Office of Retirement and Disability Policy • Office of Research, Evaluation, and Statistics

Research and Statistics Note

No. 2009-01 July 2009

Access Restrictions and Confidentiality Protections in the Health and Retirement Study

*By Lionel P. Deang and Paul S. Davies**

Introduction

Organizations involved in statistical surveys of human subjects face two important and competing challenges: protecting data confidentiality while maximizing data accessibility to potential researchers (Singer 2005; National Research Council 2000). Protecting confidentiality becomes more difficult as the amount of microdata collected increases. This occurs when surveys collect longitudinal data, or when microdata are linked to contextual data or matched to administrative records. Repeated interviews of the same respondents increase their chances of being identified simply because of the accumulation of detailed personal information. By the same token, linkage of survey data with administrative records adds more distinguishing individual attributes to the data (GAO 2001). When taken together, large cumulated personal information significantly increases the chances of establishing an individual's uniqueness and, therefore, being identified.

Protection of confidentiality matters not only to survey respondents but also to the research community. In sample surveys, it is typical to give respondents an assurance of anonymity before an interview starts. The aim is to gain the respondent's trust and cooperation, as these are major determinants of the quality of survey responses collected. Indications of mistrust of government-sponsored surveys already exist (National Research Council 2005). Violations of confidentiality would likely exacerbate such negative perceptions.

To protect confidentiality, organizations design, organize, and distribute their statistical data in a manner intended to prevent identification of respondents. For instance, datasets released for public use are stripped of personal identifiers. Sensitive data are masked, collapsed, or recoded into broader variable categories. Earnings and benefits variables such as those from the Social Security Administration (SSA) in the Health and Retirement Study (HRS) are rounded or top coded. Similarly, geographic classifications are limited to broad levels of aggregation (for example, census divisions instead of states, or states

*Office of Research, Evaluation, and Statistics, Social Security Administration.

This note was presented at the 2008 Federal Committee on Statistical Methodology Statistical Policy Seminar, "Beyond 2010: Confronting the Challenges," November 18–19, 2008.

Acknowledgments: The authors are grateful to Irena Dushi, Susan Grad, Howard Iams, Michael Nolte, Carolyn Puckett, and David Weir for helpful comments and suggestions. Any remaining errors are the responsibility of the authors.

instead of counties). In response to elevated risks of identification due to advances in computing technology, more sophisticated data-masking methodologies have been developed. For example, statistically valid synthetic data that contain no actual individual records from the restricted data on which they are based can be generated. The synthetic data then can be released publicly (Abowd, Stinson, and Benedetto 2006; Abowd and Lane 2003; Singh, Yu, and Dunteman 2003). In totality, these disclosure-avoidance and data modification techniques make respondent identification difficult and permit at least limited public distribution of otherwise restricted data.

Selected Abbreviations

HRS	Health and Retirement Study
MICDA	Michigan Center on Demography and Aging
NCES	National Center for Education Statistics
NCHS	National Center for Health Statistics
PI	principal investigator
SSA	Social Security Administration

Although data modification serves to maintain anonymity and confidentiality, it also reduces the precision of collected information. This can affect researchers' choice of analytical techniques. Contextual analysis, for instance, may not be so useful when only very broad geographic classifications are available. Likewise, the absence of specific demographic details such as birth and death dates may limit the usefulness of survival analysis methods. Excised data may prevent studies that researchers would do if the raw data were available. In short, data modification can diminish data usage.

Facing these trade-offs, organizations devise data access procedures that aim for the optimal balance between respondent anonymity and researcher data usage. Organizations often complement their public-use files with restricted-use data files. The Census Bureau, the National Center for Health Statistics (NCHS), the National Center for Education Statistics (NCES), and the Institute for Social Research of the University of Michigan, which conducts the HRS, are four organizations that have both public-use and restricted data files. Use of restricted files is permitted only under tight screening procedures. Presently, these organizations use one or more of three methods to make their restricted files available to the research community: a) licensing, b) use of a research data center, and c) remote processing. The cost in researcher time and money, as well as the risk of confidentiality violations, varies between these methods.

This note looks at how the HRS attempts to balance data confidentiality with the desire to broaden the pool of potential data users. We first briefly note SSA's stake in giving access to its administrative data and concomitant concerns about confidentiality protections. We then summarize the current procedures for accessing the HRS restricted-use data[1] and compare them with those used by the Census Bureau, NCHS, and NCES. We also discuss potential ways to expand HRS use without compromising confidentiality.

