. The training will elucidate the employees’ responsibilities with respect to personal data, which includes the responsibility to be familiar with the applicable laws and regulations, limitations on uses, potential civil and criminal ramifications that can apply to data misuse, etc. Because of the training’s required audience, it represents an opportunity to reach a large swathe of state employees and to begin establishing key privacy tenets across state agencies.

Synopsis:

Privacy Practice Assessment

- We assessed a subset of technical security controls to determine whether IT systems have adequate encryption mechanisms implemented.

NIST Privacy Framework

- **PR.DS-P1:**
  Data-at-rest are protected.
- **PR.DS-P2:**
  Data-in-transit are protected.
- **ID.IM-P1**:
  Systems/ products/services that process data are inventoried.

Assessment #6 - 2022

KEY FINDINGS:

DTS has adopted a standard process of implementing disk encryption on all DTS administered computers (desktops and laptops).

There is no definitive inventory of all websites on which PII may be processed which inhibits DTS' ability to automate encryption monitoring.

There is no single statewide requirement that all PII be processed in an encrypted format, though the practice is to do so.

RISKS:

Encryption of PII at-rest and in-transit are foundational technical controls used to maintain the confidentiality of the data. Lack of encryption during PII processing may leave data susceptible to unauthorized access by different threat actors.

RECOMMENDATIONS:

The CISO and GOPO should propose a policy to the Cabinet Security Council that:

state agencies be required to maintain an inventory of websites and applications that process PII; and

state agencies be required to implement encryption mechanisms on all electronic PII processes.

Encryption

State agencies may use computers or websites to process PII. State agencies should have an inventory of PII processes that can be assessed to ensure appropriate controls are implemented, i.e., encryption.

Computer Encryption

DTS has implemented automated mechanisms to track and report on the encryption status of computers that are administered by DTS. As of September 8th, 2022, DTS administered 20,194 devices.[9] Of those devices, 17,637 (87.34%) had disk level encryption implemented and 2557 (12.66%) did not. It is now DTS' standard practice to implement disk level encryption on all computers being deployed for use and to monitor the encryption status. Computers that are unencrypted are older computers that were deployed prior to the established encryption practice and must be in secured locations until they are able to be replaced—which will increase the percentage of encrypted computers in use. It is not known how many of the computers process PII, as this is not currently tracked.

Website Encryption

DTS' standards require adequate encryption on all publicly accessible state agency websites in addition to automated scanning of those websites for vulnerability management.[10] As of September 8th, 2022, DTS has an inventory of 1,100 websites which are scanned. Of the inventoried websites, 752 (68.4%) have strict transport security enforced, meaning the applications adequately prevent users from connecting to it over unencrypted connections. Whereas 348 (31.6%) of the websites do not have strict transport security enforced, such that a user may transmit data with the website via either encrypted or unencrypted mechanisms. Of the inventoried websites, 104 (9.5%) are implemented with no encryption, such that users transmit data with the website via unencrypted mechanisms. How many of these websites process PII is unknown, so it is not currently possible to determine the risk to individuals' privacy rights.

Inventory Requirement and Encryption Policy

DTS and state agencies maintain multiple inventories of IT systems and processing activities, these inventories are often disparate and incomplete due to the shared responsibilities. Lack of complete inventories is prohibitive of ensuring that adequate controls are in place. Thus, it is recommended that state agencies be required to maintain a complete inventory of websites that may process PII so that adequacy of controls can be assessed. State agencies and DTS have made substantial progress implementing encryption mechanisms for non-public PII data at-rest and in-transit even though not explicitly required to do so. Thus, it is recommended that all state agencies be required to encrypt PII at-rest and in-transit on all electronic processes, with allowance for exceptions or alternate mitigations to be approvable via appropriate risk management processes.

Synopsis:

Public Individual’s Request for a Privacy Practice Assessment

- We assessed the adequacy of notice, use, and consent language in the DHHS-OVRS form Parent’s Worksheet to Register Birth Information.

NIST Privacy Framework

- **CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals’ data processing preferences and requests are established and in place.

Assessment #7 - 2022

KEY FINDINGS:

The Parent’s Worksheet to Register Birth Information did not fully inform the data subject of the purposes for which each piece of information was requested, whether the requested information was required for the provision of the requisite government services or whether provision of the information was optional, or whether there were consequences for refusing to provide the information.[11]

RISKS:

Recognized information practice principles establish that the collection of personal information should be obtained with the knowledge and consent of the individual; the purposes for the collection of the information should be disclosed before collection of the information; collected information should be limited to only what is necessary for the specified purposes; and information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or by legal authority. Failure to adhere to these information practice principles poses risks to the individual’s right of privacy as well as legal and reputational risks to the entity.[12]

RECOMMENDATIONS:

The worksheet should be updated to make clear which requested information is required and which is optional and identify the intended purposes for which the information is being requested.

The worksheet should be reviewed and, where possible, information fields removed that are not germane to the provision of the intended government services.

Analyze and Respond to Requests from Individuals for the Review of a State Agency's Privacy Practice

The GOPO is statutorily directed to implement a process to analyze and respond to requests from individuals for the GOPO to review a state agency’s privacy practice.[13] While this has been accomplished in an ad hoc manner thus far, a website (www.privacy.utah.gov) has been reserved for development to address this issue by providing a formalized and easily accessible manner for the public to make such a request in the future.

The GOPO addressed an ad hoc request from the public for the review of a state agency’s privacy practice during the fall/winter of 2021. A member of the public reached out to the Utah Department of Health, the Utah Attorney General’s Office, elected representatives, and the media to express their concerns about a form from the Office of Vital Records and Statistics that she had been required to complete.[14] She was concerned about the amount of personal information that was requested as well as how that information was used and who it was shared with. The issue was the impetus of significant media coverage. The form at issue was the OVRS Parent’s Worksheet to Register Birth Information. The GOPO was able to work with all relevant stakeholders to address what information was requested, to specify what information was required, what purposes the information was used for, and who the information was shared with.

Utah birth certificates withheld in exchange for personal information

by Heidi Hatch, KUTV | Monday, November 15th 2021

The form requires certain information so that a birth certificate can be created for the child as well as help parents with the SSN, driver license, and passport processes. Additionally, the form requested information that was very beneficial for maternal and newborn mortality and morbidity research. DHHS has implemented the recommendations above and the form now provides the requisite information necessary for people to be informed and be able to make a conscientious decision about what information they provide to the government and how that information is used in a transparent manner. For reference and comparisons, a copy of the current version of the form is attached to this report as Appendix B, and a copy of the previous version of the form is attached as Appendix C.

State Agency Engagement

Privacy Practices:

State agencies are already showing their recognition of the importance of prioritizing privacy practices and the assistance of the GOPO to assist in making improvements to their privacy practices. The creation of the state agency privacy council and training of privacy officers is resulting in a cultural shift in which State agencies are proactively engaging in steps to implement privacy by design principles in new and upcoming projects and programs. State agencies have been especially proactive in seeking to work with the GOPO to ensure privacy considerations are accounted for in upcoming projects that may impact the processing of large amounts of personal data. Thus, in addition to reviewing and analyzing privacy practices that the GOPO has selected, the GOPO is being invited by agencies to review particular practices and programs that are under development or just getting underway.

