As expanding use of health information technology generates larger volumes of health care data, organizations need to realize the value of this information. At the same time, organizations must preserve the confidentiality of these data since an adverse disclosure event can be catastrophic.

The result is a growing demand for expertise and tools to both manage the risk of inadvertent disclosure and maximize data utility.

**NORC OFFERS EXPERTS AND SOLUTIONS TO ADDRESS THIS DEMAND**

NORC’s practice in disclosure-safe data dissemination covers a broad spectrum, from data access to data de-identification and data re-identification threat analysis.

**Data De-Identification:** NORC’s X-ID generates HIPAA-compliant, disclosure-safe public use files, with maximum data utility and minimized risk.

**Secure Data Access:** NORC’s Data Enclave provides secure remote access to confidential microdata for authorized users.

**CONTROLLING DISCLOSURE SAFETY THROUGH ASSESSMENT AND DE-IDENTIFICATION**

NORC is skilled in developing methods for evaluating and reducing the risk of a disclosure event, thereby adding rigor to disclosure-limitation rules for both tabular and microdata, and in assessing the impact of disclosure limitation on data quality.

While many data producers currently rely on removing variables altogether or suppressing data to limit the risk of disclosure, such approaches, including HIPAA Safe Harbor, are limited in their effectiveness. These approaches typically remove too much valuable data that have analytic utility. Also, in many cases, the remaining data are still vulnerable to attack as portions of the data frequently are available on multiple data systems, and those partial records can be used to re-identify records on data that have been treated using HIPAA Safe Harbor methods.

**NORC’S X-ID SOLUTION: MAXIMIZING DATA UTILITY, MINIMIZING RISK**

NORC provides advice on best practices of statistical disclosure limitation to enable release of data for health analysts and policymakers. NORC has provided guidelines for federal agencies within a unified principled framework of de-identification based on data-specific risk-utility trade-off analysis in order to mitigate the mosaic effect. In particular, NORC’s X-ID solution protects individual identities in unit-level data so clients can use a full range of analytics as well as methods for collaboration and dissemination.

NORC X-ID is the only de-identification solution that applies a unique micro-grouping method to eliminate the risk of re-identification associated with using unit-level data. This method provides for better data utility by allowing the inclusion of variables typically excluded through other de-identification processes, while also eliminating the suppression of specific levels of other variables. X-ID further reduces and controls disclosure risk by replacing true micro-group-level data values with unbiased estimates derived from subsampling the source data.

NORC’s prior experience working with the U.S. Census Bureau, the Social Security Administration, the National Center for Education Statistics, the Bureau of Labor Statistics, and the Office of the Assistant Secretary for Planning and Evaluation at the U.S. Department of Health and Human Services, among others, attests to a rich background in working with sensitive, protected data that nonetheless must be made useful to those seeking informed evaluations and decisions on issues of social policy and programs. Visit [XID.NORC.org](http://XID.NORC.org) for more information.
GENERATING SYNTHETIC HEALTH CARE DATA

Synthetic data can serve multiple purposes, but perhaps one of the most important is its utility for developers of analytic systems and workflows. Developers need test data that are structured exactly as the data to which their systems will eventually be applied. However, they do not have to be encumbered by the restrictions placed on access to personal health information while they do their work writing and testing software.

NORC has skills and expertise in health care data formats and in the generation of 100 percent disclosure-safe synthetic public use files of any size suitable for testing both the functionality and performance of newly developed analytic software and workflows.

NORC’S DATA ENCLAVE: ENSURING DISCLOSURE SAFETY OF DATA

The Data Enclave is NORC’s proprietary secure research environment and is recognized as the standard for providing access to sensitive data. By creating and hosting custom platforms on secure NORC servers, the Data Enclave enables clients to store, manage, and facilitate the remote analysis of data—unlocking the power of large, complex datasets.

Researchers’ access to the Data Enclave is strictly controlled by the latest secure gateway technology. With this approach, the user’s “home” session is equivalent to a remote terminal with no local processing or data capture capabilities, thus reducing the risk of security breach and/or nefarious tampering. Additionally, access requires multi-factor authentication, ensuring that only authorized users are granted access to the data to which their authorization applies.

The NORC Data Enclave operates under a National Institute of Standards and Technology (NIST)-approved System Certification and Accreditation framework, including an approved Information Technology (IT) Security Plan, Data Protection Plan, and a System Certification Test Plan, as outlined in the Department of Commerce IT Security Program Policy, Section 6.5.2. NORC’s Data Enclave IT Security Plan is fully compliant with the Federal Information Security Management Act, provisions of mandatory Federal Information Processing Standards, and meets all of NIST’s IT, data, system, and physical security recommendations.

NORC’s Data Enclave support team offers a full cycle of data services, ranging from study design and concept to data archiving and access. In addition to a full range of analytic software tools available to the Data Enclave user within its secure processing environment, the Data Enclave team can provide a comprehensive set of analytic services.

- Statistical Analysis
- Disclosure Analysis
- Data Cleaning and Coding
- Imputation
- De-Identification
- Data Visualization Tools
- Data Harmonization

About NORC at the University of Chicago

NORC at the University of Chicago is an independent research institution that delivers reliable data and rigorous analysis to guide critical programmatic, business, and policy decisions. Since 1941, NORC has conducted groundbreaking studies, created and applied innovative methods and tools, and advanced principles of scientific integrity and collaboration. Today, government, corporate, and nonprofit clients around the world partner with NORC to transform increasingly complex information into useful knowledge.

NORC has built a team of professional disclosure experts who use scientific principles and statistical methods to assign suitable measures of disclosure risk and data utility, through its work on large and complex projects for clients such as the Centers for Medicare & Medicaid Services, Centers for Disease Control and Prevention, Federal Reserve Board, Bureau of Labor Statistics, and others.