Contractual Limitations on Data Sharing
Report prepared for ICPSR
Alex Kanous
Elaine Brock
March 31, 2015

Purpose

This report was commissioned by the Inter-university Consortium for Political and Social Research at the University of Michigan Inter-University Consortium for Political and Social Research to engage in an in-depth review of exemplar data sharing, data license, non-disclosure, and other forms of agreements under which data are made available for research use. It is part of a project on "Building Community Engagement for Open Access to Data" sponsored by the Alfred P. Sloan Foundation.[1] The intent of the review was to identify common limitations imposed on the use and re-disclosure of data, variations on those common limitations, and the implications of such limitations on the researcher. Finally, cognizant of the varying reasons for imposing these conditions of use, such as proprietary or privacy concerns, the review sought to identify approaches to conditional data use that represent the data discloser's compelling concerns and the data user's need for latitude in use, in a standardized way in order to facilitate data transfer and reduce the administrative burden of tracking a multitude of varying data use limitations.

Summary

This initial review re-affirmed the general beliefs that prompted the inquiry. First, that agreements under which data and information are disclosed for use in research over-reach by imposing restrictions on a researcher's ability to disclose results of the research or are not clear about the allowable uses of the data thereby engender a perception of restriction. Second, that implicit or explicit restriction in agreements result from data providers' characterization of released data as confidential, which is better applied to proprietary information or other data not released for research use. Treatment of data as confidential may mean that the agreement includes other related provision, e.g., a failure to clearly articulate the allowable uses of the data; treatment of the provided data as intellectual property, or an attempt to define research results as derivatives of the provided data and thus controlled by the provider, and similar issues. Most of these problems do not seem to originate from a data provider's willful intent to restrict academic freedom or deliberately create ambiguity as much as they arise from a poor understanding of the nature of the data warranting protection and poor contract drafting. These

[1] "Building Community Engagement for Open Access to Data," George Alter (Principal Investigator), Alfred P. Sloan Foundation Grant Number 2012-6-11.

can be remedied by a clear definition of data being provided, a better understanding of how the data will be used, why data may need to be protected, and the establishment of appropriate standards described in the agreements for releasing and using the data.

Methodology

The conclusions in this report were drawn upon review of a collection of 36 exemplar agreements. Some of the agreements were provided by ICPSR others were collected by the authors. The reviewed agreements are listed in Appendix A. This review focused on reviewing data use limitations imposed by non-government entities, but agreements from a few governmental agencies, both state and federal, were included. While it is private data providers that tend to have the most onerous restrictions on data use, the existence and nature of data use limitations imposed by governmental data providers can also prove instructive, especially when considered in the light of the growing interest in dissemination of results and data resulting from public funding.

The reviewed agreements were described or labeled by the data providers in a myriad number of ways, including non-disclosure/confidentiality agreements, letter agreements, restricted-use data agreements, data use agreements, license agreements, and memorandums of understanding. Regardless of the title however, all were aimed at achieving the same effect – the provision of data to a recipient for research use, subject to conditions on the use of those data. The title of the various agreements did however occasionally presage the tone or direction the terms of use for the data.

In an attempt to identify commonalities amongst the various types of agreements, a matrix was created that sought to capture the existence, or lack thereof, of elements in each reviewed agreement, including the agreement type, the aim of the agreement, and whether it contained an explicit description of the data provided or the use of the data permitted, specific language regarding data destruction or return, restrictions on the results of the use of the data or any arising publications, characterizations of the data as confidential information or intellectual property, and data protection language. It is the review of these elements that constitute the majority of this report and the following findings are roughly organized into sections according to these elements.

Findings

1. Restrictions on re-distribution of data

Every agreement reviewed contained language in some form that restricted the ability of a data recipient to re-distribute the data they were provided. These generally ranged from simple but comprehensive prohibitions on any distribution to any party except those identified in the agreement to allowances for re-distribution provided the subsequent recipient entered into an agreement with language at least as restrictive as the agreement to which the original recipient was subject.

