DRAFT

Data Release Policy for Utah's IBIS-PH Web-Based Query System, Utah Department of Health

1. Introduction

Public Health Assessment refers to the measurement and monitoring of health and well-being in the population. The Institute of Medicine* identified three core functions of public health agencies at all levels of government as follows:

1. Assessment (systematically collect, assemble, analyze, and make available information on the health of the community),
2. Policy Development (serve the public interest in the development of comprehensive public health policies), and
3. Assurance (assure their constituents that services necessary to achieve agreed upon goals are provided).

The Utah Department of Health regularly uses health data for the following purposes:

- Track and evaluate progress toward goals
- Guide policy decisions, priorities and long-range strategic plans
- Develop, focus, and streamline data collection and reporting capacity in the department
- Provide comprehensive information of Utah's health and health care system to inform anyone involved in private or public health activities

Public health practice is increasingly moving towards the use of indicators to assess and evaluate status and trends for specific health issues. Indicators have been developed for many

* The Institute of Medicine is a national health advisory institute chartered by the National Academy of Sciences. It issued a statement on the role of government in public health in its 1988 publication, *The Future of Public Health*.

priority health events. To enhance the capacity of Utah public health practitioners to perform public health assessment, the Utah Department of Health has developed the Indicator-Based Information System for Public Health (IBIS-PH). The website disseminates health data in the form of indicator profile reports and provides access to public health data sets through a web-based interactive IBIS-PH Query system.

The UDOH Data Release Policy Workgroup, consisting of the 2004 Data Stewards for data sets accessible through the IBIS-PH Query website, met approximately monthly for a period of four months from June through September 2004 to produce this written policy. The purpose of this Data Release Policy is to document the mechanisms we use to protect the identification of subjects represented within the IBIS-PH query system datasets. It describes the relevance of HIPAA as public health context for data release, the risks inherent in making data available to the public, and the considerations that have gone into current solutions that attempt to balance the benefits of information dissemination against the risk of inappropriate disclosure.

2. HIPAA, How It Applies and How It Doesn't

The Health Insurance Portability and Accountability Act (HIPAA)[1] is a federal law that was enacted in 1996 to permit data sharing and establish a standard for sharing that safeguards individual privacy. An excellent review of HIPAA and its relevance to public health activities may be found at: http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm [2]. Section 2. of this document has borrowed extensively from that article.

2.1 Protected Health Information

The HIPAA privacy rule applies only to "Protected Health Information" (PHI). For information to be considered PHI, it must have all of the following four characteristics:

- Health information
- With an identifier
- Transmitted or maintained by
- A covered entity.

"The Privacy Rule protects *certain information* that *covered entities* use and disclose. This information is called protected health information (PHI), which is generally individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) *the past, present, or future physical or mental health, or condition of an individual*; 2) *provision of health care to an individual*; or 3) *payment for the provision of health care to an individual*. If the information identifies *or provides a reasonable basis to believe it can be used to identify an individual*, it is considered individually identifiable health information." [2] [emphasis added]

Technically, the information that is on the IBIS website is not PHI because it derives from Utah Department of Health functions that are not covered by HIPAA. However, it is not

[1] Health Insurance Portability and Accountability Act of 1996. Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[2] Epidemiology Program Office, U.S. Centers for Disease Control and Prevention (2003) HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services. Mortality and Morbidity Weekly Report (MMWR), April 11, 2003, (52) 1-12. Atlanta, GA: Author.

sufficient merely to say that the information on IBIS is not PHI, and therefore no policy for protection of individual privacy is necessary.

2.2 Covered Entity

The Privacy Rule defines "covered entities" as health care providers who transmit health information electronically in connection with a transaction for which the Secretary has adopted standards. The Administrative Simplification standards adopted by HHS under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) apply to any entity that is: [3]

- a health care provider that conducts certain transactions in electronic form (called here a "covered health care provider")
- a health care clearinghouse
- a health plan

A public health department is not a covered entity. HIPAA makes special provisions for public health activities.