SSA Data in the HRS

The HRS asks its respondents to allow SSA to release certain information from their Social Security program records to the HRS. In fact, SSA provides funding to the HRS to support efforts to increase the percentage of respondents who agree to sign the data-matching consent form.[2] For those who consent, a variety of personal information is available in various waves of the HRS restricted data. Such information includes Social Security covered wage and self-employment earnings; Old-Age, Survivor, and

[1] Details of the access procedures can be found at the HRS website http://hrsonline.isr.umich.edu.

[2] Actually, respondents are asked to sign the form twice—one signature to permit SSA to release benefits information to HRS, and a second signature to authorize the release of earnings information to HRS. Presumably, respondents may choose to authorize one, both, or neither release.

Disability Insurance (OASDI) benefits; Supplemental Security Income (SSI) benefits; and projected earnings and Social Security benefits. Note that SSA collects earnings and benefits data primarily for the administration of the Social Security and SSI programs, and not for research purposes. Because they are federal program data and are matched to HRS survey data, confidentiality protection is provided by various laws and federal regulations, such as the Privacy Act, the Federal Policy for the Protection of Human Subjects, certain SSA laws and regulations, and the Internal Revenue Code (GAO 2001; Singer 2005).

SSA Concerns

Given the sensitivity and the legal protections of SSA administrative data, there are concerns about their distribution and use. SSA's prime concern is data security. Although the HRS handles the distribution of restricted data, SSA still has an ethical responsibility to maintain the confidentiality of its data. SSA also has an interest in promoting the use of the HRS-SSA restricted data. This has become the premier data source for studying questions related to retirement and Social Security, many of which have important policy implications. Moreover, some SSA researchers and many of the research projects funded by SSA through the Retirement Research Consortium use HRS public and restricted data.

The risk of confidentiality violations with HRS data is highest when respondents can be identified directly from variables contained in the data. The risk is substantially lower if specific identifier variables such as respondent name, address, Social Security number, and dates of birth, death, and marriage are removed from the data. However, even when they are stripped of such identification variables, datasets with detailed information contain other measures of personal characteristics that may lead to inferential identification of individual respondents. For example, as more variables are introduced, one can expect cross-tabulations to yield smaller and smaller cell frequencies, thus making it easier to identify individuals with a given combination of personal characteristics. Using narrow geographic areas to code respondents' residences produces a similar effect.

Violations also could occur if restricted data files are not adequately protected from unauthorized access. Unencrypted electronic data files are vulnerable to access by unauthorized persons. Housing restricted data on shared personal computers would increase the risk. Connectivity with networks and the Internet or even indirect connections through a variety of communications software would leave workstations vulnerable to outside intrusion. Likewise, the risk of intrusion would increase with the use of removable storage devices not encrypted or stowed in secure physical locations. Aware of these vulnerabilities, the HRS and SSA developed access procedures to safeguard confidentiality.

Granting Access to HRS Restricted Files

As mentioned earlier, three methods of granting data access are currently used by most statistical organizations: licensing, use of an onsite data center, and remote processing. The HRS mainly uses two of these methods: a license authorizing offsite use of HRS restricted data and, for those unable to obtain a license, use of an onsite research data center. The third method, remote access, is used by the HRS only as an adjunct to the onsite research data center method.

Licensing

The HRS uses licensing as its primary method of giving access to restricted files. A license can be secured only after meeting a stringent set of criteria that leads to a contractual agreement between the HRS and the researcher. The license enables the user to receive restricted files and use them at the researcher's own institutional facility.

For an offsite license, a potential user must meet the following requirements:

1. The applicant must be affiliated with an institution that has a "federal-wide assurance"—an Assurance of Compliance from the Office for Human Research Protections of the Department of Health and Human Services. In addition, the applicant must have a permanent, faculty-level appointment at an accredited academic institution. Most, but not all, research institutions are affiliated with colleges and universities with federal-wide assurance.
2. The applicant must be a principal investigator (PI) or co-PI of an ongoing research project funded by a federal agency. A researcher may apply for access to the HRS restricted datasets while applying for federal funding such that the applications for data access and funding will be reviewed concurrently. Once the funding application is approved by a U.S. government agency, access to the HRS restricted datasets can be granted almost simultaneously. The HRS limits restricted-data users to holders of a current federal grant primarily because potential loss of the grant is a deterrent to violating the use agreement. Violators may be sanctioned in a number of ways. HRS administrators may
    a. order the stoppage of restricted data use;
    b. report the violation to the funding agency and recommend the termination of the current grant;
    c. make additional recommendations for denial of future grants from various federal agencies; or
    d. report the violation to the institution with which the researcher is affiliated and request sanctions in accordance with the institution's policy on scientific integrity and misconduct.
3. The applicant must develop and submit to the HRS committee a one- to three-page research proposal detailing the reasons restricted data are needed and the particular variables that are to be used in the proposed research. Use of the restricted variables must be justified, and the applicant must explain why public-use files, which may contain variants of the restricted variables, would not meet the needs of the proposed research.
4. The applicant must develop and submit to the same committee a data protection plan. General guiding principles for the data protection plan include:
    a. Restricted-use data from the HRS must be protected from access by unauthorized persons. Any person other than the PI, co-PIs, research staff, and involved system administration personnel is unauthorized.
    b. The computing environment must be secure enough to protect HRS restricted data from intrusion by unauthorized persons. It must be structured and managed in such a way that it precludes the sharing of restricted HRS files. A preferred computing environment is one in which restricted HRS files are housed and processed on a standalone workstation that is not connected to the outside world through the Internet, FTP, or any electronic means. An additional layer of security is provided when the computing environment is restricted and confined in a room that can be locked and dedicated solely to the use of authorized project personnel. Removable storage media containing restricted HRS files must be kept in a locked cabinet, preferably located within the dedicated working room. The guiding principle is isolation of the restricted HRS files, limiting access only to authorized project personnel.
    c. Hard copies of output processed from restricted HRS files must be protected from viewing by nonproject personnel. In this regard, preference is given to dedicated printers installed in the project working room.
    d. Any plan to link restricted HRS datasets to other HRS and non-HRS datasets must be explicitly stated in the data development plan. Any linking plan must meet the following conditions:

i. A restricted HRS dataset may not be linked to any other restricted HRS dataset without explicit written permission from the HRS.

ii. Administrative data from SSA may not be linked to datasets containing geographic variables smaller than census divisions. Use of narrower geographic areas with SSA data requires the approval of SSA and use of the data is restricted to the secure Data Enclave (described below).

5. The applicant must submit a certification from the Institutional Review Board/Human Subjects Review Committee of the applicant's institution that it has received and approved the data protection plan previously approved by the HRS data confidentiality committee.
6. The applicant must comply with the data use agreement. Significant items in this agreement stipulate
   a. use of the data for research and statistical purposes only;
   b. strict adherence to HRS disclosure guidelines, which allow only the reporting of summary information;[3]
   c. use of the data solely for the project approved by the HRS and not for any other research;
   d. signing by all persons who will have access to restricted data as well as a representative of the receiving institution of the "Agreement for Use of Restricted Data" form prepared by the HRS;
   e. destruction of the original restricted data files and any derived variables from them in accordance with the date in the agreement or upon demand by the HRS; and
   f. consent to treat any violation to the agreement also as a violation of the institution's policies on scientific integrity and misconduct, in that a representative of the researcher's institution is a signatory to the agreement.

Research Data Center

With the strict requirements for a license, many potential researchers would not qualify. These would include junior researchers who may have fellowship appointments but do not have a tenure-track faculty position at a college or university. Most graduate students also would not qualify for a license as they are likely not to have a permanent faculty position and a research project that is federally funded.[4] For these researchers, the HRS offers the use of a secure research data center to access HRS restricted data: the Michigan Center on the Demography of Aging (MICDA) Data Enclave.

The Data Enclave is a secure research facility located in the Institute for Social Research building of the University of Michigan, Ann Arbor. To maintain utmost security, the facility isolates its computer network. There is no connection to the Internet or to any other local or wide area networks. Four workstations are connected to the server which contains the computer software, statistical applications, and utilities that a user is likely to need for his or her analysis. A systems administrator maintains the network and resident staff provide computing-related assistance to Data Enclave users. The facility also provides office space for users.

---

[3] Summary information refers to tabulations and other descriptive summary statistics such as means, variances, regression coefficients, and correlation coefficients. Consult http://hrsonline.isr.umich.edu/index.php?p=resappguide for detailed HRS disclosure guidelines.