While the severity of these prohibitions may not always align with the actual risk posed by re-disclosure for all data, these limitations are generally understandable. Ownership of intangible objects such as data is only maintained via the exertion of control over the data, and thus articulating explicitly those individuals or entities that are allowed access to the data is logical. However, many agreements include blanket bans that do not distinguish data that may have been de-identified or for which the sensitivity concerns prompting the prohibition on re-distribution have been sufficiently mitigated from data that requires sensitive treatment. The unnecessarily broad bans potentially run afoul of the increasing obligations of researchers to redistribute research data to which researchers are subject by public and some private sponsors and also by journal publishers. Additionally, as discussed further in this report, a lack of nuance in drafting the sensitivity obligations of agreements can cause researchers other problems.

2. Descriptions of covered data

Noticeably absent from many of the agreements reviewed was a clear description of the data being provided. Some agreements rely on such vague language as "all information regarding the company" or "information provided to Recipient." The importance of clear identification of the covered data is obvious – if the data recipient's institution is unsure which data are subject to the terms of the agreement, how can it protect the data as required by the data provider in the agreement? The best handling of this issue occurs in those agreements that identify specific data sets within the agreement or include appendices where requested data sets can be selected by the requestor. Common amongst those contracts characterized as non-disclosure or confidentiality agreements are descriptions of the restricted information as that information which has been marked or otherwise identified as confidential. While this latter treatment is functional, it raises a significant administrative burden on the provider that is not borne when the covered data sets are clearly stated in advance.

Even in those situations where the agreement contains an explicit description of the covered data additional expansive language was occasionally found. This additional language is likely intended to provide a safety net to prevent the inadvertent exemption of those data that don't fit within the explicit description. For instance, while one agreement limited the covered information to

those data that the requestor could "describe with as much specificity as possible, so the data can be identified easily by others," in conflict with that purpose it also noted that the definition of governed data "also includes any other [Provider] data that the user access, obtains, and/or uses which might not be listed . . ." (*See Agreement 15*). This expanded language makes it impossible for the data recipient to determine which data are subject to the terms of the agreement with any amount of reliability. This sort of expansive language is something that will be seen within other findings herein.

3. Articulation of allowed scope of use of data

The review also disclosed that the analyzed data agreements often failed to clearly specify the allowed uses of the data by the recipient. Some agreements did not address the recipient's data use at all. While some included the specific name of the research project or activity for which the data were to be used, or contained data applications in which a requestor described the activities in which they intended to use the data, others contained more generic limitations such as "solely for the purpose of scientific and public policy research" (*See Agreement 8*) or "solely for scientific and public policy statistical research as described in the Research Plan submitted to and approved by [provider]" (*See Agreement 24*)."

Although it may very well be in the best interest of a researcher to receive data free, or substantially free, of any limitations on the uses to which these data can be put, the general desire of the provider to extend control of the data in the hands of the recipient, it was unexpected to not consistently encounter explicit statements of allowable use. Additionally, as noted throughout this report, fostering a sense of surety amongst data recipients as to exactly what they are allowed to do with the data, and how they must maintain it, will create more responsible data recipients and facilitate university administration of the agreements including the necessity for related compliance approvals and monitoring. Thus, a clear articulation of allowable uses of shared data, even if those uses are broad and unrestricted, is important.