> "The Privacy Rule allows covered entities to disclose PHI to public health authorities when required by federal, tribal, state, or local laws [45 CFR 164.512(a)]. This includes state laws (or state procedures established under such law) that provide for receiving reporting of disease or injury, child abuse, birth, or death, or conducting public health surveillance, investigation, or intervention.
>
> "For disclosures not required by law, covered entities may still disclose, without authorization, to a public health authority authorized by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability, the minimum necessary information to accomplish the intended public health purpose of the disclosure [45 CFR 164.512 (b)]...
>
> "For example, to protect the health of the public, public health officials might need to obtain information related to persons affected by a disease. In certain cases, they might need to contact those affected to determine the cause of the disease to allow for actions to prevent further illness. The Privacy Rule continues to allow for the existing practice of sharing PHI with public health authorities who are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting adverse events, reporting births and deaths, and investigating the occurrence and cause of injury and disease (1).
>
> "Although it is not a defined term, DHHS interpreted the phrase 'authorized by law' to mean that a legal basis exists for the activity. Further, DHHS called the phrase 'a term of art,' including both actions that are permitted and actions that are required by law [64 FR 59929, November 3, 1999]. This does not mean a public health authority at the federal, tribal, state, or local level must have multiple disease or condition-specific laws that authorize each collection of information. Public health authorities operate under broad mandates to protect the health of their constituent populations." [2]

[3] Centers for Medicaid and Medicare Services, Covered Entity Decision Tools, Internet Resource: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp, accessed 7/14/2004.

2.3 Identified Data

The HIPAA privacy rule defines different levels of identification in public health data. The rule then specifies different allowable uses for data at those different levels of identification. De-identified data (e.g., aggregate statistical data or data stripped of individual identifiers) require no individual privacy protections and are not covered by the Privacy Rule. De-identifying can be conducted through complete or statistical de-identification.

Complete De-identification/Safe Harbor Method. At the most conservative end of the spectrum is completely de-identified information. This is health information in a data set in which none of 18 specific elements is present (see Table 1), *and* no knowledge that remaining information can (alone or in combination with other information) identify the individual. Complete de-identification is also called the "safe-harbor method." In this method, a covered entity or its business associate de-identifies information by removing all 18 identifiers and the covered entity does not have actual knowledge that the remaining information can be used alone or in combination with other data to identify the subject.[2]

Table 1: List of 18 Personal Identifiers that Must Be Removed From Data in Order for Those Data to Be Considered "Completely De-Identified"

1. names;
2. all geographic subdivisions smaller than a state, including county, city, street address, precinct, ZIP code and their equivalent geocodes;
3. all elements of dates (except year) directly related to an individual; all ages >89 and all elements of dates (including year) indicative of such age (except for an aggregate into a single category of age >90);
4. telephone numbers;
5. fax numbers;
6. electronic mail addresses;
7. Social Security numbers;
8. medical record numbers;
9. health-plan beneficiary numbers;
10. account numbers;
11. certificate and license numbers;
12. vehicle identifiers and serial numbers, including license plate numbers;
13. medical device identifiers and serial numbers;
14. Internet universal resource locators (URLs);
15. Internet protocol (IP) addresses;
16. biometric identifiers including fingerprints and voice prints;
17. full-face photographic images and any comparable images; and
18. any other unique identifying number, characteristic, or code, except that covered identities may, under certain circumstances, assign a code or other means of record identification that allows de-identified information to be re-identified.

Source: HIPAA and public health: http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

* The first three digits of a ZIP code are excluded from the PHI list if the geographic unit formed by combining all zip codes with the same first three digits contains >20,000 persons.

Statistical De-identification. Statistically "de-identified" information is information for which a *qualified statistician,* using accepted analytic techniques, concludes that there is a "very small" risk that the information could be used, alone or in combination with other reasonably available information, to identify the individual. The methods and results of the analysis that was used to support the risk assessment must be documented.

Limited Data Set. In certain instances, working with de-identified data may have limited value to clinical research and other activities. When that is the case, a limited data set may be useful.

Health information in a limited data set is not directly identifiable, but may contain more identifiers than completely de-identified data that has been stripped of the 18 identifiers in Table 1. Of the 18 identifiers in Table 1., date elements (#3) and town or city, state, and ZIP Code (elements of #2) MAY be included in the data set, and it will qualify as a limited data set: [4]

Table 2: List of 16 Personal Identifiers that Must Be Removed From Data in a Limited Data Set

1. Names.
2. Postal address information, **other than** town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face photographic images and any comparable images.

