Appendix B

Data Use Agreements and Memorandums of Understanding: Sample Text and Documents

Agreements and memorandums of understanding are types of contracts and as such are legal documents. Contracts describe a business relationship between two parties and usually begin by identifying the parties involved. The contract then describes the parties' mutual understanding of what each is agreeing to "give to" and "receive from" the other party. A contract is not valid if each party does not "give" something of value and "receive" something of value. It is not valid if there is not a "mutual understanding" about what is given and received.

All important terms should be included in writing in the contract. For example, a contract may specify that one party may give data and one party may pay for that data. If the data owner also expects that the data will be kept confidential and private or that s/he will have a role in determining how the data may be used, then these terms should be included in writing in the contract. From a legal perspective, all rights and obligations of the parties should be defined in the written contract. The term "agreement" will be used throughout this document. "Contract" and "agreement" are interchangeable terms. "Memorandum of understanding" is usually reserved for parties that already have other, more complex relationships. For instance, the Centers for Disease Prevention and Control may enter into a memorandum of understanding with the National Institutes of Health; both are agencies within the Department of Health and Human Services.

TABLE OF CONTENTS

1. IDENTIFICATION OF PARTIES TO THE AGREEMENT

The parties identified in the agreement should have authority to legally bind their organizations to all of the terms of the contract. The parties may be corporations, government agencies or individuals. It is important that the part of the organization that you will be working with is identified in the agreement and that the person signing the agreement has authority to legally bind the organization (i.e., a person who is an officer of a corporation or who has an executive position within the organization).

Example 1:
This data use agreement ("Agreement") is effective upon execution, and is entered into by and between the Regents of the University of XYZ ("Recipient") and Company ABC ("Data Provider"). *(The underlined text identifies the parties.)*

Data Provider and Recipient **mutually agree to enter into this Agreement to comply with the requirements of Section 514(e) of the Privacy Rule, 45 Code of Federal Regulations ("C.F.R.") § 164.514(e),** issued pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). *(The bold text shows the purpose of the contract.)*

Example 2:
This memorandum of understanding will refer to a joint project between researchers at X University and at the University of Y. **It will serve to clarify understanding of work roles and credit for all of the individuals involved in the aforementioned project. The joint project will focus on accessing and analyzing the publicly available tobacco industry documents, and the topic of the project will be "abc," with a likely focus on a case study of marketing strategies. *The individuals involved in this project are: Dr. A, Dr. B, Dr. C, and Dr. D.*** *(The underlined text identifies parties; the bold text identifies purpose; the italicized and bold text shows research project participants.)*

2. PURPOSE

- Detailed description in purpose can vary depending on existing agreements or relationship with researcher/quitline.
- This section is usually short and provides a global overview of the purpose of the agreement and may also describe the overall purpose of the project. The purpose section can also include the goals, objectives, project period, and rationale for the research.

Example 1:
This memorandum of understanding will refer to a joint project between researchers at X University and at the University of Y. **It will serve to clarify understanding of work roles and credit for all of the individuals involved in the aforementioned project.** The joint project will focus on accessing and analyzing the publicly available tobacco industry documents, and the topic of the project will be "abc," with a likely focus on a case study of marketing strategies. The individuals involved in this project are: Dr. A, Dr. B, Dr. C, and Dr. D. (*The bold text describes purpose of the agreement (or contract) and underlined text the purpose of the project.*)

3. PROJECT PERIOD

The project period, which is the overall time required to complete the proposed project, should include both the start date and the end date of the project.

Example 1:
This Data Use Agreement is by and between X Company and The University of ABC (Recipient) and is effective this # day of Month, Year through # day of Month, Year.

Example of end dates:
The agreement will end on # day of Month, Year.

4. ROLES AND RESPONSIBILITIES

The roles and responsibilities included in the agreement help to clarify roles in advance of the project starting, which can be useful for maintaining good relationships between the parties. They are helpful for determining the cost of the project. Also, they will become the legally binding "obligations" of one party and "rights" of the other party named in the agreement.

Example 1:
This memorandum of understanding will refer to a joint project between researchers at X University and at the University of Y. It will serve to clarify understanding of work roles and credit for all of the individuals involved in the aforementioned project. The joint project will focus on accessing and analyzing the publicly available tobacco industry documents, and the topic of the project will be "abc," with a likely focus on a case study of marketing strategies. The individuals involved in this project are: From X University, Dr. A and Dr. B; and from University of Y, Dr. C and Dr. D.

