Short text responses for UPDB/RGE legislative report:

1. What specific statutory authority do RGE and UPDB have to collect, store, and use the highly sensitive medical, driver license, voter registration, genealogical, birth, and multiple other records of Utahns?

The State of Utah formally recognized RGE approximately a half century ago. This recognition originally occurred through the issuance of executive orders citing statutory authority empowering the State to gather and transfer data for the purpose of reducing morbidity or mortality, or for the purpose of evaluating and improving the quality of hospital and medical care. The Utah Code has evolved considerably since that time but still authorizes collection and transfer of information critical to reducing morbidity or mortality and to evaluating and improving hospital and medical care. Applicable statutory authority is tied to the particular data source. For example, Utah Code section 53-3-109(1)(v) specifies that the Driver License Division may disclose information "to the University of Utah for data collection in relation to genetic and epidemiologic research." Other statutes may not reference the University of Utah, RGE, or UPDB specifically, but disclosures to RGE and UPDB are made for statutorily authorized purposes. See, e.g., Utah Code § 26B-8-406(2) & (3) (authorizing disclosure of identifiable health data to another governmental entity for use consistent with the purpose of original collection or for bona fide research purposes).

Observation:
The explanation leans on very broad and somewhat dated authority, spread across different parts of the code, rather than pointing to a clear and current statute that directly authorizes the full scope of today's data collection and linkage. That could raise questions about whether today's practices match modern expectations for privacy.

Question:
Is it time for the Legislature to spell out directly and in one place what data RGE/UPDB can collect, how long it can be kept, and what rights Utahns have over it?

2. Which governmental and non-governmental entities provide data resources to the RGE and UPDB?

UPDB receives and stores data from the following entities.
1. Driver License Division
2. Utah Department of Health and Human Services (UDHHS)
3. Lieutenant Governor's Office
4. Utah Genealogical Society
5. IPUMS USA – 1870-1940 US Census data
6. Social Security Death Index (SSDI)

On a project-specific basis, UPDB may facilitate access to data from other sources if a project receives necessary approvals.

3. Would the administrators of the RGE and UPDB support requiring informed consent before using any personally identifiable information and personally identifiable medical information? Why or why not?

The University considers informed consent a fundamental principle of research ethics. But while consent is central to protecting individual autonomy, it is not always feasible or appropriate in all research contexts. For example, for research designed to improve population health, it is critical that analyses reflect the full population so that observed patterns, associations, and trends are valid and useful for generalizable statewide and national health improvements. A blanket requirement for informed consent for personally identifiable or medical information for such research is logistically infeasible for large-scale population studies.

Federal law, recognizing these challenges, has long provided a mechanism for researchers to carefully assess and pursue such projects. Specifically, an IRB must review the project and make several determinations, including a conclusion that the research (i) involves no more than minimal risk to individuals; (ii) could not practicably be carried out if individual informed consent were required; (iii) could not practicably be carried out without using the identifiable private information; and (iv) will not adversely affect the rights and welfare of the individuals.

Observation:
The response leans on feasibility and federal IRB standards but doesn't directly address the core concern: Utahns have no say in whether their identifiable data is used in research, even highly sensitive medical data. A legislator focused on individual rights might feel the answer sidesteps the question of whether people *should* have a voice, not just whether it's convenient.

Question:
Even if consent isn't practical for every project, is there a way to give Utahns at least some form of choices, such as an opt-out or tiered consent, so their identifiable data isn't automatically included in research they may not support?

4. Would the executive branch support statutory changes requiring agencies of the government to provide informed consent before collecting any personally identifiable information and personally identifiable medical information, except in the commission of a crime? And a provision that, if the individual is later exonerated or charges are not filed, the PII and Medical PII must be destroyed?

This question appears to be directed to leadership within the executive branch. We note that the Government Data Privacy and Protection Act requires delivery of a privacy notice in connection with personal information collection activities of government entities.

5. Do entities holding Utahns' most sensitive individual identifying and medical information obtain the informed consent of the individual before transferring their records to the RGE and UPDB? If not, why not?

In most cases, individual informed consent is not required for data transfers to the UPDB. These transfers occur consistent with applicable statutory authorization, data use agreements, and ethical oversight requirements, rather than as part of direct individual research participation. Agreements governing these transfers define data elements, acceptable use principles, security standards, and oversight mechanisms. RGE and UPDB are committed to meeting all legal and compliance expectations associated with its receipt, storage, and use of data.