[4] A graduate student working as research assistant for a permanent faculty member on a project using HRS restricted data does not necessarily qualify to have access to HRS restricted data. To be a qualified user, a student must a) be assigned to work on the HRS restricted data as named among the authorized project staff, and b) sign the "Agreement for Use of Restricted Data" from the HRS.

The Data Enclave is less restrictive than the licensing method with respect to who may use the data. The Data Enclave is open to faculty members, graduate students, and undergraduate students from accredited academic institutions. There is no need for a current grant from a federal funding agency. Various costs are incurred in using the Data Enclave. Examples include user fees for the maintenance of the facility, user service in data installation and preparation, and other computing-related assistance during the researcher's tenure at the facility. User fees are $200 per day for faculty members and government researchers; $50 per day for students; and $500 per day for other researchers, such as those employed by private companies. Add to these the cost of travel and accommodations during the researcher's stay in Ann Arbor.

Use of the Data Enclave requires submission of various items as part of the application. A complete listing of these items is available at the HRS website. The more significant requirements include a research proposal, which closely resembles that for a license; a listing of datasets to use, whether supplied by the researcher or by the Data Enclave; a listing of statistical software to use; and a description of expected analysis results. In addition, two application-related forms must be signed: the Confidentiality Agreement Restricting Disclosure and Use of Data from the MICDA Data Enclave, and the Pledge to Safeguard Respondent Privacy.

Data Enclave staff regulate the items users can bring into and take out of the facility. The facility prohibits users from taking outside the facility any analysis output that has not been subjected to disclosure review and approved by Data Enclave staff. The same restrictions apply to handwritten notes.

Remote Access

Data Enclave services extend to remote job processing but only under special circumstances. Use of remote access applies when a researcher who recently visited the Data Enclave needs additional work for the same project. In such a case, the researcher may send by e-mail, for example, a SAS program written in ASCII format to the Data Enclave staff. The Data Enclave then runs the job, reviews the output for disclosure limitations, and sends the cleared output back to the researcher. The time required for additional processing should not exceed one full workday; otherwise, the researcher must make arrangements to return to the facility.

HRS Response to the Challenges

The introduction to this note cites two competing challenges facing statistical organizations handling sensitive data: protecting confidentiality while promoting data use. The HRS responds to these challenges by using two methods to enable access to restricted data, and by imposing rigid requirements on researchers. These responses still have limitations. Although in some ways the access procedures adopted by the HRS serve the research community as well as or better than the procedures adopted by other statistical organizations, the HRS still continues to search for better access methods.

The HRS licensing method restricts qualified users to tenured faculty with current federal grants. The grant element is a centerpiece to this requirement because it serves as a potent sanction against willful violation of the use agreement. However, since many faculty members do not have federal grants, the pool of qualified users is quite limited. Furthermore, even with all the safety precautions laid out in the use agreement—including the threat of unannounced spot checks by HRS staff—confidentiality violations are more likely with licensing than with the Data Enclave because the researchers involved are essentially left to monitor themselves. The lack of tight screening of processed data by HRS personnel enables possible confidentiality violations. Indeed, violations have occurred, although these mostly have been violations of protocol or procedures specified in the data use agreement. A common violation found

in unannounced inspections of HRS licensee sites has been the failure to update the roster of authorized users in a timely fashion. A typical case was the replacement of an authorized graduate student who had recently graduated. None of the violations have resulted in a breach of confidentiality. Similar minor violations were discussed at a 2003 workshop on data access and confidentiality protection (National Research Council 2005). As an access method, therefore, licensing alone is not the best response to the two competing challenges.

The HRS complements licensing with the availability of a secure Data Enclave. With its less restrictive requirements, the Data Enclave widens the pool of researchers who can access HRS restricted data. But this method requires the physical presence of researchers in order to use the facility. Costs incurred in using this method may be prohibitively high for some potential users. Although this method serves the confidentiality issue well, associated costs may impede wider data use.

