Utah Cancer Registry Confidentiality and Data Use Agreement

This Utah Cancer Registry (Registry) Confidentiality and Data Use Agreement (the "Agreement") applies to all data provided to_____ for the purpose of _____ (Project).

Utah Department of Health (UDOH) retains all ownership rights to the data, including rights to control or limit the use and dissemination of the data. UDOH may terminate access at any time and require data to be returned or destroyed with 30 days written notice.

REGISTRY AND UDOH MAKE NO REPRESENTATIONS OR WARRANTIES, EITHER IMPLIED OR EXPRESS, REGARDING THE ACCURACY OR COMPLETENESS OF THE DATA, WHICH IS PROVIDED AS IS. REGISTRY AND UDOH CANNOT GUARANTEE THAT THE DATA HAS NOT CHANGED OR WILL NOT CHANGE.

Confidentiality Pledge

I hereby swear or affirm to maintain strict confidentiality in all matters related to the knowledge or use of Registry data obtained under the Project. I understand and agree that my access to these data is conditioned upon my adherence to this Agreement and compliance with all Registry policies and procedures. I understand that the confidentiality of these data is a material and essential aspect of the state statutes and a violation of this Agreement will result in a material breach of contract by me, my employer, or principal and may subject me to disciplinary actions, civil damages, or criminal prosecution under applicable law, including, but not limited to, Utah Code sections 26-25-5 and 63G-2-802(1).

I will notify Registry within 24 hours of any unauthorized disclosure, access, or use, or suspected unauthorized disclosure, access, or use of these data, whether mine or anyone else's, whether intentional or accidental.

Data Use

I agree to follow all Registry information safeguards specified in Attachment A, including limiting access to Registry data to authorized persons.

I will use Registry data only for the purposes approved by the Registry to conduct the activities detailed in the Project plan.

I will store Registry data in locations described in the approved Project plan.

I will not disclose, sell, copy, reproduce, assign, license, market, transfer, or otherwise dispose of, give, or grant access to Registry data to any unauthorized persons or entities without prior written approval of the Registry. I will only transfer RGE data using secure methods described in the approved Project plan and in keeping with Attachment A.

I will not attempt to identify or contact any persons represented in these data. I will not attempt to re-identify persons represented in de-identified or limited data sets.

I will not attempt to link these data with or attempt to generate hashes or other kinds of derivative data from data that can be used to link to any other data not described in the Project plan.

I will not contact or attempt to contact any entities, providers, or payers represented in these data.

I will not attempt to discover specific terms of contracts, discounts, or fixed reimbursement arrangements, or other specific reimbursement arrangements between health care providers and individuals or entities paying for health care items or services.

I agree to submit all manuscripts and documents intended for publication or public presentation to Registry for review prior to publishing or presenting. This review will confirm that data presented do not permit identification of individuals or their families or identification of entities, providers, or individuals or entities paying for health care items or services.

_____ _____

Signature **Date**

[Electronic signatures are not accepted.]

Please print or type your name: _____

ATTACHMENT A.
Utah Department of Health (UDOH)
Privacy and Security Terms and Conditions

A. **Definitions**

"Agreement" means the underlying agreement between the Utah Department of Health ("Department") and the University of Utah ("University") dated July 1, 2016.

"Breach" shall mean unauthorized acquisition, access, use, or disclosure of identifiable health data which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

"Health Data" means any information provided by the **Department** to **University** relating to the health status of individuals, the availability of health resources and services, and the use and cost of these resources and services as defined in Utah Code 26-3-1.

"Identifiable Health Data" means any item, collection, or grouping of health data which makes the individual supplying it or described in it identifiable as defined in Utah Code 26-3-1.

"Information Security Officer" means the individual identified in Section I.

"Minimum Necessary" means reasonable efforts are made to limit identifiable health data to only that which is necessary to accomplish the intended purpose of the use, disclosure, or request.