Observation:
This answer focuses on compliance and agreements between institutions but doesn't really speak to the individual whose data is being transferred. A privacy-minded legislator may notice that the core issue, people never being told their identifiable medical or personal records are being handed over, is left unaddressed.

Question:
If Utahns aren't asked or even notified, how can we be confident their rights and expectations of privacy are being respected when their most sensitive information is shared?

6. Do the RGE and UPDB obtain the informed consent of individuals before releasing their de-identified information for research, policy, and other purposes? If not, why not?

RGE and UPDB do not seek individual consent before releasing de-identified data for approved purposes. This is approach is consistent with the HIPAA Privacy Rule and the federal common rule 45 CFR 46, which are designed to protect health information and the welfare of research participants. All de-identified datasets are reviewed and approved through rigorous de-identification process, undergo IRB review, and are subject to data use agreements that prohibit any re- identification efforts.

Requiring individual consent for each de-identified dataset would make most of Utah's health and outcomes research infeasible and would provide only minimal additional privacy benefits because de-identified data cannot be linked to individual identities. The existing framework preserves both individual privacy and the public value derived from responsibly conducted research.

Observation:
The response assumes that de-identification fully protects privacy, but recent high-profile cases and academic research shows that reidentification of "de-identified" data can be trivial to achieve with current technological advances when combined with other datasets.

Question:
What safeguards or penalties exist in code, agreements or your processes if supposedly

de-identified data is later shown to be re-identifiable or is reidentified by the recipient and should Utah law require stronger protections or limits on its release?

7. Who decides when an individual's identifiable medical and other information will be released for research, policy, and other purposes? Who ensures that all individuals who are granted access to the UPDB are not copying, saving, or in any way storing any of the information in the database? Who ensures compliance with researcher agreements and how?

RGE and the IRB review projects based on federal, state, and University regulatory expectations and determine what will be released to researchers. Each project has a principal investigator who is responsible for compliance with the approved requirements for data security and storage. Researchers do not have direct access to the UPDB. Instead, they only have access to project-specific data prepared by UPDB professional staff confined to the specific data elements approved by RGE and the IRB for the project. RGE and the IRB monitor compliance with agreements signed by the principal investigator and through annual project review.

The release or use of any identifiable medical or personal information from the UPDB to approved researchers requires prior review and approval by:

- o The University of Utah Institutional Review Board (IRB), which ensures compliance with federal human subjects protection regulations (45 CFR 46);
- o The RGE Committee, which oversees access to the UPDB and ensures all uses serve a legitimate health research purpose; and
- o When applicable, data-providing sources, each of which must authorize data release consistent with their own privacy and legal requirements.

UPDB staff undergo regular training in human subjects protections, research ethics, data privacy, and information security. This ensures that all activities comply with federal regulations, institutional policies, contractual obligations, and the highest ethical standards for data stewardship.

Observation:
UPDB indicated in last month's committee presentation that no identifiable data is accessible or used in the system; however, this answer describes processes for reviewing, releasing, and monitoring the use of identifiable information, which conflicts with what was previously stated.

Question:
If researchers never have access to identifiable data, why does the approval process repeatedly reference releasing identifiable information and can you clarify exactly where identifiable data exists, who can see it, and under what circumstances?

8. Why does the Utah Drivers License Division MOU with the RGE, dated 1-2-2018, include the following requirement: "Individuals contacted based on data contributed by DLD may not be informed contact was from data provided by the DLD?"

Unclear. The language has been included in MOUs with the DLD for over a decade. We are uncertain of the rationale for its inclusion. The University would have no concerns removing the Language.

Observation:
This answer indicates the University doesn't know why that provision required that Utahns not be told their driver license data was used to contact them, a clause that understandably raises red flags about transparency.

The admission that no one knows why an MOU prohibits informing Utahns that their driver-license data was used to contact them, together with the possibility that individuals may actually be contacted based on data they never consented to share and cannot opt out of, raises serious transparency and autonomy concerns. It also seems to contradict your response that "The University considers informed consent a fundamental principle of research ethics."

Question:
If people are being reached using information they didn't knowingly provide for that purpose, doesn't that suggest a need for clear statutory limits, and should the Legislature require that any contact based on state-held personal data be both disclosed to the individual and subject to an opt-out?