4. Treatment of data as "confidential information"

Common to many of the reviewed agreements was the inclusion of language speaking to the treatment of confidential information by the data recipient. In the context of an activity more complex than the simple transfer of data, e.g., where research data are being transferred alongside information deemed proprietary to the provider such as unique business methods or processes by which the data were collected, inclusion of confidentiality language is reasonable. When the provided data are characterized as confidential, such as language stating that "[a]ll information delivered or provided to Recipient shall be presumed to be Confidential

Information," (*See Agreement 10*) the overbroad definition presents a potential problem. Information/data designated as confidential is typically completely barred from re-distribution by the recipient. This would conflict with obligations on the data recipient to disclose or publicly disseminate the data collected for their research as provided by their research sponsor. This confidential designation of data prohibits publications that disclose the confidential information. The publications would have to be first vetted and approved by the information/data provider and may mean that publications cannot meaningfully describe the results of the recipient's use of the information/data thus frustrating the academic mission of most research institutions.

It should be noted that simply calling the provided data "confidential information," as opposed to more typical terms of characterization such as "sensitive" or "restricted-use" doesn't itself give rise to any particular issues, unless the agreement under which the data are provided is structured as a non-disclosure agreement. Such agreements typically, but not always, anticipate an exchange of information intended to be viewed or used for a limited and specific purpose, such as determining the feasibility of a proposed business relationship for example, and then either destroyed or returned to the data provider. This kind of structure is wholly inappropriate for governing the sharing of sensitive data for research purposes as these non-disclosure agreements generally contemplate such preliminary evaluative activities that they do not, and cannot, cover research endeavors (*See Agreements 32, 33, and 34*). To the extent that these agreements are intended to speak to data transfers for research activities, this is simply a failure of the parties to understand the recipient's intentions and to put in place the appropriate type of agreement.

Similar to the above-advised caution on interpreting intent when data are defined as confidential, the fact that the agreement under which data are released may be entitled a non-disclosure or confidentiality agreement should not be used to presume the intent of such agreement. The more specific a non-disclosure agreement becomes about the exact information governed and the scope for which the data may be used, the more analogous to a data sharing agreement it becomes. Treatment of data as confidential information particularly begins to complicate matters when it is tacked on as a means of capturing information beyond the defined data being released. Functionally, this extension casts a wide net of application and acts as a failsafe for the provider against the inadvertent release by the recipient of information beyond the specified data. This is similar to the effect of the failure to include an explicitly articulated description of the governed data, as noted earlier. However, the expansive use of the confidential information characterization can have other problematic implications, including the attempt to reach through to the work product of the data recipient. As one reviewed agreement noted, the confidential information at issue included not just the materials provided to the recipient, but also any

information that was "developed jointly and/or separately by [Provider] or Recipient, as part of any assignment under this Agreement" (*See Agreement 36*).

The treatment of research data as confidential information raises an additional set of potential issues that should be of as great a concern to the data provider as the recipient, if not more so. As confidentiality agreements oftentimes reference the governed information generally, or rely upon the recipient to reasonably know which information are to be held confidential, the data provider runs the risk of creating uncertainty as to which data the restrictions apply. As suggested earlier, how can a data recipient accurately protect the received data if they are unaware to which data the restrictions apply? Additionally, non-disclosure agreements often contain a list of conditions under which the confidentiality obligations would no longer be deemed to apply, typically including situations where the information was previously known to the recipient, becomes part of the public domain without the recipient's breach of the agreement, was received from a third party, or is compelled to be released by law or court order. When compared to an ideal data sharing agreement, with its exertion of control over the data achieved through the explicit articulation of the governed data and the allowable uses, these available exceptions within non-disclosure agreements constitute a potential weakening of the provider's' control of the data, as they provide conditions under which confidentiality need not be maintained.

5. Treatment of data as intellectual property

References to the data provider's various intellectual property rights in the data being transferred were found in several of the reviewed agreements. Some of this language sought affirmation from the recipient that the provider owned "all copyrights, trademarks, patents, trade secrets and other proprietary rights in and to the Licensed Data," (*See Agreement 13*). Other terms required acknowledgement from the recipient "that the [data] furnished hereunder are subject to U.S. Copyright Law" (*See Agreement 21*). However, as discussed below, affirmations such as the former are problematic due to the confusion they can engender and assertions like the latter are likely simply inaccurate statements of law.