"Offshore Contractor" refers to a contractor who is in a country that is not one of the fifty United States or one of the United States Territories (American Samoa, Guam, Northern Marianas, Puerto Rico, and Virgin Islands).

"Chief Information Privacy/Security Officer" means the individual identified in Section I.

"Security Incident" means the successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system that is created, received maintained or transmitted by or on behalf of **Department**.

"**Subcontractor**" means a person to whom the **University** has delegated a function, activity, or service the **University** has agreed to perform for **Department**. Further, a subcontractor shall comply with these Privacy and Security Terms and Conditions where that function, activity, or service involves the creation, receipt, maintenance, or transmission of identifiable health data.

"UPDB" means Utah Population Database.

B. **Permitted Uses and Disclosures. University** may use or disclose identifiable health data it creates for or receives, maintains or transmits from **Department** as necessary in order to perform the **University's** obligations under the Agreement, **University's** proper management and administration, or to carry out **University's** legal responsibilities.

C. **Limitations on University's Use or Disclosure**. **University** shall neither use nor disclose identifiable health data it creates for or receives, maintains or transmits from **Department**, except as listed in Section B.

1. **Confidentiality/Privacy Policies. University** shall implement appropriate privacy and confidentiality policies and procedures to ensure the confidentiality of the identifiable health data.

University is responsible to obtain the appropriate Institutional Review Board(s) approvals, as necessary or as required by **University's** policies or procedures, prior to linking any identifiable health data to the UPDB.

2. **Compliance with Laws. University** shall comply with all applicable state and federal laws or regulations regarding the confidentiality, privacy, and security of identifiable health data and **University** shall use and disclose such information only in accordance with these laws or regulations.

3. **Information Safeguards.** The **University** shall establish, maintain, and practice information procedures and controls that comply with applicable federal and state laws or regulations to preserve the integrity, confidentiality, and availability of health data created or received for or from **Department.**

   At a minimum, information security safeguards shall include: (i) limiting access to identifiable information to authorized employees/authorized persons; (ii) securing university facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device application, database and platform security; (iv) securing information transmission, storage and disposal; (v) implementing authentication and access controls within media, applications, operating systems and equipment; (vi) encrypting personal identifiable health data stored on any mobile media and computing devices that allow remote access (other than secure Virtual Private Network (VPN)); (vii) encrypting identifiable health data transmitted over public or wireless networks; (viii) strictly segregating identifiable health data that **University** receives from other data sources unless permitted by the Agreement or authorized by the **Department**; (ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (x) providing appropriate privacy and information security training to University employees. For purposes of the above, remote access shall mean access to information assets from any remote location outside of the University's network or physical boundaries.

4. **Subcontractors and Agents. University** shall require any subcontractor or agent to whom **University** provides identifiable health data to agree in writing to (i) implement reasonable and appropriate safeguards to protect the data, and (ii) comply with the same restrictions and conditions on identifiable health data as required by these Privacy and Security Standard Terms and Conditions.

5. **Minimum Necessary.** In its performance of the functions, activities, services, and operations specified in the Agreement, **University** shall make reasonable efforts to use, disclose, or request only the minimum amount of identifiable health data reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that **University** shall not be obligated to comply with the minimum necessary limitations with respect to patient request for his or her records.

6. **Audits, Inspections and Enforcement.** Upon reasonable request by the **Department, University** and its subcontractors or agents shall allow the **Department** to conduct an inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use

or disclosure of identifiable health data in order to determine **University**'s compliance with these Privacy and Security Standard Terms and Conditions.

7. **Transmission of Data Offshore. University** is not authorized to transmit or share any identifiable health data, either directly or through a subcontractor, to any recipient Offshore without first obtaining written consent from the **Department**.

D. Breach and Secnrity Incident Reporting.

1. **Notification to the Department. University** shall notify the **Department** of any Breaches or Security Incidents. **University** shall make such report to **Department**'s Chief Privacy Officer or Chief Information Security Officer not more than five (5) business days after **University** knows of such Breach or Security Incident.