9. Do individuals whose data is being considered for release have an elected representative on the RGE Committees and/or on the Institutional Review Boards (IRB) that approve research proposals?

While RGE and IRB committees do not have elected representatives, the University's IRB panels all include public, non-affiliated members who represent community perspectives as well as faculty and staff who conduct and understand research projects. These members ensure that privacy, ethics, and community values are upheld in all decisions. Volunteer committee service is a requirement for all faculty at the University, and the University has community partners who are aware of, promote, and discuss the standards of community.

10. Given that data is the new currency, what property interests do Utahns have in their most sensitive medical and individual identifying information that the RGE and UPDB collects and distributes for research purposes?

The answer to #10 is addressed in the answer to #11.

11. When new billion-dollar products are developed that come from research conducted using Utahns' most sensitive medical and individual identifying information, what do these Utahns receive in terms of compensation? Free drugs, treatments, royalties, etc.?

Modern health care depends on research that draws from the real experiences and health data of broad populations. By using information from a broad base of people, researchers can better understand how diseases develop, how treatments work in different communities, and how to create new tools that improve care for everyone. This kind of inclusive research allows innovations—such as early diagnostic methods, precision medicine, and population health strategies—to benefit the full spectrum of society, rather than a limited subset. To conduct such studies responsibly, research activities are reviewed and approved by an IRB. The IRB ensures ethical standards are met, risks are minimized, and individuals' rights and privacy are protected. As noted above, in some cases, an IRB may grant a waiver of informed consent when research involves minimal risk, could not practicably be carried out otherwise, and includes robust safeguards for confidentiality. This means that individual permission is not sought for each data use, but data are handled under strict privacy and security controls to prevent misuse. Importantly, participation in this kind of research does not necessarily grant commercial rights or ownership of resulting products or discoveries to data contributors. This standard approach aligns with federal research ethics and existing intellectual property laws. However, the value returned to the community comes in other important forms: improved understanding of regional health needs, enhanced access to innovative care, new public health insights, and the attraction of research and development investment that benefits the broader area. These efforts also help ensure local populations are represented in studies that shape the future of medicine. By contributing to responsibly conducted, IRB-approved research, our community helps advance knowledge that leads to better health outcomes—locally, nationally, and globally—while maintaining strong ethical and privacy protections.

Observation:
The answer talks about general community benefits but does not address the fairness issue at the heart of the question. Utahns' most sensitive data, collected without consent and with no way to opt out, can contribute to highly profitable medical and commercial products. At the same time, healthcare costs keep going up, healthcare company profits are at record highs, and many Utahns may feel that their personal information is being used in ways that benefit others while they are left paying higher taxes and higher medical bills.

Question:
If Utahns' medical and personal data helps create products that generate significant commercial value, why is there no compensation, benefit-sharing, or even basic transparency for the people whose information was used?

12. How can individuals find out which records, and the specific information in those records, that the RGE and UPDB have on them?

Individuals may contact the original data sources for their records. UPDB is not authorized to provide individual-level data or access to members of the public. This restriction protects the confidentiality of all individuals represented in the database and ensures compliance with privacy and human subjects protection requirements. Members of the public may also contact RGE and UPDB administration for general information about governance, security, and data stewardship practices.

Observation:
The answer offers no way for a Utahn to learn what UPDB actually holds about them, how their records have been linked, or how their information has been used. Telling people to contact the original data sources does not address what exists inside UPDB itself. This concern is heightened by UPDB's statement in last month's committee hearing that the system is incapable of disposing of data. That means UPDB may retain highly sensitive information about Utahns forever, even after the original agencies have deleted or lawfully disposed of their own copies. For a system that aggregates lifelong medical, personal, and identifying data, the lack of both transparency and any path for deletion or correction is a serious issue.

Question:
If UPDB keeps linked records indefinitely and cannot delete them, why is there no process for Utahns to see what information UPDB holds about them, understand how it is being used, or request that outdated or sensitive information be corrected or removed?

13. Should an entity other than the University of Utah be given statutory control over the RGE and UPDB and should IRBs have elected citizen representatives on them?

The University of Utah has successfully managed the UPDB and RGE for more than four decades under strict oversight. Transferring control would disrupt research continuity and compliance systems. IRBs already include non-affiliated community members consistent with federal law. Appointing elected citizen representatives to IRBs would not align with federal regulatory expectations. The current structure—comprising scientific, non-scientific, and community members—is designed to ensure balanced and qualified ethical review consistent with national standards.