Below are a subset of engagements that state agencies have initiated to ensure privacy is properly considered:

Department of Corrections – Prison Visitor Body Scans
Tax Commission and Department of Motor Vehicles – Vanity License Plates
Tax Commission and State Treasurer – Sharing of data for the Unclaimed Property Program
Utah Department of Transportation – RUC Program
Utah Department of Transportation – High Occupancy Vehicle Lane License Plate Review

Proposed Legislative Amendments

As directed by Utah Code § 67-1-17, the GOPO, working in conjunction with, and the support and approval of, the PPOC, the SPO, the state archivist, the CISO and state's chief information officer[15], and the executives of DGO, has formulated several proposed legislative amendments that will strengthen the privacy provisions of GRAMA and PRMA to form a foundation for improving the privacy practices of state agencies to better protect all Utahns' constitutional right of privacy. The proposed legislative amendment language is attached hereto as Appendix A. A general synopsis of the proposed amendments include:

- Amend Utah Code § 63A-12-100 *et seq.*, to require the chief administrative officer of a state agency to appoint a privacy officer to address privacy related obligations and responsibilities including denoting whether a record series of a state agency contains PII and to report an inventory of record series containing PII to the GOPO. Also requires the chief administrative officer to appoint a security officer to work with the chief information security officer for the cybersecurity of the agency.

- Amend Utah Code § 63A-12-100 *et seq.*, to require the executive director of the DGO with the recommendation of the state archivist and consultation of the GOPO, to establish in rule a list of all data variables that must be considered PII for purposes of denoting PII and for reporting a PII inventory to the GOPO.

- Amend Utah Code § 63G-2-100 *et seq.*, to provide additional definitions including a definition of PII and require governmental entities to designate and classify a record series containing PII prior to implementation. Adds elements to the requirement to file a purpose statement with state archives, additions include whether the record series will contain PII, purposes and authorities, and provision of notice to the individual of the record series which the PII will be a part of.

- Amend Utah Code § 67-1-17 to change the title of the government operations privacy officer to the chief privacy officer (CPO) in order to alleviate some of the confusion caused by the various titles and provide rulemaking authority to the CPO to standardize privacy practices of state agencies into comprehensive privacy programs.

Appendices

Appendix A: Proposed Legislative Amendments
Appendix B: Current version of OVRS - Parent's Worksheet to Register Birth Information
Appendix C: Past version of OVRS - Parent's Worksheet to Register Birth Information
Appendix D: NIST Privacy Framework Controls

[1] GRAMA does not define "personal data."

[2] Utah Code § 67-1-17(1)(b) provides the definition of personal data to mean any information relating to an identified or identifiable individual and includes personally identifying information.

[3] Utah Code § 67-1-17(1)(c) defines privacy practice to mean the acquisition, use, storage, or disposal of personal data and includes a technology use related to personal data; and policies related to the protection, storage, sharing, and retention of personal data.

[4] Utah Code § 67-1-17(1)(d) defines state agency, in part, as an entity that is under the direct supervision and control of the governor or the lieutenant governor.

[5] Utah Code § 67-1-17(4)(b)

[6] A copy of the NIST Privacy Framework Core Version 1.0 has been attached to this report as Appendix D. Accessed online at https://www.nist.gov/privacy-framework

[7] Utah Code § 67-1-17(3)(a) and (b)

[8] Utah Code § 63A-12-103

[9] This includes Windows desktop, Windows laptop, and macOS devices.

[10] https://dts.utah.gov/standard/web-https-only-standard

[11] See Utah Code § 63G-2-601

[12] See Organization for Economic Cooperation and Development (OECD) Privacy Framework 2013, Basic Principles of National Application. Accessed at: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[13] Utah Code § 67-1-17(3)(d)

[14] "Utah birth certificates withheld in exchange for personal information," by Heidi Hatch, KUTV, 11/15/2021. Link: https://kutv.com/news/2news-investigates/utah-birth-certificates-held-hostage-in-exchange-for-personal-information
Legislature interim committee PDF version of above KUTV article, link: https://le.utah.gov/interim/2022/pdf/00001983.pdf
"Where does the personal information given for a Utah birth certificate go?" by Heidi Hatch, KUTV, 11/16/2021. Link: https://kutv.com/news/2news-investigates/where-does-the-personal-information-given-for-a-utah-birth-certificate-go
Leslie Corbly: Utah's Department of Health survey shows institutional failures, Opinion, Salt Lake Tribune, 12/9/21
https://www.sltrib.com/opinion/commentary/2021/12/09/leslie-corbly-utahs/

[15] Utah Code § 63A-16-201

Appendix A

Proposed Legislative Amendments for Privacy Practices

DRAFT—
Proposed Legislative Amendments
2023 General Session

AMENDS:

- Amends UCA § 63A-12-100 *et seq.* To require the chief administrative officer of a state agency to appoint a privacy officer to address privacy related obligations and responsibilities including denoting whether a record series of a state agency contains personal identifiable information (PII) and to report an inventory of record series containing PII to the chief privacy officer. Also requires the chief administrative officer to appoint a security officer to work with the chief information security officer for the cybersecurity of the agency.

- Amends UCA § 63A-12-100 *et seq.* to require the executive director of the department with the recommendation of the state archivist and consultation of the chief privacy officer, to establish in rule a list of all data variables that must be considered PII for purposes of denoting PII and for reporting a PII inventory to the chief privacy officer.

- Amends UCA § 63G-2-100 *et seq.* to provide additional definitions including a definition of personal identifiable information and requires governmental entities to designate and classify a record series containing PII prior to implementation.

- Amends UCA § 67-1-17 to change the title of the government operations privacy officer to the chief privacy officer.

UCA § 63A-12-100. Division of Archives and Records Services.

UCA § 63A-12-100. Title.

This chapter is known as the "Division of Archives and Records Service~~.~~," or as the “Public Records Management Act.”

UCA § 63A-12-100.5. Definitions.

1) Except as provided under Subsection (2), the definitions in Section 63G-2-103 apply to this chapter.
2) As used in this chapter:
    a) "division" or "state archives" means the Division of Archives and Records Service; and
    b) “privacy practice” means the same as that term is defined in Subsection 67-1-17(1)(c); and
    c) "record" means:
        i) the same as that term is defined in Section 63G-2-103; or
        ii) a video or audio recording of an interview, or a transcript of the video or audio recording, that is conducted at a Children's Justice Center established under Section 67-5b-102, the release of which is governed by Section 77-37-4.

63A-12-101 Division of Archives and Records Service created -- Duties.