Generally, data does not benefit from the protections of a copyright as that particular form of intellectual property is intended to protect original, creative expressions, and does not extend to statements of fact. Data is generally seen as a reflection of fact. The seminal case on this matter, *Feist Publications, Inc. v. Rural Telephone Service Company, Inc.*, affirmed this notion in an analysis of copyright's protection of databases. The Supreme Court ruled that there can be no copyright in the data contained within a database, but copyright protection could be afforded to the database, or other compilations of facts or data, if the compilation exhibited sufficient

creativity, such as in the unique selection of included data elements or the way in which the data were arranged within the compilation. The other members of the typical trio of intellectual property rights under United States statutes, patents and trademarks also are not appropriate to protections of data. Patents apply to inventions and trademarks serve to minimize consumer confusion by distinguishing goods.

Despite the inapplicability of intellectual property rights to data, as noted previously, such terms are nevertheless included in many data transfer agreements. This is another example of a data provider attempting to assert as much control as possible over their data by calling upon myriad legal protections, without adequate assessment of their appropriateness. But this approach creates uncertainty and risks chilling research and publication of research results. Unsure of the extent to which they can use the data, and concerned that their creative output may be co-opted via an intellectual property rights system they don't understand, researchers may self-impose an overly conservative approach to both use and disclosure of use of the data.

None of the above however should be interpreted as implying that the data provider is not encouraged to place applicable and appropriate conditions on the use of their data. The mere fact that data are not protected under copyright does not mean they are forced into the public domain. *ProCD, Incorporated v. Matthew Zeidenberg and Silken Mountain Web Services, Inc.*, a 1996 ruling by the 7th Circuit Court of Appeals, reviewed the validity and enforceability of a "shrink wrap" license on a database deemed not protectable through copyright per *Feist* and ruled that copyright law did not preempt use of contract law to impose conditions on use of the database. A data provider was still free to control access and use of their data, regardless of whether it constituted a creative expression sufficient to trigger copyright protection. Which, when viewed in this context, reinforces the need for data sharing agreements and the irrelevance of copyright language.

The foregoing should also not be interpreted as a statement that intellectual property rights do not belong within a data sharing agreement in any context. For instance, one agreement forbade a data recipient from establishing intellectual property rights in research results that would "prevent or block access to, or use or, any element of the Data, or conclusion drawn directly from the Data" (*see Agreement 30*). Such language doesn't seek to extend additional restrictions on the use of provided data through a faulty passive reference to the intellectual property protections of such data, but instead aims to reinforce the provider's control of the data by preventing the recipient from leveraging intellectual property rights of their own that interfere with or limit the future use of the data. Note, however, that in this case the provider also restricts the potential intellectual property designation of the recipients "conclusions drawn directly from the Data."

6. Rights to derivative works

A researcher's use of data is bound to result in the creation of analyses, publications, and other academic work product based on those data. In the interest of maintaining the researcher's academic freedom, rights to these research results and work product need to remain with the researcher and their institution. Unfortunately, data transfer agreements frequently attempt to circumvent this by reaching through to resultant analyses, publications, and academic work product as "derivatives" of the original data.

What makes this reach-through approach particularly problematic is that the agreement typically fails to define what constitutes a derivative, and we are thus forced to interpret intention and effect of the language. Where the concept of derivative works is most well-defined is within copyright law, which includes the right to make derivative works within the exclusive rights of the copyright holder and defines derivative work as a new work that adapts, or is derived from, an existing copyrighted work. The copyright that the recipient would obtain in such derivative works that they develop applies only to the additions, changes, or new materials that constitute the derivative work but does not extend to the original copyrighted work. Despite the fact that data, as discussed previously, is generally not protected under copyright, data providers would choose to leverage this concept in the belief that it provides yet another means by which they can extend their control beyond the specifically articulated limitations of the data they are providing under the agreement.