- Deliverables/for each party involved

- The roles and responsibilities in the agreement should only pertain to the parties who are part of the agreement.

Example 1:
Dr. A will devote at least 4-8 hours per week to this project between approximately Month Year and Month Year. Drs. A and C will communicate by email or phone at least twice per month (ideally weekly) to ensure timely progress, and to direct further data collection.

Dr. A will come to the Tobacco Center for Research and Education for at least a one week period for training in tobacco documents research and analysis methodology. This training will include but is not limited to: training on the Legacy Tobacco Documents Library, search terms and strategy, proper research documentation, standard tobacco document citations format and EndNote citations. Dr. A will also have opportunities to meet with full-time tobacco documents researchers at the Center. Dr. C will provide funding for Dr. A's travel to San Francisco; University of Y will provide work space and a computer during Dr. A's stay. Dr. C will devote most of her research time to working with Dr. A during this trip, and Drs. C and D will oversee the training.

- Can include a timeline

Example 1:
<u>Preliminary timeline:</u>
Document searches will take place between Month Year 1 and Month Year 2; data analysis, research memoranda writing, and subsequent searches will take place between Month Year 2 and Month Year 2. Manuscript writing will take place between Month Year 2 and Month Year 2. Our goal is to have a manuscript submitted by Month Year 2.

5. PUBLICATION

- Review process prior to publishing
- Discussion and documentation of authorship

Example 1:
<u>Writing and Authorship</u>:
We anticipate that at least one publication will result from this project. In addition, we anticipate that Dr. A will be available, if necessary, to travel to CITY for an intensive writing session with Drs. C and D for at least one week. Although this trip may not be necessary, in the experience of Drs. C and D it often vastly improves the quality of the finished product, as well as the efficiency of manuscript production. University of Y will provide funding for Dr. A's travel for this trip. If one paper is written as a result of the project, Dr. A will do the majority of the writing and be the first author for the paper, and Dr. C will be the last author.

If a second paper is written based on this research, Dr. C will do the majority of the writing of the paper and be the first author of this paper, and Dr. A will be the second author. Drs. B and D, and other research contributors, may appear as authors on either manuscript dependent upon the weight of their respective contributions.

Dr. C will be the senior investigator on the project and will be responsible for the final negotiations and decision making regarding inclusion of Drs. B, D, or any other authors on any publications resulting from this work. Dr. C will solicit input from Dr. A about authorship on publications that result from this project.

Example 2:
Can include additional language to refer to quitline staff if they are interested in being part of the publication process or should wish to review what is being written, such as, "any draft publication will be provided to Ms. C (quitline contract manager) for review prior to submission. Ms. C will be offered the opportunity to serve as an author for any publication."

6. DATA

- Limited data agreement defines only the portion of data that will be shared

Example 1:
[Organization] has agreed to disclose to Recipient a **Limited Data Set** consisting of the following: <u>Pharmacy and Medical Claims from 2008 related to the Medication Therapy Management (MTM) Comprehensive Call Center beneficiaries, in order to measure the impact that those reviews had on 2009 utilization</u>.

- Define the uses and disclosures of data that are permitted.
    - Identify the name of the actual data set or variables to be shared.
    - Identify who will have access (e.g., subcontractors, agents, only necessary personnel).

Example 1:
Recipient is permitted to use and disclose the **Limited Data Set** or **Individual** pieces of data contained therein as follows:

a) Assess the acceptance rate by health care providers of recommendations made by Recipient pharmacist;
b) Assess the impact of MTM services on members' utilization of healthcare services; and
c) Assess the impact of MTM services on per member per month healthcare expenditures.
Notwithstanding the foregoing, Recipient agrees that it shall not use or disclose such **Limited Data Set** or the **Individual** pieces of data therein such a manner that would cause "_____________" to be in violation of any federal or state law or regulation.

Example 2:
Data Collection and Analysis:
Dr. X will do the majority of the data collection and data analysis for the project, and Dr. Y will help with data collection and analysis in a smaller capacity. Drs. A and B may be requested to provide guidance for the research, or to assist with manuscript writing. We will utilize the following tobacco documents databases: Legacy Tobacco Documents Library, Tobacco Documents Online, the Philip Morris tobacco documents website, and other tobacco documents websites run by the tobacco industry.

7. UNAUTHORIZED USE OF DATA

- Address privacy rules and/or laws that govern the research and/or data.
- Identifiable vs. de-identified data

The agreement should define unauthorized use of data if that is important to the parties. Any existing legal restrictions on the data, any agreements made with subjects of the data, and any limits that the data owner wants to place on use of the data by the other party should be incorporated into the agreement. For example, if the law requires privacy or if the subjects have been promised that the data will be kept confidential, these terms should be included in the agreement.