1) There is created the Division of Archives and Records Service within the department.
2) The state archives shall:
    a) administer the state's archives and records management programs, including storage of records, central reformatting programs, and quality control;
    b) apply fair, efficient, and economical management methods to the collection, creation, use, maintenance, retention, preservation, disclosure, and disposal of records and documents;
    c) establish standards, procedures, and techniques for the effective management and physical care of records;
    d) conduct surveys of office operations and recommend improvements in current records management practices, including the use of space, equipment, automation, and supplies used in creating, maintaining, storing, and servicing records;
    e) establish standards for the preparation of schedules providing for the retention of records of continuing value and for the prompt and orderly disposal of state records no longer possessing sufficient administrative, historical, legal, or fiscal value to warrant further retention;
    f) establish, maintain, and operate centralized reformatting facilities and quality control for the state;
    g) provide staff and support services to the Records Management Committee created in Section 63A-12-112 and the State Records Committee created in Section 63G-2-501;
    h) develop training programs to assist records officers and other interested officers and employees of governmental entities to administer this chapter and Title 63G, Chapter 2, Government Records Access and Management Act;
    i) provide access to public records deposited in the archives;
    j) administer and maintain the Utah Public Notice Website established under Section 63A-16-601;
    k) provide assistance to any governmental entity in administering this chapter and Title 63G, Chapter 2, Government Records Access and Management Act;
    l) prepare forms for use by all governmental entities for a person requesting access to a record; and
    m) if the department operates the Division of Archives and Records Service as an internal service fund agency in accordance with Section 63A-1-109.5, submit to the Rate Committee established in Section 63A-1-114:
        i) the proposed rate and fee schedule as required by Section 63A-1-114; and
        ii) other information or analysis requested by the Rate Committee.
3) The state archives may:
    a) establish a report and directives management program; and
    b) establish a forms management program.

4) (4)
   - a) (a) As used in this Subsection (4):
     - i) (i) "Vulnerable records and data" means records and data regarding national security interests; care, custody, or control of children; fiduciary trust over money; health care to children or vulnerable adults; or the provision of care, protection, food, shelter, clothing, or assistance with the activities of daily living or financial resource management to vulnerable adults.
   - b) (b) The division may require that a current or potential employee or volunteer who applies for or holds a position with direct access to vulnerable records and data:
     - i) (i) submit a fingerprint card in a form acceptable to the division;
     - ii) (ii) consent to a criminal background check by:
       - (A) the Federal Bureau of Investigation;
       - (B) the Utah Bureau of Criminal Identification; or
       - (C) another agency of any state that performs criminal background checks.
   - c) (c) The Bureau of Criminal Identification shall provide all the results from the state, regional, and nationwide criminal history background checks to the division.
   - d) (d) The division is responsible for the payment of all fees required by Subsection 53-10-108(15) and any fees required to be submitted to the Federal Bureau of Investigation by the bureau.
   - e) (e) The division may, in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, adopt rules to implement this section.

5) ~~(4)~~(5) The executive director may direct the state archives to administer other functions or services consistent with this chapter and Title 63G, Chapter 2, Government Records Access and Management Act.

UCA § 63A-12-103. Duties of governmental entities.

1) The chief administrative officer of each governmental entity shall:
   - a) establish and maintain an active, continuing program for the economical and efficient management of the governmental entity's records as provided by this chapter and Title 63G, Chapter 2, Government Records Access and Management Act;
   - b) appoint one or more records officers who will be trained to work with the state archives in the care, maintenance, scheduling, disposal, classification, designation, access, privacy, and preservation of records;
   - c) ensure that officers and employees of the governmental entity that receive or process records requests receive required training on the procedures and

requirements of this chapter and Title 63G, Chapter 2, Government Records Access and Management Act;

d) make and maintain adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the governmental entity designed to furnish information to protect the legal and financial rights of persons directly affected by the entity's activities;

e) submit to the state archivist proposed schedules of records for final approval by the Records Management Committee created in Section 63A-12-112;

f) cooperate with the state archivist in conducting surveys made by the state archivist;

g) comply with rules issued by the Department of Government Operations as provided by Section 63A-12-104;

h) report to the state archives the designation of record series that it maintains;

i) report to the state archives the classification of each record series that is classified; ~~and~~

j) establish and report to the state archives retention schedules for objects that the governmental entity determines are not defined as a record under Section 63G-2-103, but that have historical or evidentiary value; and

2) The chief administrative officer of each state agency as defined in Section 67-1-17 shall:

a) appoint one or more privacy officers who will be trained to work with the chief privacy officer, created in Section 67-1-17, to establish and implement best practices with respect to government privacy practices;

i) the records officer appointed under Subsection (1)(b), the privacy officer appointed under Subsection (2)(a), and the security officer appointed under Subsection (3)(a) may be the same person if the requirements and obligations of the officers as established under this Chapter can be appropriately fulfilled; and

ii) the time commitments and job duties are able to be adequately carried out by the same individual, where applicable.

b) report to the state archives the denotation of each record series, record, or information within a record that is or contains personal identifiable information;

c) report to the chief privacy officer a personal identifiable information inventory based on the denotation of personal identifiable information as established in Subsection (2)(b) and in accordance with the rules for such inventory as provided in Subsection 63A-12-104(2).

3) The chief administrative officer of each executive branch agency subject to Title 63A, Chapter 16, Part 2, the Utah Technology Governance Act, shall:

a) appoint one or more security officers who will be trained to work with the chief information security officer created in Section 63A-16-210, to assess, coordinate, and manage cybersecurity of the agency.

UCA § 63A-12-104. Rulemaking authority.

1) The executive director of the department, with the recommendation of the state archivist, may make rules as provided by Title 63G, Chapter 3, Utah Administrative Rulemaking Act, to implement provisions of this chapter and Title 63G, Chapter 2, Government Records Access and Management Act, dealing with procedures for the collection,

storage, designation, classification, denotation, access, mediation for records access, and management of records.

2) The executive director of the department, with the recommendation of the state archivist and with the consultation of the chief privacy officer, shall make rules as provided by Title 63G, Chapter 3, Utah Administrative Rulemaking Act, to provide a non-exclusive list of data variables that a state agency as defined in Section 67-1-17(1)(d), shall consider as being personal identifiable information for purposes of:
   a) denoting whether a record series contains personal identifiable information as provided in Subsection 63A-12-103(2)(b); and
   b) establishing, maintaining, and reporting the personal identifiable information inventory as provided in Subsection 63A-12-103(2)(c).
3) The rule establishing the list of data variables mandated in Subsection (2), may point to an official form data dictionary maintained by the department and accessible on the department's website.
4) The official form data dictionary provided for in Subsection (3) shall be maintained and kept up to date.
5) A governmental entity that includes divisions, boards, departments, committees, commissions, or other subparts that fall within the definition of a governmental entity under this chapter, may, by rule, specify at which level the requirements specified in this chapter shall be undertaken.

UCA § 63A-12-108. Inspection and summary of record series.

The state archives shall provide for public inspection of the title and a summary description of each record series and whether the record series contains personal identifiable information.

UCA § 63G-2-101. Government Records Access and Management Act.

UCA § 63G-2-103. Definitions.