As these agreements often memorialize the transfer of sensitive data, it is reasonable that a provider would require extension of the data use conditions to resultant data that consisted of, or substantially included, the provided data. But interpretations of the derivative work characterizations suggest that they are often not this narrowly tailored. As one agreement stated, "User shall not copy, reproduce, distribute, display, or create derivative works from any portion of the [data]; provided that the User shall be entitled to present its scholarly research findings relating to the [data] (and not the [data] itself) as part of classroom instruction at a bona fide instructional institution" (*See Agreement 15*). An inverse reading can only result in the interpretation that "scholarly research findings related to the data" are considered derivative works here. Other agreements were more blatant, stating, for example, that "Restricted Data refers to . . . any fields or variables derived from these data . . ." (*See Agreement 8*).

The issues that arise from the extension of most of the data use conditions found within a data transfer agreement to derivative works that constitute the research results of an investigator are obvious. Absent approval from the data provider, results could not be shared with peers or

research funders, publications derived from the use of the data could not be submitted, and results could not be retained or further used by the researcher after termination of the agreement. This unquestioningly violates many central policies of most research institutions and should be reserved for only those situations in which the most sensitive data are being shared, and then only to the extent that results from use of the sensitive data consist of or contain those sensitive data.

7. Publication restrictions

Similar to the concerns over the inclusion of terms designating research results as derivative works are those related to contractual language regarding inappropriate review of publications or presentations resulting from the use of the data. While some review and comment language is relatively benign other more directive or restrictive language could constitute a full prior restraint on a researcher's ability to publish the results of their research.

Before looking at the variety of publication and presentation review language that commonly appears in data transfer agreements, it is important to first note that the intent of the review, or what the data provider is requesting to review, can often be informative as to the likelihood of that review being problematic. A request that the researcher share with the data provider the results arising from analysis of the data oftentimes stems less from the provider's desire to shape the message resulting from the research than an intent to review the results for quality issues tied to the portrayal of provided data or the resulting research. It is the publication or presentation, however, that contains the researcher's interpretation of the data, and thus review could be prompted by a provider's desire to foreclose interpretations that do not square with their message or image or that paint their company's interests in a negative light.

Not all publication or presentation review is problematic, or arises from an editorial intent as suggested above, with these provisions effectively existing across a spectrum of increasing control, as laid out below. The further one goes down this spectrum, the potential restriction on academic freedom increases, as does the need for a researcher and their institution to consider their ability and willingness to accept these terms.

- Required citation to the source of data used in the research
- Required time-limited review to allow provider to suggest comments that the researcher may, but is not required to, include in the reviewed publication or presentation
- Required review to allow provider to determine whether an intended publication will disclose provider's intellectual property, or potential intellectual property, with sufficient time delay to allow provider to seek intellectual property protection (assuming

intellectual property is appropriately defined and does not reach through to research results)

- Required time-limited review to allow provider to suggest comments that the research must include, and refusal to include the comments requires the insertion of a disclaimer stating that provider does not endorse the research or results
- Required unlimited review period for any purpose since it gives *de facto* control to the provider
- Required review to allow provider to determine whether an intended publication will disclose provider's intellectual property or confidential information and a requirement that such intellectual property or confidential information is removed from the publication (assuming either confidential information or intellectual property is defined to at least arguably include research results.)
- Required delay in publication at the discretion of the provider
- Required review to allow provider to determine whether they will allow publication to occur.

8. Effect of termination

Generally all contracts eventually terminate, typically either when a pre-determined end data has been reached or the activity described in the agreement has been completed. In the case of data transfer agreements, a common variation is a term that runs for as long as the recipient is in possession of the data. Any of these approaches is acceptable, as long as it is clear at what point the data recipient's obligations and rights with respect to use of the data have ended. Several agreements extend the obligations but not necessarily the use rights under the agreement indefinitely or for a period of time beyond termination of the related research activity. No doubt this is yet another example of expansive language being included in an attempt to patch potential gaps in the agreement, but as with other such instances discussed above it engenders uncertainty. And given the administrative resources often necessary to ensure compliance with a data transfer agreement, this uncertainty can have a significant financial impact due to costs of administration and monitoring.