A data-use agreement must establish who is permitted to use or receive the limited data set, and provide that the recipient will

- not use or disclose the information other than as permitted by the agreement or as otherwise required by law;
- use appropriate safeguards to prevent uses or disclosures of the information that are inconsistent with the data-use agreement;
- report to the covered entity any use or disclosure of the information, in violation of the agreement, of which it becomes aware;
- ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- not attempt to re-identify the information or contact the individual.

"If a covered entity is the recipient of a limited data set and violates the data use agreement, it is deemed to have violated the Privacy Rule. If the covered entity

[4] Department of Health and Human Services. Protecting personal health information in research --- understanding the HIPAA Privacy Rule. Department of Health and Human Services. Washington, D.C.: 2003 http://privacyruleandresearch.nih.gov/pr_02.asp

providing the limited data set knows of a pattern of activity or practice by the recipient that constitutes a material breach or violation of the data use agreement, the covered entity must take reasonable steps to correct the inappropriate activity or practice. If the steps are not successful, the covered entity must discontinue disclosure of PHI to the recipient and notify HHS."[4]

2.4 Use of Data for Research

The provisions for use and disclosure of PHI for research purposes applies only to covered entities. Because the UDOH responds to requests for data for both research and other purposes, those provisions are summarized in this document as a convenience to the reader.

In the case of public health research, the Privacy Rule provides separate provisions for disclosure of PHI by covered entities without authorization from the individual. De-identified PHI may be disclosed without authorization. PHI may also be used if the individual provides written permission in the form of an Authorization. Covered entities may use and disclose PHI for research without an Authorization in limited circumstances:

- Under a waiver of the Authorization requirement in which an IRB or Privacy Board determines that the research involves no more than minimal risk to participants and that the use of PHI is necessary and authorization is impractical, and provides written documentation of the waiver,
- as a limited data set with a data use agreement,
- preparatory to research, and
- for research on decedents' information.[4]

The Privacy Rule defines research as, "systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[2]

> "Research is designed to test a hypothesis, permit conclusions to be drawn, and thereby to develop or contribute to generalizable knowledge. The majority of public health activities (e.g., public health surveillance, and disease prevention and control projects) are based on scientific evidence and data collection or analytic methods similar to those used in research. However, they are not designed to contribute to generalizable knowledge. Their primary purpose is to protect the health of the population through such activities as disease surveillance, prevention, or control.
>
> "The Belmont Report (11)[5] defines practice as interventions designed solely to enhance the well-being of a person, patient, or client, and which have reasonable expectation of success. The report further states that the purpose of medical or behavioral practice is to provide diagnosis, preventive treatment, or therapy to particular patients. For public health agencies, the patient is the community. Public health practice activities (e.g., public health surveillance, disease control, or program evaluation) are undertaken with the intent to benefit a specific community, although occasionally they may provide unintended generalizable benefits to others."[2]

[5] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Belmont report: ethical principles and guidelines for the protection of human subjects of research. Department of Health, Education and Welfare. Available at http://www.med.umich.edu/irbmed/ethics/belmont/BELMONTR.HTM.

2.5 Tracking Use and Disclosure of Data

Covered entities must maintain an accounting of certain disclosures of PHI. However, even covered entities are not required to account for all disclosures of PHI, such as disclosures made as part of a limited data set.

To summarize the applicability of the HIPAA Privacy Rule to the dissemination of population health data using the IBIS-PH Query System, the data accessible on IBIS, although not "Protected Health Information" by definition (because the UDOH is not a covered entity) probably best meets the definition of a Limited Data Set. The IBIS website does utilize a Data Use Agreement that all users must agree to prior to use of the data.

3. Data Dissemination: Value and Risks

3.1 Using Data to Inform Resource Allocation, Policy and Program Decisions

The problem of making evidence-based public health policy, management, clinical, and personal decisions affects public health practitioners, whether they are in traditional public health environments (i.e., public sector health departments), health plans, private providers, educators, and members of the general public. The citizens of Utah benefit from the availability of good public health data. Without accurate and timely public health assessment information, public health dollars are wasted, opportunities for prevention are missed, and individual lives are endangered.