2. **Report. University** shall cooperate with **Department** in investigating such Breach or Security Incident, and in meeting **Department**'s obligations. **University** shall provide a written report to the **Department** within five (5) business days of the Breach or Security Incident. To the extent such information is available, the report must include, at a minimum: (i) the identification of each data element and individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed; (ii) the date of the Breach or Security Incident; (iii) the scope of the Breach or Security Incident; and (iv) a description of **University**'s response or corrective action **University** took to mitigate the Breach or Security Incident.

E. Termination and Continuing Privacy and Security Obligations.

1. **Termination. Department** may, in addition to other available remedies, terminate the Agreement if **University** has materially breached any provision of these Privacy and Security Standard Terms and Conditions and has failed to cure or take actions to cure such material breach within thirty (30) calendar days of the **Department**'s notification to **University** of the potential material breach.

2. **Obligations upon Termination.**
   a. Within thirty (30) calendar days after the effective date of the termination, cancellation, expiration or other conclusion of the Agreement, **University** shall immediately return or destroy all identifiable health data within **University**'s possession or control, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the identifiable health data, in any form or medium, and at any location such information resides.
   b. If such return or destruction is not feasible, **University** shall notify the **Department**. **University** shall extend the protections, limitation, and restrictions of this Privacy and Security Standard Terms and Conditions to any identifiable health data retained after the termination of the Agreement and shall limit further uses and disclosures to those purposes that make the return or destruction of the identifiable health data infeasible.

3. **Continuing Privacy and Security Obligations.** This provision shall survive the termination, cancellation, or expiration of the Agreement.

F. Miscellaneous.

1. **Amendments.** The Privacy and Security Standard Terms and Conditions may be amended by agreement of the parties, but no such amendment shall become effective until it is reduced to writing and signed by duly authorized representatives of each party.

2. **Waiver**. No review, approval, acceptance, or payment by the **Department** for any services per this Addendum shall operate as a waiver by the **Department** of any of its rights per this contract or of any cause of action arising out of the performance or nonperformance of the contract.

3. **No Third Party Beneficiaries.** Nothing in these Privacy and Security Standard Terms and Conditions shall be considered or construed as conferring any right or benefit on a person or imposing any obligations on a person who is not a party to the Agreement.

4. **Confidentiality. University**, and anyone to whom the **University** may be liable, must maintain the confidentiality of any non-public personal information. Personal information includes, but is not limited to, names, social security numbers, birth dates, address, credit card numbers and financial account numbers. This duty of confidentiality shall be ongoing and survive the term of this contract.

5. **University** and the **Department** acknowledge that certain information provided by **University** to the **Department** under this Contract may constitute "Protected records" (as defined in Utah Code § 63G-2-103 and § 63G-2-305) and may be classified as such by the **Department. University** agrees to appropriately mark as "trade secret," "confidential" or with a similar designation any materials that it believes may qualify as "Protected records." Any such materials that the **Department** classifies as Protected records shall be protected by the **Department** as required by Utah Code § 63G-2-309.

G. **Conflicts.** The terms and conditions in the Agreement shall prevail in the event any terms and conditions herein conflict with any provision of the conditions set forth in these Privacy and Security Standard Terms and Conditions.

H. **Notices.** Any notices pertaining under these Privacy and Security Standard Terms and Conditions shall be in writing and addressed to the following individuals:

In an event of a Breach or Security Incident, **UNIVERSITY** shall also notify:

Chief Information Privacy/Security Officer
UTAH DEPARTMENT OF HEALTH

Attn: Francesca Lanier
288 N. 1460 W.
P.O. Box 144004
Salt Lake City, Utah
Phone: 801-538-6271
Mobile: 801-573-3176
E-mail: flanier@utah.gov