Upon termination, most of the reviewed agreements required the provided data to either be destroyed or returned to the provider, typically at the provider's option and instruction. This is reasonable given the provider's need to maintain control of their data. However, which data needed to be destroyed or returned at termination was occasionally unclear in these agreements, with some characterizing the subject data to potentially include the researcher's work product derived from use of the data. For instance, one agreement required, upon conclusion of the agreement, that the "Receiving party shall immediately return and redeliver to

the other all tangible material . . . and all notes, summaries, memoranda, drawings, manuals, excerpts or derivative information deriving there from and all other documents or materials . . . based on or including any Confidential Information" (*See Agreement 32*). While not explicitly defined, "Based on" would no doubt include any research work and analyses of the data, regardless of whether it included the data designated as confidential information or not. The far better situation agreement is one in which the researcher's work product is specifically excluded from the data to be destroyed, such as the reviewed agreement that required the recipient to "destroy all copies of the Licensed Data in their possession or control except to the extent components of the Licensed Data have been incorporated into reports and analyses permitted" under the agreement (*See Agreement 12*).

Recommendations

The following suggestions are based upon the contract review discussed previously and the foregoing findings and are aimed at providing clarity to data recipients, minimizing their confusion about the conditions that apply to the receipt and use of the data, while preserving the understandable interests of the data provider in ensuring their released data are received, managed, and disclosed appropriately.

1. Appropriate agreement title

While it is the content of the agreement under which data are disclosed that are of greatest relevance when determining the conditions for use of received data, the manner in which the agreement is presented, especially the title of the contract, can be the first source of confusion. Non-disclosure or confidentiality agreements, by their very name, create the perception of a different intent than data sharing or data use agreements. Avoiding the use of such misleading names is a simple fix that can net exponential clarity of the parties intent. For this reason, it is recommended that an agreement under which data are to be transferred for research use are titled such that this intent is obvious, specifically suggesting "Data Use Agreement," "Data Sharing Agreement," or "Data Transfer Agreement."

2. Description of data

Most agreements did not include an explicit description of the data being shared or which data is subject to a confidentiality obligation. This is no doubt done in part to prevent the provider/discloser from inadvertently excluding some of their provided data from the the contractual obligations due to their failure to include it within the definition or description of

data being provided. This however, ironically, may serve to place their data within greater danger as a data recipient cannot fully protect information they cannot identify as subject to the obligations. Given this, it is recommended that a data transfer agreement include within its terms a clear identification of the data governed by the agreement. This could take various appropriate forms including a description of the data within the agreement itself, a list of data elements appended to the agreement in the case of larger or more complex data sets, or even a website url where only specific data can be accessed per instructions of the provider.

3. Articulated scope of use

Similar to the previous recommendation, the failure of an agreement to include a clear and comprehensive description of the activities for which the data recipient may use the data creates ambiguity that may alternately result in a researcher unnecessarily limiting the scope of their research out of fear of overstepping their bounds. Alternatively an unclear description of permitted uses places the data at risk by not conveying to the recipient the parameters and what uses are outside permitted boundaries. As such, it is recommended that any data transfer agreement include specific terms regarding the allowable uses of the data. Permitted use may be presented relatively broadly, allowing all uses in support of, and compliant with, a particular named research project. Or this could be much more narrowly tailored based on particular characteristics of the data, giving explicit activities that are permitted, such as data analysis via a particular device or process and the return of analyses or not permitted, such as use with other datasets that could lead to identification of individuals.