- Public health policy makers need accurate and timely information on the health of the population to make informed decisions on resource allocation, legal and regulatory interventions, public information campaigns and more.
- Public health managers need public health assessment information to plan, target, and implement effective programs that control and prevent adverse health events, evaluate progress toward health objectives, and manage their budgets and long-range strategic plans.
- Health educators need information to provide useful and credible information, including specific local examples, to the students and the public.
- Teachers need accurate and timely information and information resources to pass along to their students.
- Health plans need information to improve the health of their insured populations, plan effectively for change, and promote disease prevention activities among their insured members and providers.
- Private providers need information to direct useful, timely and appropriate healthy lifestyle and disease prevention messages to their patients.
- Public administrators (e.g., local boards of health, healthy communities initiatives) need accurate and timely public health information to make informed decisions on resource allocation, legal and regulatory interventions.
- Members of the general public need information to make healthy lifestyle and disease prevention decisions.

3.2 Examples of Public Benefit From Use of IBIS Data

What follows are three anecdotes illustrating uses of IBIS data to improve health status and health systems in the state.

Program Manager, Cardiovascular Health Program, Bureau of Health Promotion. Because of the data available to us on IBIS, we were able to describe incidence, mortality, hospitalizations, costs, target populations, average age of death, primary payers of hospital costs, discharge status, etc. for each type of stroke. This influenced neurologists and emergency room personnel in Wasatch Front hospitals, documenting the increasing problems of stroke, and the impact changing the system of emergency care in the hospital ER might have on stroke outcomes. Because we had these data, we have been able to educate the physicians and ER personnel, bring them together in an action group, and we are on our way to improving emergency care for stroke. We would not have been able to do this without IBIS.

Program Manager, Cancer Control Program, Bureau of Health Promotion. Colorectal cancer is the second leading cause of cancer-related deaths in the U.S. and Utah. Screening for this cancer is important as deaths can be substantially reduced when precancerous polyps are detected early and removed. When colorectal cancers are detected at an early, localized stage of disease, the 5-year survival rate is 90%. However, only 37% of colorectal cancers are discovered at that stage. Several scientific organizations recommend that routine screening for colorectal cancer begin at age 50 for adults at average risk.

In 2001 the Utah Cancer Control Program applied to the Centers for Disease Control and Prevention (CDC) for a grant to fund a colorectal cancer screening public education campaign. Evidence to support the grant application was obtained from IBIS. The data included the 2001 Utah colorectal cancer death rate of 13.7 per 100,000 population and the use of colorectal cancer screening tests by Utahns aged 50 and older within the last 5 years of only 31%.

In June 2002 the Utah Cancer Control Program received grant funding from the CDC to launch a statewide colorectal cancer screening public education campaign. Additional funds were received in June 2003 to continue this effort.

The proportion of Utahns aged 50 or older who report having had a colorectal cancer screening test within the past five years will be monitored annually and should increase, thereby decreasing the death rate due to colorectal cancer among this population.

Community Developer, Midvale City, Utah. Midvale City's Community-Building-Community Initiative (CBC) began almost 6 years ago in response to health data presented by UDOH. It was the first time data was broken down by zipcode; since Midvale City is one zipcode, this was extremely useful for the City. Infant mortality rates were twice as high as the state and county and surrounding communities. Suicide rates were also very high. In the intervening years, we have continued to track a series of 12-15 data points to gauge what the CBC needs to improve and what is improving. Tracking data is time consuming and often difficult. Over the past few years, it has been difficult to keep the data points current.

At several Health Department meetings, I had heard that the IBIS system was being designed and would soon be available for use. Now that the system is up and running, it has made data collection for health indicators much simpler, quicker, and easier to create data sheets and graphs for presentations and distribution. Last year, the CBC team (more than 160 organizations and community members) met to celebrate successes of the past year and kick-off

the new year. Mayor Seghini presented information on the infant mortality rate to the team: 5 years after the CBC was formed and had instituted community wide emphasis on infant mortality (including applying for and receiving a March of Dimes grant), the rate had been cut in half and was only a few tenths of a point away from the county and state levels. The team cheered and the Mayor cried. Today, more babies are alive and healthier in Midvale than otherwise would have been. Recently, I have been able to report to the Mayor and the CBC Board that suicide rates have dropped significantly. While the county and state rates are also dropping, Midvale rates are dropping more quickly. I retrieved this data from the IBIS website and was able to compare it to other cities surrounding Midvale, the county, and state.