As used in this chapter:

…

(*) "Chief privacy officer" means the person appointed in accordance with Subsection 67-1-17(2).

…

(*) "Denote," "denoting," and their derivative forms mean determining whether a record series, record, or information within a record is or contains personal identifiable information based on a governmental entity's review of a record series.

…

(*) "Distinguish" means to identify an individual.

…

(*) "Identifier" means a data element/variable that is considered to be personally identifiable information…

…

(*) "Linkable information" means information about or related to an individual for which there is a possibility of logical association with other information about the individual.

(*) "Linked information" means information about or related to an individual that is logically associated with other information about the individual.

…

(*) “Personal identifiable information” or “PII” means any information about an individual, collected or maintained by or on behalf of a governmental entity that can be used to distinguish or trace an individual’s identity and any other information that is linked or linkable to an individual.

a) Personal Identifiable Information, as defined in this Chapter, applies to a state agency, as defined in Subsection 67-1-17(1)(d), for purposes of:
   i) denoting whether a record series contains personal identifiable information as provided in Subsection 63A-12-103(2)(b);
   ii) establishing, maintaining, and reporting the personal identifiable information inventory as provided in Subsection 63A-12-103(2)(c); and
   iii) establishing and implementing best practices with respect to government privacy practices in conjunction with the chief privacy officer as provided in Subsection 63A-12-103(2)(a).

b) The data variables that a state agency shall consider as being an identifier that would make data personal identifiable information shall be established in administrative rule pursuant to Section 63A-12-104.

c) Personal Identifiable Information, as defined in this Chapter applies to a state agency as defined in Subsection 67-1-17(1)(d), unless:
   i) the definition is inconsistent with the manifest intent of the Legislature or repugnant to the context of the statute; or
   ii) a different definition is expressly provided for the respective title, chapter, part, section, or subsection; or
   iii) a different definition is expressly provided for by governing federal law or regulation.

(*) “Personal identifiable information inventory” or “PII inventory” means the inventory of personal identifiable information reported to the chief privacy officer in accordance with Subsection 63A-12-103(2)(c).

…

(*) “Privacy officer” means the individual appointed by the chief administrative officer of each state agency pursuant to Subsection 63A-12-103(2).

…

(*) “Privacy practice” means the same as that term is defined in Subsection 67-1-17(1)(c);

…

(*) “Trace” means to process sufficient information to make a determination about a specific aspect of an individual’s activities or status.

…

UCA § 63G-2-107. Disclosure of records subject to federal law.

1) Notwithstanding Subsection 63G-2-201(6), this chapter does not apply to the disclosure of a record containing protected health information as defined in 45 C.F.R., Part 164, Standards for Privacy of Individually Identifiable Health Information, if the record is:
   a) controlled or maintained by a governmental entity; and
   b) governed by 45 C.F.R., Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information.

2) The disclosure of an education record as defined in the Family Educational Rights and Privacy Act, 34 C.F.R. Part 99, that is controlled or maintained by a governmental entity shall be governed by the Family Educational Rights and Privacy Act, 34 C.F.R. Part 99.

UCA § 63G-2-307. Duty to evaluate records and make denotations, designations, and classifications.

1) A governmental entity shall:
   a) evaluate all record series that it uses or creates;
   b) designate those record series as provided by this chapter and Title 63A, Chapter 12, Division of Archives and Records Service; ~~and~~
   c) report the designations of its record series to the state archives~~.~~; and
   d) denote a particular record series, record, or information within a record that will or may contain data variables that are considered identifiers that would make information personally identifiable as provided in administrative rule pursuant to Subsection 63A-12-104(2).
2) If ~~A governmental entity may classify~~ a particular record, record series, or information within a record is not or does not contain personal identifiable information, a governmental entity may classify the particular record, record series, or information within a record at any time, but is not required to classify a particular record, record series, or information until access to the record is requested.
3) A governmental entity may redesignate a record series or reclassify a record or record series, or information within a record at any time.
4) A governmental entity shall denote a particular record, record series, or information within a record that will or may contain personal identifiable information prior to the collection of any personal identifiable information.

Part 6 - Collection of Information and Accuracy of Records

UCA § 63G-2-601. Rights of individuals on whom data is maintained -- Classification statement -- Notice to provider of information.

(1) (a) Each governmental entity shall file with the state archivist a statement explaining the purposes for which a record series that is designated as private or controlled or that otherwise contains personal identifiable information is collected and used by that governmental entity.

(b) The statement filed under Subsection (1)(a) shall plainly state the purposes for which the record series is collected and used by that governmental entity and shall include the specific corresponding authority that mandates, calls or allows for the collection of personal identifiable information.

(c) The statement filed under Subsection (1)(a) is a public record.

(d) The requirements of this Subsection (601)(1) are applicable to a record series that may otherwise be exempt from requirements of this Act due to being subject to HIPAA or FERPA as provided in Section 63G-2-107 or as provided in Subsection 63G-2-201(6) where disclosure of a record is governed by other statute, rule, or regulation.

(2) (a) A governmental entity shall provide notice of the following to a person that is asked to furnish information that could be classified as a private or controlled record:

(i) the record series which the information is a part of;

(ii) the reasons the person is asked to furnish the information;

(iii) the intended uses of the information;

(iv) the consequences for refusing to provide the information; and

(v) the classes of persons and the governmental entities that currently:

(A) share the information with the governmental entity; or

(B) receive the information from the governmental entity on a regular or contractual basis.

(b) The notice shall be:

(i) posted in a prominent place at all locations where the governmental entity collects the information; or

(ii) included as part of the documents or forms that are used by the governmental entity to collect the information.

(3) Upon request, each governmental entity shall explain to a person:

(a) the reasons the person is asked to furnish information that could be classified as a private or controlled record;

(b) the intended uses of the information referred to in Subsection (3)(a);

(c) the consequences for refusing to provide the information referred to in Subsection (3)(a); and

(d) the reasons and circumstances under which the information referred to in Subsection (3)(a) may be shared with or provided to other persons or governmental entities.

(4) A governmental entity may use private or controlled records only for those purposes:

(a) given in the statement filed with the state archivist under Subsection (1); or

(b) for which another governmental entity may use the record under Section 63G-2-206.

UCA § 63G-2-604. Retention and disposition of records.

(1) (a) Except for a governmental entity that is permitted to maintain the governmental entity's own retention schedules under Part 7, Applicability to Political Subdivisions, the Judiciary, and the Legislature, each governmental entity shall file with the Records Management Committee created in Section 63A-12-112 a proposed schedule for the retention and disposition of each type of material that is defined as a record under this chapter.

(b) After a retention schedule is reviewed and approved by the Records Management Committee under Subsection 63A-12-113(1)(b), the governmental entity shall maintain and destroy records in accordance with the retention schedule.

(c) If a governmental entity subject to the provisions of this section has not received an approved retention schedule from the Records Management Committee for a specific type of material that is ~~classified~~defined as a record under this chapter, the model retention schedule maintained by the state archivist shall govern the retention and destruction of that type of material.