The HRS also responds to the two competing challenges through the specific requirements of its two methods of granting access. For instance, two of the licensing requirements address many of the HRS' data security concerns. The first of these is the data protection plan. Such a plan must be sufficiently extensive and rigorous to cover a variety of safeguards, from establishment of a secure physical space to house the restricted files, to isolation of electronic files, to the final destruction of all HRS restricted files including datasets derived from them. Further, this plan must be approved by a working committee on data confidentiality. The committee's careful evaluation increases the chances of identifying potential improper disclosures even before access to the restricted data is granted. The second is the requirement to limit offsite use of restricted data to tenured faculty in an accredited academic institution with a current federal grant. These researchers have their tenured position, reputation, and current and future federal grants at stake. They are therefore likely to be more careful to avoid willful violation of the contractual use agreement.

The other response to security concerns involves disclosure. The HRS specifically prohibits combining SSA restricted data with geographic area variables smaller than the census division. As pointed out earlier, the possibility of reidentification increases as the geographic classification used in a cross-tabulation gets smaller. When narrower geographic variables are critically necessary for the research, permission must first be obtained from SSA and use of the data is restricted to the secure Data Enclave.

Comparison Between Agencies

There are many similarities in the statistical organizations' requirements for the use of their restricted data. The HRS, NCHS, NCES, and Census Bureau all require a research proposal, a signed certificate of confidentiality, and strict adherence to disclosure avoidance guidelines. However, subtle differences in emphasis may result in varying levels of access to restricted data. The Census Bureau, for instance, is more likely to reject a research proposal whose primary analytical output comprises tabular data such as frequency counts and percentage distributions. The bureau strongly prefers analyses that focus mainly on results from statistical modeling such as regression coefficients and standard errors. Additionally, an applicant for the use of the Census Bureau's research data centers must demonstrate that the proposed research benefits Census Bureau programs. Examples of such benefits include enhancing data quality, improving data collection methodologies, and developing new and improved measures and estimates. Similarly, NCHS requires a research data center applicant to describe the public health benefits of the proposed research project. Such requirements have been noted to contribute to delays in the application approval process (National Research Council 2005). The HRS avoids such delays because it does not require research using restricted data to benefit the HRS itself.

Use of restricted data also may vary because of the method of access adopted by the sponsoring organization. NCHS and the Census Bureau do not use licensing, whereas the HRS and NCES do.[5] The HRS and NCES licensing procedures differ in subtle but potentially important ways. The HRS, for example, issues licenses only to researchers with a federal grant. NCES does not impose this restriction and thus may provide access to a broader group of researchers. On the other hand, NCES requires a formal commitment from the principal researcher's organization that binds the organization to the provisions of the license.[6] The HRS requires the researcher to be affiliated with an institution that has an Assurance of Compliance from the Office for Human Research Protections of the Department of Health and Human Services. By requiring the researcher's institution to sign the data use agreement, the HRS also requires the institution to agree to treat any violation of the data use agreement as a violation of the institution's policies on scientific integrity and misconduct.

One attractive feature of both HRS and NCES licenses is the provision of offsite data access, which allows researchers to use restricted data at their own institutional facility. Although the pool of qualified researchers and institutions may be small, this is still an advantage the HRS and NCES have over other organizations that do not offer licensing.

Although the Census Bureau and NCHS do not use the licensing method, they make extensive use of the research data center method. The Census Bureau operates nine research data centers across the country. NCHS has its own research data center, which researchers may use onsite or through remote access. In addition, by way of an agreement with the Census Bureau, NCHS extends access to its research data center resources through the nine Census Bureau research data centers.[7]

Finally, the Census Bureau has begun to develop synthetic data files that are derived from restricted-access data using methods that preserve the statistical properties of the restricted data but prevent disclosure of confidential information. With funding from SSA and in partnership with the Internal Revenue Service (IRS), the bureau created a file based on the 1990–1993 and 1996 panels of the Survey of Income and Program Participation (SIPP) matched with SSA benefit records and IRS earnings records. SSA currently is evaluating the analytical validity of this so-called SIPP Synthetic Beta file. Interested researchers may test it by applying for remote access through the Census Bureau's virtual research data center.[8] It remains to be seen whether data synthesizing techniques will be adopted by other organizations as a way to provide information from restricted data sources to the research community.

Potential Future Access Methods

The two methods regulating the use of HRS restricted data clearly cannot serve all potential users. Licensing is available only to a qualified few and the Data Enclave is relatively expensive. HRS administrators recognize these limitations and in response are experimenting with more innovative methods to reduce costs, enable a wider audience to qualify for access, and maintain the confidentiality of the data.