A few months ago, while updating the CBC data indicators, I checked the teen birth rate using the IBIS website—a data indicator not previously tracked by the CBC. The numbers were alarming—Midvale rates are more than double the state rates and soaring. I have presented this data to the Mayor, the City Administrator, the Director of Economic and Community Development, and the CBC Board. All agree that the CBC needs to address the teen birth rate along with its other activities. Next month, the data will be presented to the CBC Health Committee. The Board has met twice to discuss the issue and how to proceed. They have outlined an action plan and set activities for the next few months. The Mayor will address the issue in various settings to the community and a religious summit will be held in the spring to present the problem to the religious leaders and seek their help and support. Resources and program models are currently being identified and collected. The CBC team and City administration believe that the teen birth rate can be reduced, improving the health (pregnancy, STDs, etc.) and general well being of Midvale teens, while preventing problematic births.

The IBIS system is extremely useful to me in my job as Midvale's Community Developer and benefits the entire community.

3.3 Assessment of Risks to the Public

The practice of making data available to the public presents an ethical challenge. As articulated in the preceeding sections, the data are extremely valuable for public policy decision-making and provide for the public good. However, the data should be made available without personal identifiers, and to the extent possible, in such a way that no individual represented within the data set may be identified. As a public agency, the Utah Department of Health, its officers, agents, volunteers, and employees, have an obligation to the public to protect the information entrusted to it to prevent harm coming to any individual as a result of release of the information. We have this obligation, regardless of HIPAA. However, as a set a guidelines, the HIPAA privacy rule provides a good framework for drafting our policy, including definitions of terms and guidelines for disclosure.

The UDOH Data Release Policy Workgroup, consisting of the Data Stewards for data sets accessible through the IBIS-PH Query website, has assessed the potential for identification of individuals in the various data accessible through the website. The following describes the results of our assessment.

1. IBIS website data are not "completely de-identified," primarily because IBIS provides access to geographic subdivisions smaller than the state; most commonly county and zip code, or zip code combinations known as, "Utah's 61 Small Areas."
2. IBIS website data contain certain information that is sensitive. Although it is not, by definition, Protected Health Information (PHI) because the UDOH is not a covered entity, it does contain information on individuals, including mental and physical

health status, health care, and payment for health care. In this sense, it is PHI-type data.

3. IBIS datasets do contain unique records. That is, using only non-PHI-type data elements available through the website, such as year, county, age, and sex, it would be theoretically possible for a user to "drill down" to a single data record. In the case of our survey data sets, a user could do so in the majority of data records.
   a. The ability to drill down to a unique data record is constrained primarily by use of "cell suppression." Although no cell suppression algorithm is completely foolproof, it does provide a barrier, especially to persons who are casual users of the data and are not consciously trying to circumvent the cell suppression system.
   b. The ability to do so does not necessarily mean that an individual from the population may be identified. Knowing that there was only one Asian male age 26 who contracted HIV/AIDS is not enough to identify that individual. One must also know the incidence of 26 year old Asian males in the population. In Salt Lake County, there are several, in other counties there will be fewer.
   c. In most cases, an individual may not be identified solely by the information in a limited data set, even when there is only one individual with those characteristics in the population. Typically, to identify the individual, one must have access to other information about that individual. Some information is readily accessible, such as the individual's county of residence, race, or pregnancy status. Other information is less readily available, such as the fact that an individual had a hospital or emergency department visit during a calendar year. Still other information would be almost impossible to know, for instance, that an individual responded to a telephone survey during a calendar year. Any analysis of the risk of identification of an individual must take into account the availability of other information that would, if used in conjunction with the information in the database, would identify an individual represented in the data.
4. We currently have a data use agreement that meets the criteria set forth by HIPAA for disclosure of limited data sets by covered entities. It is neither formal nor explicit, but it does attempt to communicate to the user 1) who is afforded access to the data, 2) for what purposes, and 3) states conditions for use of the data. The Data Use Agreement may be found in Appendix 1.
5. Protecting the privacy of individuals represented in the IBIS data sets may only be assured to the extent that the physical security of the data is assured. IBIS data stewards help to ensure security of IBIS data sets through standard precautions, such as protecting their computer passwords and keeping identified data records in locked cabinets.

4. Data Release Policy for the IBIS-PH Web-Based Data Query Tool

The following policy was drafted in response to the obligation experienced by the UDOH to protect the public's interest. The policy attempts to seek a balance between providing access to valuable data for purposes of public health decision-making, while minimizing the risk of exposure of individually identified health information.