(2) A retention schedule that is filed with or approved by the Records Management Committee under the requirements of this section is a public record.

UCA § 67-1-17. Government operations privacy officer.

1) As used in this section:
   a) "Independent entity" means the same as that term is defined in Section 63E-1-102.
   b) (i) "Personal data" means any information relating to an identified or identifiable individual.
      (ii) "Personal data" includes personally identifying information.

   c) (i) "Privacy practice" means the acquisition, use, storage, or disposal of personal data.
      (ii) "Privacy practice" includes:
         (A) a technology use related to personal data; and
         (B) policies related to the protection, storage, sharing, and retention of personal data.
   d) (i) "State agency" means the following entities that are under the direct supervision and control of the governor or the lieutenant governor:
         (A) a department;
         (B) a commission;
         (C) a board;
         (D) a council;
         (E) an institution;
         (F) an officer;
         (G) a corporation;
         (H) a fund;
         (I) a division;
         (J) an office;
         (K) a committee;
         (L) an authority;
         (M) a laboratory;
         (N) a library;
         (O) a bureau;
         (P) a panel;
         (Q) another administrative unit of the state; or
         (R) an agent of an entity described in Subsections (A) through (Q).
      ii) "State agency" does not include:
         (A) the legislative branch;
         (B) the judicial branch;
         (C) an executive branch agency within the Office of the Attorney General, the state auditor, the state treasurer, or the State Board of Education; or
         (D) an independent entity.
2) The governor ~~may~~shall, with the advice and consent of the Senate, appoint a ~~government operations privacy officer~~ chief privacy officer.
3) The ~~government operations privacy officer~~ chief privacy officer shall:
   a) compile information about the privacy practices of state agencies;
   b) make public and maintain information about the privacy practices of state agencies on the governor's website;
   c) provide state agencies with educational and training materials developed by the Personal Privacy Oversight Commission established in Section 63C-24-201 that include the information described in Subsection 63C-24-202(1)(b);
   d) implement a process to analyze and respond to requests from individuals for the ~~government operations privacy officer~~ chief privacy officer to review a state agency's privacy practice;

e) identify annually which state agencies' privacy practices pose the greatest risk to individual privacy and prioritize those privacy practices for review;

f) review each year, in as timely a manner as possible, the privacy practices that the ~~government operations privacy officer~~ chief privacy officer identifies under Subsection (3)(d) or (e) as posing the greatest risk to individuals' privacy;

g) when reviewing a state agency's privacy practice under Subsection (3)(f), analyze:

i) details about the privacy practice;

ii) information about the type of data being used;

iii) information about how the data is obtained, shared, secured, stored, and disposed;

iv) information about with which persons the state agency shares the information;

v) information about whether an individual can or should be able to opt out of the retention and sharing of the individual's data;

vi) information about how the state agency de-identifies or anonymizes data;

vii) a determination about the existence of alternative technology or improved practices to protect privacy; and

viii) a finding of whether the state agency's current privacy practice adequately protects individual privacy; and

h) after completing a review described in Subsections (3)(f) and (g), determine:

i) each state agency's use of personal data, including the state agency's practices regarding data:

(A) acquisition;

(B) storage;

(C) disposal;

(D) protection; and

(E) sharing;

ii) the adequacy of the state agency's practices in each of the areas described in Subsection (3)(h)(i); and

iii) for each of the areas described in Subsection (3)(h)(i) that the ~~government operations privacy officer~~ chief privacy officer determines require reform, provide recommendations to the state agency for reform.

4) The ~~government operations privacy officer~~ chief privacy officer shall:

a) quarterly report, to the Personal Privacy Oversight Commission:

i) recommendations for privacy practices for the commission to review; and

ii) the information described in Subsection (3)(h); and

b) annually, on or before October 1, report to the Judiciary Interim Committee:

i) the results of any reviews described in Subsection (3)(g), if any reviews have been completed;

ii) reforms, to the extent that the ~~government operations privacy officer~~ chief privacy officer is aware of any reforms, that the state agency made in response to any reviews described in Subsection (3)(g);

iii) the information described in Subsection (3)(h); and

iv) recommendations for legislation based on the results of any reviews described in Subsection (3)(g).

5) The chief privacy officer may, by rule made in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act:

a) provide standards that impose requirements on state agencies that:

i) are related to the state agency’s privacy practices; and

ii) establish standards for determining when a state agency’s privacy practices in each of the areas described in Subsection (3)(h) are not adequate and require reform.

b) establish training for privacy officers, created in Subsection 63A-12-103(2), to work with the chief privacy officer, created in Section 67-1-17, to establish and implement best practices with respect to government privacy practices.

Appendix B

Current OVRS Parent Worksheet to Register Birth Information

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: ______________________________

17. OPTIONAL
If you need your child's social security card mailed in care of someone else please indicate the name and address. 30

Mail Person's Name: ______________________________

Street Address or PO Box: ______________________________

City/Town or Location: ____________ U.S. State: ____________Zip: ____________

18. OPTIONAL
What would Parent 2 like to be known as on the child's birth certificate? (If not indicated, default is Father) 36

○ Mother ○ Father ○ Parent (female) ○ Parent(male)

19. REQUIRED
What is Parent 2's current legal name? 37

First Name(s): ______________________________

Middle Name(s): ______________________________

Last Name(s): ______________________________ Suffix (Jr. Sr. etc): ____________

20. OPTIONAL
What was Parent 2's name prior to first marriage? (Name as it appears on the current birth certificate) 38

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): ____________

21. REQUIRED
What is Parent 2's date of birth? 39

mm/dd/yyyy: ____________

22. OPTIONAL 40
Please provide a phone number where we can reach you if we have questions about any of the information provided.

Parent 2 Phone Number: ______________________________

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 <u>for themselves</u> 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): __________________

Appendix C

Past OVRS Parent Worksheet to Register Birth Information

Parent's Worksheet to Register Birth Information

The information gathered on this worksheet will be used to register information for your child's birth certificate and to apply for your child's Social Security Card.

Use of Birth Registration Information from this worksheet:

The information you enter here is REQUIRED to register your child's birth information and create your child's Birth Certificate.

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

Complete, Accurate and Readable information on this worksheet is very important. It must be registered within 10 days of birth.

In addition to legal information, data gathered here will be used by health researchers to study and improve the health of mothers and newborn infants. This information will not appear on the birth certificate.

State laws protect against the unauthorized release of identifying information from this birth registration worksheet to ensure the confidentiality of the parents and their child.

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

Provide email addresses on this worksheet to receive an electronic notification when the information has been registered.

After Registration, order the certificate online at **vitalrecords.utah.gov** and pay the fee on the Utah.Gov website.

The footprint card or registration form you receive from the hospital or midwife is not an official birth certificate.

THIS WORKSHEET IS NOT AN APPLICATION FOR A BIRTH CERTIFICATE

What if there is a mistake on the birth certificate or I want to add or change something later?

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

Use upper and lower case *English standard characters only* . Non-standard English characters are not accepted by the Social Security Administration. Non-standard characters on a birth certificate require special processes, ask birth clerk for more info.