Example 1:
Prohibition on Unauthorized Use or Disclosure.

a) Recipient will neither use nor disclose the "Limited Data Set" for any purpose other than as permitted by Section x of this Agreement, as otherwise permitted in writing by Data Provider, or as Required by Law.

b) Recipient is not authorized to use or disclose the "Limited Data Set" in a manner that would violate the Privacy Rule, 45 C.F.R. Part 164, Subpart E (http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html), if done by Data Provider.

c) Recipient will not attempt to identify the information contained in the Limited Data Set or contact any individual who may be the subject of information contained in the Limited Data Set.

- Sharing with additional parties without written permission

Example 1:
Permitted Recipients, Subcontractors, and Agents. Recipient will require any agent or subcontractor, to which Recipient is permitted by this Agreement or in writing by Data Provider to disclose and let use the Limited Data Set, to agree to comply with the same restrictions and conditions that apply to Recipient's use and disclosure of the Limited Data Set pursuant to this Agreement.

Example 2:
Recipient agrees not to use or further disclose the **Limited Data Set** or **Individual** pieces of data therein other than as permitted by the Data Use Agreement or as otherwise **Required by Law.** Recipient further agrees to use appropriate safeguards to prevent use or **Disclosure** of the information other than as provided for by this Data Use Agreement. Recipient shall promptly report to "____________" any use or **Disclosure** of the information not provided for by this Data Use Agreement of which Recipient becomes aware and shall ensure that any agents, including a subcontractor, to whom Recipient provides the **Limited Data Set** or **Individual** pieces of data therein agrees to the same restrictions and conditions that apply to Recipient with respect to such information. Recipient agrees that under no circumstance shall Recipient take steps to identify the information it receives from "__________________" or contact the **Individuals** about whom the information pertains.

8. BREACH OF PRIVACY, DISCLOSURE

If one party fails in their privacy obligations, disclosure of the breach of privacy to the other party is always required. The parties may also agree on ways to reduce harm due to a breach of privacy. If they have agreed that there will be penalties for breach (i.e., monetary or termination of the agreement), they should be included as a term.

Example 1:
Breach of Privacy Obligations**.** Recipient will report to Data Provider any use or disclosure of the Limited Data Set that is not permitted by this Agreement or in writing by Data Provider. Recipient will make the report to Data Provider's Director of Research Programs within 7 days after Recipient learns of such non-permitted use or disclosure. Recipient's report will at least:

a) Identify what corrective action Recipient took or will take to prevent further non-permitted uses or disclosures;

b) Identify what Recipient did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and

c) Provide such other information, including a written report, as Data Provider may reasonably request.

d) Identify the nature of the non-permitted use or disclosure;

e) Identify the Limited Data Set content used or disclosed;

f) Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;

g) Identify what corrective action Recipient took or will take to prevent further non-permitted uses or disclosures;

h) Identify what Recipient did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and

i) Provide such other information, including a written report, as Data Provider may reasonably request.

Example 2 (more severe, could be a condition or requirement based on funding):
a) ***Notification of Breach.*** During the term of this Agreement.

b) ***Discovery of Breach.*** To notify DHCS **immediately by telephone call plus email or fax** upon the discovery of breach of security of PHI in computerized form if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person; or **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Agreement, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the DHCS contract manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notification shall be provided by calling the DHCS ITSD Help Desk. Business Associate shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and
ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

c) ***Investigation of Breach.*** To immediately investigate such security incident, breach, or unauthorized use or disclosure of PHI or confidential data. Within 72 hours of the discovery, to notify the DHCS contract manager(s), the DHCS Privacy Officer, and the DHCS Information Security Officer of:
i. What data elements were involved and the extent of the data involved in the breach,
ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data,
iii. A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized,
iv. A description of the probable causes of the improper use or disclosure; and
v. Whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breach are triggered.

d) ***Written Report.*** To provide a written report of the investigation to the DHCS contract managers, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

e) ***Notification of Individuals.*** To notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal laws and to pay any costs of such notifications, as well as any costs associated with the breach. The DHCS contract manager, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications.

f) ***DHCS Contact Information.*** To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated herein. DHCS reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or the Agreement to which it is incorporated.