Relationship to HIPAA. As defined by the HIPAA Privacy Rule, the data on the IBIS website is not Protected Health Information (PHI) because the UDOH is not a covered entity. If the UDOH *were* a covered entity, each IBIS data set would meet the definition of a "limited data set."

Data Use Agreement. In accordance with the requirements of disclosure of a limited data set under the HIPAA Privacy Rule, it is our policy to provide a data use agreement for IBIS data query users. The agreement is in the form of a computer screen that a user must pass through to get from the IBIS homepage to the query system. Users must agree to the stated conditions for use of the data in order to get past that screen. It should be noted that, once past that screen, a user may bookmark the query system and avoid the screen in future sessions. It should also be noted that the data use agreement is implicit in use of the system, and that we have no explicit or formal, signed data use agreement in place, and no mechanism in place to track use of the system back to individual users. It is believed that requiring users to sign a written data use agreement prior to use of the IBIS system is not warranted given the limited ability to identify individuals in the data, and that it would impose restrictions that would inhibit legitimate use of the data for its intended purposes. The data use agreement (see Appendix 1.) is compliant with the HIPAA definition of a data use agreement.

Cell Suppression. For the IBIS-PH Query System application, it is not enough merely to provide a limited data set under an implicit data use agreement. Just because we *can* release individual-level information doesn't mean that we should. In an effort to ensure that the IBIS-PH Query system may not be used to identify an individual, the UDOH will implement a cell supression algorithm so that data results with fewer than five cases in the numerator and fewer than 30 cases in the denominator will not be made available to the user.

Computer System Security. All reasonable precautions to protect the electronic data records in the limited data sets on the IBIS server shall be taken by staff in the UDOH Office of Information Technology. Server operating systems must be maintained, and "security patches" to operating system software must be implemented as soon as they become available. The network architecture shall employ current I.T. industry best practices to protect the stored data from intrusion, such as the use of a three-tiered network architecture and protection of the server IP address from public discovery.

Data Sharing Agreement. Although the scope of this policy was not originally intended to reach beyond Internet access to IBIS-PH data, the IBIS Data Release Policy Workgroup selected to include a data sharing agreement example. UDOH data stewards who release data sets to researchers or others shall use a data sharing agreement similar to the example agreement shown in Appendix 2.

Appendix 1. – Online Query Data Use Agreement

What follows the data use agreement currently displayed on the IBIS website. This agreement is shown to any user who navigates to the Custom Query section of the website from the IBIS-PH home page. Users must click on the "OK" button to proceed to the query system.

Utah Department of Health
IBIS Query System, Data Use Agreement

The data and information provided through the IBIS-PH Query System are intended to support any individuals or entities engaged in activities designed solely to enhance the well-being of a specific community, which may include State of Utah. Activities include informing evidence-based decision making in Utah to plan and improve health service delivery, evaluate health care interventions and systems, and inform health policy decisions. **Other uses are not permissible.**

As an IBIS-PH Query System user, I agree to:

- Use the data for statistical reporting and analysis only.
- Avoid any attempt to identify or contact individual(s) represented in the IBIS-PH query system data.
- Avoid disclosure or use of the identity of any individual(s) discovered inadvertently.
- Avoid linkage of IBIS-PH query system data with other data that, after linkage, might allow identification of an individual represented in the IBIS-PH query system data.
- Use appropriate safeguards to prevent the inappropriate use or disclosure of individual(s) represented in the data, including when disclosing IBIS-PH Query System data to others.
- Report IMMEDIATELY any inadvertent or intentional identity disclosures or violations of this agreement of which I become aware to the Director of the Center for Public Health Data, Utah Department of Health.

I understand that failure to adhere to the above stated agreement items will result in loss of access to UDOH Internet databases, and I may be subject to legal penalties. Any use, release, or publication of health data contrary to the provisions stated is a class B misdemeanor, with subsequent violation begin class A misdemeanors punishable by a fine of up to $5,000 per offense (Chapter 23, Title 26, Utah Code Annotated). If I am a Utah state government employee, this may be grounds for immediate dismissal.

Press the [OK] button to accept the stated conditions, or press the [Cancel] button to decline.

OK Cancel

Appendix 2. – Example Data Sharing Agreement

What follows is an example data sharing agreement. This is one used by the Reproductive Health Program, Maternal and Child Health Bureau, Utah Department of Health for sharing of Pregnancy Risk Assessment and Monitoring (PRAMS) survey data.