If you need to change something after the information is registered, you must file an amendment with the Office of Vital Records.

All changes made to the birth certificate after registration will show as amendments to the original record.

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

To order a Social Security Card for your child, be sure to check "Yes" to item #11 and sign the worksheet.

The card will be mailed in 2-3 weeks to the address listed as the 'Mail To' address in #31.

*The 'in-care-of name' and the names of ALL who live there **MUST** be listed visibly on or in the mailbox for the SSA card to be delivered.*

The Post Office cannot forward the card. A Social Security Card cannot be mailed out of the country.

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

Birth Clerk Message

Parents: Please tear this sheet off for your records.

Mother's Name: ____ Room Number: _____________

PLEASE PRINT CLEARLY. DO NOT TAKE THIS WORKSHEET HOME.

THIS WORKSHEET **MUST BE LEFT** FOR THE BIRTH CLERK AT TIME OF DISCHARGE.

Please fill in Circles completely ●

1. Child's legal name, as parents wish it to appear on the birth certificate.

Child First Name(s) ____

Middle Name(s) ____

Last Name(s) ____ Suffix (Jr. Sr. etc): ____________

2. Child Sex: ○Male ○Female ○Undetermined (SSA Card cannot be processed without a sex for the child.)

3. Date of birth mm/dd/yyyy: ______________________ 4. Time of birth (24 hr clock): ______________________

5. Child birth Weight: __________LBS ___________OZ. 6. Child birth Length (Inches): ______________________

Length will not be listed on the Birth Certificate

7. Where was the baby born?

○ 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. Intended place of delivery. When labor *started,* where did Mother *plan* to give birth?

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. Mother had a C-section without labor.

9. If child was NOT born at, or while traveling to, a hospital or birth center, please list the full street address of birth location here: ____

____

10. Name of delivering birth professional or other birth attendant: ____Title: _____________________

11. ○**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 ____**

MOTHER

12. On my child's birth certificate, I wish to be known as: ○Mother (Female) ○Father (Male) ○Parent (Female) ○Parent (Male)

13. I Gave Birth: ○Yes ○No

14. Mother's Marital Status:
○ Married to Biological father (Skip to Question #18)
○ Not married
○ Married, not to biological father (Skip to Question #17)

15. Was Mother ever married?
○ Yes ○ No

16. Was Mother married any time within the last 300 days (about 10 months)?
○ Yes ○ No

17. If not married to the biological father, do you wish to legally acknowledge him on the birth certificate? ○Yes ** ○No (Skip to #18)
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 the mother must** sign the VDP.
If married within the last 300 days: the **ex-spouse, the biological father and the mother must** sign the VDP.

**This Parental Worksheet must be turned in to the birth clerk in order for the Voluntary Declaration of Paternity form to be prepared for parents to sign.

18. Was child delivered by a gestational surrogate? ○Yes ○No

19. Mother's current Legal Name:

First Name(s) ____

Middle Name(s) ____

Last Name(s) ____________________________________ Suffix (Jr. Sr. etc): ____________

20. Mother's Name prior to first marriage - name as it appears on the current birth certificate, not a name prior to an adoption or other court order 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): ____________

21. Date of Birth mm/dd/yyyy: ____________________ 22. Phone Number: ____________________

23. Social Security Number: ____________________
SSN is required by Federal Law, 42 USC 405(c) Section 205(c) Social Security Act

24. State of Birth: ____________________
Spell out name of U.S. State

25. Country of Birth, if not U.S.A.: ____

26. Usual or Permanent Residence
Complete number and street Address: ____
Indicate directional such as Apt, Unit, Space, etc. in front of the location number to assist in mail delivery accuracy. Example: 124 West Maple Unit B

City/Town or Location: ____________________ U.S. State: ____________ Zip: ____________

County ____________________ Foreign Country if not in U. S.: ____________________

27. Inside City Limits? ○ Yes ○ No ○I don't know

28. Mother's Email Address: ____ **Print Clearly**

You will receive an *immediate* email confirming the registration of chid's birth from the Office of Vital Records and Statistics which will allow for immediate ordering and purchase of your child's birth certificate for insurance and other family records purposes.

29. Mother's mailing address same as residence? ○Yes ○No - Please Complete #31

30. In Care of Mail Person's Name: ____

Failure to list this person's name in or on the mail/PO Box will result in the SSA card being returned to SSA as undeliverable.
Parents will then need to apply to SSA for a replacement card. Hospital and Vital Records cannot process a second request.

31. Complete Mailing Address: ____

City/Town or Location: _________________________ U.S. State: ______________________ Zip: _________________________

To order a Social Security Card for your child, be sure to check "Yes" to item #11 and sign the worksheet.
The Social Security card will be mailed in 2-3 weeks.
The 'in-care-of name' and the names of ***ALL*** *who live there* ***MUST*** *be listed visibly on or in the mailbox for the SSA card to be delivered.*
The Post Office cannot forward the card. A Social Security Card cannot be mailed out of the country.

32. Mother Signature: ____

By signing here, I certify that the personal information provided on this worksheet is correct to the best of my knowledge and belief.

FATHER

33. Travel out of Utah in the last 12 months? ○Yes ○No

34. If Yes, list U.S. States and Foreign Countries: ____

35. Tested for Zika? ○Yes ○No ○Unknown

36. On my child's birth certificate, I wish to be known as: ○Mother (Female) ○Father (Male) ○Parent (Female) ○Parent (Male)

37. Father's current Legal Name:

First Name(s) ____

Middle Name(s) ____

Last Name(s) ____ Suffix (Jr. Sr. etc): ______________

38. Father's Name prior to first marriage - name as it appears on the current birth certificate, not a name prior to an adoption or other court order name change. Print clearly using upper and lower case characters and spacing as needed.

<u>The name listed below will appear on the child's birth certificate.</u>

First Name(s) ____

Middle Name(s) ____

Last Name(s) ____ Suffix (Jr. Sr. etc): ______________

39. Date of Birth mm/dd/yyyy: _________________________ 40. Phone Number: ____

41. Social Security Number: ___________________________________ 42. State of Birth: __________________________________

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

Spell out name of U.S. State

43. Country of Birth, if not U.S.A.: ____

44. Usual or Permanent Residence
Complete number and street Address: ____

Indicate directional such as Apt, Unit, Space, etc. in front of the location number to assist in mail delivery accuracy. Example: 124 West Maple Unit B

City/Town or Location: ______________________ U.S. State: ________________ Zip: ______________

County ______________________________ Foreign Country if not in U. S.: ______________________

45. Inside City Limits? ○Yes ○No ○I don't know

46. Father's Email Address: ____ **Print Clearly**

You will receive an *immediate* email confirming the registration of chid's birth from the Office of Vital Records and Statistics which will allow for immediate purchase of your child's birth certificate for insurance and other family records purposes.

47. Father Signature: ____

By signing here, I certify that the personal information provided on this worksheet is correct to the best of my knowledge and belief.

ADOPTION?