4. Rights to research products resulting from data use

Whether defined as derivative works or not, ownership and control of the results of an investigator's use of the provided data generally need to be retained by the researcher and their institution. The typical situations where it could be acceptable to soften this stance is when the researcher is receiving data not to conduct their own research, but to perform a service of some sort on behalf of the provider, or when the data provider requires specific rights to the results but does not prohibit the recipient researcher from continued use of their results. It is recommended that as a general rule a data transfer agreement not include language providing a data provider's exclusive rights to, or ownership of, any of the work product or results a researcher develops via use of the provider's data.

5. Publication and presentation rights

It is reasonable to accept certain publication conditions that recognize the proprietary interest of the provider or significant sensitivity of the data being provided. Conditions that arise to the level of editorial control or potential prior restraint, however, should are generally unacceptable. It is recommended that data transfer agreements include language about publications resulting from use of the data that do not go beyond requirements to cite the source of the data, grant the data provider a time limited period in which to review and suggest comments, and/or require that intellectual property and confidential information (appropriately defined to exclude research results) be removed.

6. Effect of termination

Just as imperative as understanding which data are subject to the conditions of the agreement and for what purposes the data may be used, is a clear understanding of when those conditions and rights end. It is thus recommended that the term of a data sharing agreement either run to a specific future date, with the option of requesting extensions, or until the recipient is no longer in need and possession of the data. Tying it to the duration of a project, which might not be explicitly defined, or requiring that certain terms run beyond termination of the agreement serve only to create confusion as to what continued rights to use the data the recipient has, and what obligations they must continue to bear.

Upon termination it is critical that a researcher does not find their research results subject to the requirements of destruction or return to which the original data are. To avoid this, it is recommended that data transfer agreements require only the destruction or return of the provided data to the extent such data have not been incorporated into a report or analysis and that such destruction and return obligations do not apply to research results that do not contain, or consist of, the provided data.

Appendix A

Reviewed Agreements

1. Economic Research Institute Data Sub-License Agreement
2. Educational Research Foundation Memorandum of Understanding
3. Federal Agency Confidential Access to Sensitive by Unclassified Information Non-Disclosure Agreement
4. Financial Group Letter Agreement
5. For-profit Company Confidentiality Agreement
6. For-profit Consulting Company Non-Disclosure Agreement
7. For-profit Research Company Agreement for Use of Restricted Survey Data
8. For-profit Research Company Confidentiality Agreement
9. For-profit Research Company Data Use License Agreement
10. For-Profit Subsidiary Company Confidentiality and Non-Disclosure Agreement
11. Health Association Data License Agreement
12. Health Professional Association License Agreement
13. Health Professional Society Data Sharing License Agreement
14. Health Research Institute Confidential Data Disclosure Agreement
15. Insurance Company Data Use Agreement
16. Law Firm Confidentiality Agreement
17. National Lab Non-Disclosure Agreement for Evaluation of Proprietary Data
18. Non-profit Finance Corporation Non-Disclosure Agreement
19. Non-profit Medical Organization Date Use Certificate
20. Non-profit Organization Agreement for Educational Organizations
21. Non-profit Organization Data Sharing Agreement
22. Non-profit Organization Letter Agreement
23. Non-profit Organization Memorandum of Understanding
24. Non-profit Research Company Letter Agreement
25. Private For-profit Company Data Services Master Agreement
26. Private For-profit Company Data Transfer Agreement
27. Public For-profit Company Academic Research License Agreement
28. Research Consortium Data Access Agreement
29. Small For-profit Company Data License Agreement
30. Social Science Research Organization Restricted-Use Data Agreement
31. State Department of Community Health Data Use and Non-Disclosure Agreement
32. State Department of Community Health Non-Disclosure Agreement
33. State University Research Foundation of New York Confidentiality Agreement

34. Unnamed Non-Disclosure Agreement
35. Unnamed Non-Disclosure Agreement
36. Unnamed Non-Disclosure Agreement