UTAH DEPARTMENT OF HEALTH
DATA SHARING AGREEMENT

BACKGROUND

Data are essential to the mission and purpose of the Department of Health (Department). Data collected by organizational units or individuals within the Department are collected under the authority of the Department and the stewardship and use of those data are ultimately the responsibility of the Department. The missions and purposes of organizational units within the Department overlap in many instances and sharing data will often help the Department to accomplish its mission.

Organizational units and individuals within the Department are responsible for maintaining the integrity and confidentiality of data, acting as stewards of the Department's responsibility and authority. In many cases, use of data is governed by specific state and/ or federal statutes. In general, when identifiable data are shared with Department data users, other than the organizational unit charged with data stewardship, a written data sharing agreement should be enacted to assure that data are used and managed in accordance with those statutes and with other established policies to protect the confidentiality and integrity of the data. This model data sharing agreement is suggested for that use.

Requester

Division/Office: _____
Bureau/Program: _____
Data User(s): _____
_____
_____
Supervisor: _____
Address: _____
_____
Phone: _____

Data Provider

Division/Office: _____
Bureau/Program: _____
Data Steward: _____
Address: _____
Phone: _____

I. PURPOSE

State the purpose(s) of the agreement, i.e., how the data will be used, what studies will be performed, or what the desired outcomes are perceived to be as a result of obtaining the data.

II. PERIOD OF AGREEMENT

The period of agreement shall extend from __starting date__ to __ending date__, unless sooner terminated as provided herein.

III. JUSTIFICATION FOR ACCESS

The Utah PRAMS project data will be used for academic research only. All papers, pre-publications will be submitted to the project's Data Manager who will check for accuracy of results and for assurances of confidentiality.

IV. DESCRIPTION OF DATA

Provide specific detailed information concerning the data to be shared or exchanged, including definitions of the subjects or records to be included and the data elements needed.

V. METHOD OF DATA ACCESS OR TRANSFER

A de-identified SAS dataset will be provided on compact disc.

VI. LOCATION OF DATA AND CUSTODIAL RESPONSIBILITY

_____ (organizational unit and/or individual) will be the "Custodian" of the file(s) and will be responsible for observing all conditions for use, for establishing and maintaining security as specified in this agreement to prevent unauthorized use.

State where and how the data will be stored and maintained.

This agreement represents and warrants further that, except as specified in an attachment or except as authorized in writing, that the data covered by this agreement shall not be disclosed, released, revealed, showed, sold, rented, leased, loaned or otherwise have access granted to any person. Access to the data covered by this agreement shall be limited to the minimum number of individuals necessary to achieve the purpose stated in this agreement and to those individuals on a need-to-know basis only.

Any results of data matching that contain individually identifiable data cannot be released to persons except as authorized in this agreement.

Summary results (those items which cannot be used to identify any individual) of analyses conducted as part of this agreement can be shared.

VII. CONFIDENTIALITY

The User agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it.

VIII. DISPOSITION OF DATA

The requestor and its agents will destroy the requested PRAMS data, any data files produced from it, and any printouts or other copies of the data that contain individual level survey responses as soon as the purposes of the project have been accomplished or by the data this agreement terminates and notify the PRAMS Data Manager to this effect in writing.

IX. DATA-SHARING PROJECT COSTS AND RESOURCES

Data will be provided free of charge. The user agrees to provide their own data analysis software

X. SIGNATURES

In witness whereof, the authorized representatives attest to and execute this agreement effective with this signing for the period set forth in Article III.

_____	_____
(Signature)	(Signature)
_____	_____
(Type/print name)	(Type/print nane)
_____	_____
(Title)	(Title)
_____	_____
(Date)	(Date)

Data Steward

_____	_____
(Signature)	(Date)

~~~~~~

IBIS Data Release Policy Document -- Revision History

Created	6/14/2004	Lois M. Haggard, UDOH
Revised	7/14/2004	Lois M. Haggard, UDOH
Revised	7/14/2004, PM	Lois M. Haggard, UDOH
Revised	8/10/2004	Lois M. Haggard, UDOH
Revised	8/25/2004	Lois M. Haggard, UDOH
Revised	10/5/2004	Lois M. Haggard, UDOH
Revised	10/15/2004	Lois M. Haggard, UDOH
Revised	11/5/2004 (typos)	Lois M. Haggard, UDOH
~~~~~~