48. Is this child to be relinquished or placed for adoption? ○Yes ○No

49. If 'Yes', please list the name of the agency and/or attorney or 'private adoption': ______________________________

CONFIDENTIAL HEALTH INFORMATION OF BIOLOGICAL MOTHER

50. Was Mother enrolled in Medicaid at time of birth? ○Yes ○No

51. Did Mother receive food vouchers for Women, Infants and Children (WIC) food <u>for herself</u> during this Pregnancy?
○ Yes ○ No ○ I Don't know

52. 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)

53. Does anyone in the family (child's mother, father, 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? ○ Yes ○ No ○ I don't know

54. Mother height: _________ Feet _________ Inches

55. Mother weight prior to pregnancy: ______________ Lbs.

56. Mother weight at Delivery: ______________________ Lbs.

57. Did Mother Smoke? ○ Yes ○ No

58. 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 # ____________________

59. Were e-cigarettes or other electronic nicotine products used during pregnancy? ○ Yes ○ No

60. If 'yes' frequency of e-cigarette use: ○ More than once per day ○Once a day ○ 2-6 days per week ○ 1 day per week or less

61. Is infant being breast-fed at discharge? ○Yes ○ No

62. Was Mother told by her healthcare provider that she had gestational diabetes during this pregnancy? ○Yes ○No

63. During your most recent pregnancy, did a doctor, nurse, or other health care worker try to keep your new baby from being born too early by giving you a series of weekly shots or daily vaginal suppositories of a medicine called Progesterone, Makena ® or 17P (17 alpha-hydroxyprogesterone)?
○ Yes - weekly injection ○ Yes - vaginal suppository ○ No ○ Unknown

64. Date of last menses (last period) mm/dd/yy: ____________________ 65. Number of previous births now living: #_______________
Do not include this child.

66. Date of last live birth (do not include this child) mm/yyyy: _________________ 67. Number of previous live births now deceased: #________

68. Total number of pregnancies not resulting in live birth: #__________ 69. Date of last pregnancy not resulting in a live birth: ______

70. Total number of stillbirths: _____________ 71. Number of previous live multiple birth pregnancies: # ____
Losses at 20+ weeks or greater born without signs of life, do not include induced terminations - any weeks)

72. Date of first prenatal care visit mm/dd/yyyy: ____________________ 73. Number of prenatal visits this pregnancy: # ____________

74. Prenatal care Provider(s) / Facility: ____

75. Did Mother transfer to a hospital *during labor, but before delivery* from an attempted home or birth center birth?
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, Mother did not transfer to a hospital *during labor* from an attempted home or birth center birth.
○ Unknown if Mother transferred to a hospital *during labor* from an attempted home or birth center birth.

76. Did Mother transfer to a hospital *within 24 hours after delivering* at a home or birth center?
○ Yes, transferred after delivering at *home* Midwife Name: ____
○ Midwife attended, name unknown ○ Unknown if midwife attended ○No midwife
○ Yes, transferred after delivering at *freestanding birth center* - Midwife Name: ____
Facility Name: ____
○ No, Mother did not transfer to a hospital *within 24 hours after delivering* at a home or birth center.
○ Unknown if Mother transferred to a hospital *within 24 hours after delivering* at a home or birth center.

77. During most recent pregnancy, did Mother have teeth cleaned by a dentist or dental hygienist? ○Yes ○No ○Unknown

78. Did any of the following things make it difficult for Mother to go to a dentist or dental clinic during the most recent pregnancy?
○ Could not find a dentist or clinic who would take pregnant patients
○ Could not find a dentist or clinic who would take Medicaid patients
○ Did not think it safe to go to dentist during pregnancy
○ Could not afford to go to a dentist or dental clinic

79. During the month before pregnancy, how many times per week did Mother take a multivitamin, prenatal vitamin or folic acid vitamin?
○ Did not take vitamins ○ 1 to 3 times per week ○ 4 to 6 times per week ○ Every Day ○ Unknown

80. If Mother did not take vitamins, what were the reasons - choose all that apply.
○ Wasn't planning to get pregnant
○ Didn't think vitamins were needed
○ Unknown
○ Didn't want to take vitamins
○ Vitamins were too expensive
○ Vitamins gave side effects
○ Other - specify reasons:
____
____

81. Did Mother travel out of state in the last 12 months? ○Yes ○No If 'yes', list U.S. states and foreign countries:

____

82. Was Mother tested for Zika virus by healthcare provider? ○ Yes ○ No ○ Unknown

83. Was Mother tested for Hepatitis B by a healthcare provider during this pregnancy or at the hospital? ○Yes ○No ○Unknown

RACE/ETHNICITY

84. Mother of Hispanic Origin? ○ Yes ○ No ○ Unknown
if 'Yes', check all that apply: ○ Mexican, Mexican American, Chicana ○ Puerto Rican ○Cuban
○ Other Spanish / Hispanic / Latina - Specify: ___________________________________
(e.g. Spaniard, Salvadoran, Dominican, Colombian)

85. Race of Mother, Check all that apply:
○ White
○ Black
○ American Indian or Alaska Native - Specify: ________________________________
○ Chinese
○ Japanese
○ Native Hawaiian
○ Filipino
○ Other Asian - Specify: ____________________________
○ Asian Indian
○ Korean
○ Samoan
○ Vietnamese
○ Guamanian
○ Pacific Islander - Specify: _________________________
○ Tongan
○ Other - Specify: _________________________
○ Unknown

86. Mother's Education
○ 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 Prof. Degree (e.g. MD, DDs, DVM, LLB, JD)
○ None
○ Unknown

87. Father of Hispanic Origin? ○ Yes ○ No ○ Unknown
if 'Yes', check all that apply: ○ Mexican, Mexican American, Chicano ○ Puerto Rican ○Cuban
○ Other Spanish / Hispanic / Latino - Specify: ___________________________________
(e.g. Spaniard, Salvadoran, Dominican, Colombian)

88. Race of Father, Check all that apply:
○ White
○ Black
○ American Indian or Alaska Native - Specify: ________________________________
○ Chinese
○ Japanese
○ Native Hawaiian
○ Filipino
○ Other Asian - Specify: ____________________________
○ Asian Indian
○ Korean
○ Samoan
○ Vietnamese
○ Guamanian
○ Pacific Islander - Specify: _________________________
○ Tongan
○ Other - Specify: _________________________
○ Unknown

89. Father's Education
○ 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 Prof. Degree (e.g. MD, DDs, DVM, LLB, JD)
○ None
○ Unknown

MOTHER'S MEDICAL INFORMATION

Questions have been raised regarding the incidence of birth defects and other birth outcomes and fertility treatments. Your answers to the following questions will help scientists answer these questions. Answers are important whether or not your baby had any problems and whether or not you used any fertility treatments.