14. Do you have a defined plan for a data breach response at both the UPDB level and the individual researcher level? Has the plan ever been activated?

The UPDB Incident Response Plan follows the National Institute of Standards and Technology (NIST) Special Publication 800-61 framework, which outlines four phases: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activities. During the preparation phase, communication channels, contact information, and incident tracking procedures are clearly defined. The detection and analysis phase includes criteria for

identifying incidents and assessing their impact. The containment, eradication, and recovery phase provides detailed guidance on mitigating damage, removing threats, and restoring systems and data integrity. Finally, the post-incident phase involves documenting the response through the report, evaluating root causes, and revising technical controls and policies to prevent recurrence.

The UPDB also aligns with NIST SP 800-171 standards for security scanning, detection, containment, investigation, and remediation. When appropriate, incidents are escalated to the University of Utah Information Security Office (ISO) and the Huntsman Cancer Institute IT (HCI-IT) team for systems under their oversight. The University's Office of General Counsel and Privacy Office are also engaged when appropriate.

UPDB has not experienced a data breach in our many decades of stewardship.

For datasets that have been disbursed to researchers, the RGE and UPDB must be immediately notified of any suspected data deviation or protocol violation. A coordinated triage process follows, involving the researcher, UPDB, and IT representatives for the affected systems to determine the appropriate response. When a deviation report is necessary, it is submitted to the IRB and RGE, and must describe the issue, corrective actions taken, and plans to prevent recurrence. The report is reviewed for sufficiency by the IRB and RGE, including relevant data contributors. This structured and collaborative approach ensures that any cybersecurity or privacy concern is addressed promptly, transparently, and in full compliance with institutional, state, and federal requirements.

Observation:

The response describes internal incident-response mechanics but never mentions notifying the individuals whose data would be affected. UPDB holds some of the most comprehensive and sensitive linked information about Utahns anywhere in state government, yet the breach plan as described offers no assurance that people would be told if their data is compromised. This is not routine data that is already widely available to threat actors; it is uniquely aggregated and deeply personal. Given that the Government Data Privacy Act requires notification to individuals when their personal data is breached, the absence of any discussion of individual notice stands out.

Question:

Why does your incident-response plan not include a clear requirement to notify every affected Utahn if their aggregated personal or medical data is breached, and how will you ensure compliance with the Government Data Privacy Act's breach-notification requirements?

15. Are the datasets used by researchers de-identified to a level that prevents the researcher or UPDB staff from reconstructing the original data subject's identity?

All research using UPDB data must follow the principle of minimum necessary use, meaning that only the specific data required to conduct the approved analysis are accessible. This approach ensures that datasets remain protected to a degree that effectively prevents reconstructing the identity of any individual, while still allowing for meaningful and compliant population-based research.

16. Are researchers allowed to take data obtained from UPDB and aggregate it into AI training models?

Researchers are not permitted to incorporate UPDB data into external artificial intelligence (AI) or large language model (LLM) training systems.

UPDB datasets are not allowed to be used as tokens, data sources, or training material in external AI agents or large language models. While AI and machine learning are recognized as powerful analytical tools capable of identifying patterns, trends, and connections that may not be visible through traditional methods, which is a goal of the UPDB, their use within UPDB research is limited to approved, secure environments. Any machine learning analyses involving UPDB data must occur within a secure environment reviewed by the IRB and RGE, ensuring that the data remain protected, and used solely for the purposes specified in the approved research protocol.

17. What contractual relationship exists between UPDB and researchers to ensure that data obtained from the UPDB is deleted at the conclusion of a study?

Researchers provide a plan for disposition of data at the end of the study and agree to a standard statement of assurances to dispose of data. At the end of the study, researchers submit a Certificate of Data Disposition.

18. What is the process for handling reports of privacy violations and misuse of data? What is the IRB's role?

Investigations are conducted by cross-functional teams, with containment, documentation, and corrective actions. The IRB reviews violations related to approved research to determine whether noncompliance or unanticipated problems

Question:
Can you explain in clear terms what actually happens when someone misuses UPDB data, including whether affected Utahns are notified, what penalties or corrective actions follow, and what role, if any, individuals have in understanding or responding to a violation involving their information?

19. Are any identifiable student records held by the RGE or the UPDB?
No student records are held by RGE or UPDB.