---

[5] Other organizations and research projects that use licensing include the Bureau of Labor Statistics, the National Science Foundation's Division of Science Resources Statistics, the University of Michigan's Archive of Criminal Justice Data, the Wisconsin Longitudinal Survey (National Research Council 2005) and the University of North Carolina's Add Health Study (http://www.cpc.unc.edu/projects/addhealth).

[6] Details on the NCES restricted-use data procedures can be found at http://nces.ed.gov/statprog/rudman/.

[7] Details on the Census Bureau research data centers can be found at http://www.ces.census.gov/. Details on the NCHS research data center can be found at http://www.cdc.gov/nchs/r&d/rdc.htm.

[8] Details on accessing the SIPP Synthetic Beta file are available at http://www.census.gov/sipp/synth_data.html.

One method being developed is the "virtual enclave." This method essentially permits the user to process the restricted data remotely using the MICDA Data Enclave (Nolte and Keller 2004). Confidentiality is maintained by using intruder-safe communication lines between the client and the Data Enclave server. This method therefore can cater to the wider network of potential Data Enclave users at reduced cost because the user avoids the need to be physically present at the University of Michigan. The virtual enclave has been built and tested but not yet implemented.[9] As noted above, NCHS currently supports remote access to its research data center,[10] which could serve as a model for further testing and implementation by the HRS.

The HRS seeks other methods to increase the use of restricted information. One is by extending access to the nine Census Bureau research data centers. Being able to tap into these resources could increase HRS data use by reducing costs to potential users who reside near one of these facilities. HRS administrators are now negotiating with the Census Bureau for the use of their research data centers.

One other innovative method initiated by David Weir, the principal investigator of the HRS, involves the improvement of public-use files by adding information from restricted data that has been transformed into disclosure-proof measures. These measures are developed from statistical models applied to SSA administrative data and are general enough to prevent identification of individual records. The method essentially enables the HRS to release to the public summary measures or predicted values of a certain variable developed from SSA administrative data. The addition of such new information to public-use files enhances their quality, promotes accessibility, maintains confidentiality, and at the same time reduces the need for access to restricted data among researchers. The fewer researchers are using restricted files outside the MICDA Data Enclave, the less the threat to data security. This method is a promising approach toward meeting the two competing challenges that face statistical organizations.[11]

References

Abowd, John M., and Julia I. Lane. 2003. Synthetic data and confidentiality protection. Technical Paper No. TP-2003-10. Suitland, MD: Census Bureau, Longitudinal Employer-Household Dynamics Program.

Abowd, John M., Martha Stinson, and Gary Benedetto. 2006. Final report to the Social Security Administration on the SIPP/SSA/IRS Public Use File Project. Suitland, MD: Census Bureau, Longitudinal Employer-Household Dynamics Program.

[GAO] General Accounting Office. 2001. Record linkage and privacy: Issues in creating new federal research and statistical information. Report No. GAO-01-126SP. Washington, DC: GAO.

National Research Council. 2000. *Improving access to and confidentiality of research data: Report of a workshop,* eds. Christopher Mackie and Norman Bradburn. Committee on National Statistics, Commission on Behavioral and Social Sciences and Education. Washington, DC: National Academies Press.

———. 2005. *Expanding access to research data: Reconciling risks and opportunities.* Panel on Data Access for Research Purposes, Committee on National Statistics, Division of Behavioral and Social Sciences and Education. Washington, DC: National Academies Press.

Nolte, Michael A., and Janet J. Keller. 2004. Research use of restricted data: The HRS experience. Paper presented at the 2004 Joint Statistics Meeting, Toronto, Canada.

Singer, Eleanor. 2005. Access to research data: Reconciling risks and benefits. *Journal of Law and Policy* XIV(1): 85–114.

Singh, A. C., F. Yu, and G. H. Dunteman. 2003. MASSC: A new data mask for limiting statistical information loss and disclosure. Paper presented at the Joint ECE/EUROSTAT Work Session on Data Confidentiality, Luxembourg.

[9] Per personal communication with HRS Senior Researcher Michael Nolte, who leads the development of this method.

[10] Details on the NCHS remote access process are available at http://www.cdc.gov/nchs/r&d/rdcremote.htm.

[11] Per personal communication with David Weir and HRS staff member Cathy Liebowitz.