90. Did you take any fertility drugs or receive any medical procedures to help you get pregnant for this pregnancy? ○ Yes ○ No

91. How long had you be trying to get pregnant when you conceived? Please count the time from when you first started having sexual intercourse without any contraception.
○ 0-5 months ○6-11 months ○1-2 years ○3-4 years ○5-6 years ○>6 years

92. Did you use any of the following fertility treatments?
○Fertility enhancing drugs by mouth (Clomid, Clomiphene, or others)
○Fertility enhancing drugs by injection (Pergonal, Follistim, HGG or others)
○Artificial Insemination or Intrauterine Insemination (AIH, AID/DI)
○Assisted Reproductive Technology (IVG, GIFT, ZIFT, ICSI)
○Other Medical Treatment - Specify: ____
○Use of Donor Semen ○ Use of Donor Eggs ○ Surgery for endometriosis
○Metformin or Glucophage ○ Progesterone
○None of the Above

Mother's Name: ____ Room Number: _____________

SFN# of Baby A: ____

MULTIPLE CHILD DELIVERY

TWIN B / TRIPLET B / QUADRUPLET B

93. Child's legal name, as parents wish it to appear on the birth certificate.

Child First Name(s) ____

Middle Name(s) ____

Last Name(s) ____ Suffix (Jr. Sr. etc): ____________

2. Child Sex: ○Male ○Female ○Undetermined (SSA Card cannot be processed without a sex for the child.)

3. Date of birth mm/dd/yyyy: ______________________ 4. Time of birth (24 hr clock): ______________________

5. Child birth Weight: __________LBS ___________OZ. 6. Child birth Length (Inches): _____________________

Length will not be listed on the Birth Certificate

TRIPLET C/ QUADRUPLET C

94. Child's legal name, as parents wish it to appear on the birth certificate.

Child First Name(s) ____

Middle Name(s) ____

Last Name(s) ____ Suffix (Jr. Sr. etc): ____________

2. Child Sex: ○Male ○Female ○Undetermined (SSA Card cannot be processed without a sex for the child.)

3. Date of birth mm/dd/yyyy: ______________________ 4. Time of birth (24 hr clock): ______________________

5. Child birth Weight: __________LBS ___________OZ. 6. Child birth Length (Inches): _____________________

Length will not be listed on the Birth Certificate

QUADRUPLET D

95. Child's legal name, as parents wish it to appear on the birth certificate.

Child First Name(s) ____

Middle Name(s) ____

Last Name(s) ____ Suffix (Jr. Sr. etc): ____________

2. Child Sex: ○Male ○Female ○Undetermined (SSA Card cannot be processed without a sex for the child.)

3. Date of birth mm/dd/yyyy: ______________________ 4. Time of birth (24 hr clock): ______________________

5. Child birth Weight: __________LBS ___________OZ. 6. Child birth Length (Inches): _____________________

Length will not be listed on the Birth Certificate

Appendix D

NIST Privacy Framework Controls

Version 1.0

NIST PRIVACY FRAMEWORK CORE

January 16, 2020

Certain Categories or Subcategories may be identical to or have been adapted from the Cybersecurity Framework. The following legend can be used to identify this relationship in the table. A complete crosswalk between the two frameworks can be found in the resource repository at https://www.nist.gov/privacy-framework.

░	The Function, Category, or Subcategory aligns with the Cybersecurity Framework, but the text has been adapted for the Privacy Framework.
▓	The Category or Subcategory is identical to the Cybersecurity Framework.

	Function	Category	Subcategory
	IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing. ░	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.
			ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
			ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
			ID.IM-P4: Data actions of the systems/products/services are inventoried.
			ID.IM-P5: The purposes for the data actions are inventoried.
			ID.IM-P6: Data elements within the data actions are inventoried.
			ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
			ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.
		Business Environment (ID.BE-P): The organization's mission, objectives, ░	**ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified and communicated. ░

	Function	Category	Subcategory
		stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P2:** Priorities for organizational mission, objectives, and activities are established and communicated.
			ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.
		Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).
			ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.
			ID.RA-P3: Potential problematic data actions and associated problems are identified.
			ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
			ID.RA-P5: Risk responses are identified, prioritized, and implemented.
		Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.
			ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.
			ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.
			ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.

	Function	Category	Subcategory
			ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations.
	GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.
			GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
			GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.
			GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
			GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
			GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.
		Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
			GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.
			GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.
		Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with	**GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities.
			GV.AT-P2: Senior executives understand their roles and responsibilities.
			GV.AT-P3: Privacy personnel understand their roles and responsibilities.

	Function	Category	Subcategory
		related policies, processes, procedures, and agreements and organizational privacy values.	**GV.AT-P4:** Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.
		Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
			GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.
			GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
			GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
			GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).
			GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.
			GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.
	CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with	**Data Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
			CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).

	Function	Category	Subcategory
	sufficient granularity to manage privacy risks.	organization’s risk strategy to protect individuals’ privacy.	**CT.PO-P3:** Policies, processes, and procedures for enabling individuals’ data processing preferences and requests are established and in place.
			CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.
		Data Processing Management (CT.DM-P): Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P1:** Data elements can be accessed for review.
			CT.DM-P2: Data elements can be accessed for transmission or disclosure.
			CT.DM-P3: Data elements can be accessed for alteration.
			CT.DM-P4: Data elements can be accessed for deletion.
			CT.DM-P5: Data are destroyed according to policy.
			CT.DM-P6: Data are transmitted using standardized formats.
			CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
			CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
			CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.
			CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.
		Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization’s risk strategy to protect individuals’ privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).
			CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).
			CT.DP-P3: Data are processed to limit the formulation of inferences about individuals’ behavior or activities (e.g., data processing is decentralized, distributed architectures).
			CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.
			CT.DP-P5: Attribute references are substituted for attribute values.

	Function	Category	Subcategory
	COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.
			CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
		Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
			CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
			CM.AW-P3: System/product/service design enables data processing visibility.
			CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
			CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
			CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
			CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.
			CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.
	PROTECT-P (PR-P): Develop and implement	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles	**PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).

Function	Category	Subcategory
appropriate data processing safeguards.	and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**PR.PO-P2:** Configuration change control processes are established and in place.
		PR.PO-P3: Backups of information are conducted, maintained, and tested.
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.
		PR.PO-P5: Protection processes are improved.
		PR.PO-P6: Effectiveness of protection technologies is shared.
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.
		PR.PO-P8: Response and recovery plans are tested.
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
		PR.PO-P10: A vulnerability management plan is developed and implemented.
	Identity Management, Authentication, and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
		PR.AC-P2: Physical access to data and devices is managed.
		PR.AC-P3: Remote access is managed.
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
	Data Security (PR.DS-P): Data are managed consistent with the	**PR.DS-P1:** Data-at-rest are protected.
		PR.DS-P2: Data-in-transit are protected.

	Function	Category	Subcategory
		organization’s risk strategy to protect individuals’ privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P3:** Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
			PR.DS-P4: Adequate capacity to ensure availability is maintained.
			PR.DS-P5: Protections against data leaks are implemented.
			PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
			PR.DS-P7: The development and testing environment(s) are separate from the production environment.
			PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.
		Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
			PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
		Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.
			PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
			PR.PT-P3: Communications and control networks are protected.
			PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.