DHCS Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer

9. RETURN OF DATA

- Clear identification of ownership of data
- Process for returning data/limited data sets or destruction

Example 1:
Return of "Limited Data Set"

a) Upon termination or expiration of this Agreement, Recipient will, if feasible:

i) return to Data Provider or destroy the "Limited Data Set", and

ii) obtain from each subcontractor, agent or other recipient, that received the "Limited Data Set" under Section x of this Agreement, the return or destruction of the Limited Data Set.

The return or destruction must include (1) the "Limited Data Set", (2) all copies of the "Limited Data Set", and (3) any work derived from the "Limited Data Set" that may allow identification of any individual whose information is contained in the "Limited Data Set", in the custody or under the control of Recipient or of such subcontractor, agent or other recipient, whether in tangible or electronic medium. Recipient will complete such return or destruction as promptly as possible, but not later than 30 days after the effective date of the termination or expiration of this Agreement, and will within such period certify in writing to Data Provider that such return or destruction has been completed.

b) If return or destruction is not feasible, Recipient will, within 30 days after the effective date of the termination or expiration of this Agreement:

i) provide Data Provider with a written explanation why return or destruction is not feasible, and

ii) certify in writing to Data Provider that Recipient, or subcontractor, agent or other recipient under Section 5 of this Agreement, will neither use nor disclose the Limited Data Set for any purpose other than the purposes that make return or destruction of the Limited Data Set infeasible.

While users of data are responsible for adhering to the terms of the data use agreement, it is advisable for owners of the data to check on data sets currently in use by others, and either extend existing data use agreements or confirm return or destruction of data. The data owner may want to engage in a practice of sending a letter to verify the return or destruction of data.

10. SAFEGUARDS, COMPUTER SECURITY (password protection, hard-drive locks, etc.)

In order to protect the data and personal health information the data may contain, additional security measures should be in place. These safeguards can be written into the data use agreement or contract. Computer security passwords, hard-drive locks, locked offices and filing cabinets are just a few examples of data safeguards. Below are samples of text that could be included in the agreement or contract:

Example 1:
Recipient further agrees to use appropriate safeguards to prevent use or disclosure of the information other than as provided for by this Data Use Agreement. Recipient shall promptly report to X any use or disclosure of the information not provided for by this Data Use Agreement of which Recipient becomes aware.

Example 2:
Information Safeguards. Recipient will adopt and use appropriate administrative, physical, and technical safeguards to preserve the integrity and confidentiality of the Limited Data Set and to prevent its use or disclosure, other than as permitted by Section 2 of this Agreement, as otherwise permitted in writing by Data Provider, or as required by law.

Example 3 (if data set includes Personal Health Information (PHI):

Is an adequate plan presented in the protocol to protect data from improper use, including the implementation of effective administrative, physical and technical safeguards? □ Yes □ No

Locked cabinets or rooms? □ Yes □ No

Computer password protected? □ Yes □ No

Access is limited to authorized personnel only? □ Yes □ No

Data transported by secure carrier only? □ Yes □ No

Data not accessible to the Internet? □ Yes □ No

Laptop computers never left unattended in cars or other unsecure sites? □ Yes □ No

Example 4 (if data set includes PHI):

<u>Security.</u> To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI, and provide data security procedures for the use of DHCS at the end of the contract period. These steps shall include, at a minimum:

1) Complying with all of the data system security precautions listed in the Attachment A portion of this Agreement;

2) Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement;

3) Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III-Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

4) In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of this Agreement.

Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with DHCS.

11. HIPAA and IRB

The IRB and HIPAA approvals or waivers need to be obtained before the research project can commence. Both are governed by federal law.

The IRB, Institutional Review Board, is a formal committee that reviews, approves, and monitors behavioral and biomedical research that involves humans as the research subjects. The IRB has the task of overseeing the protection of the rights and welfare of the research subjects especially when vulnerable populations are included. There are multiple types of an IRB review process of research with human subjects including Full, Expedited, and Exempt.

HIPAA stands for Health Insurance Portability and Accountability Act of 1996. This act consists of two parts, the <u>Privacy Rule</u> and <u>Security Rule</u>. The Privacy Rule establishes the standards for the protection of certain individually identifiable health information. The Security Rules provides a national set of security standards for protecting the health information that is held or transferred in electronic form.

Example 1:
<u>Description of Human Subjects Involved in the Study</u>

Limited datasets containing medical and pharmacy claims for patients enrolled in the state Medicaid program and are receiving health care services in one of the clinics participating in the pilot project will be provided by DHCS for the purpose of this evaluation.

<u>Description of the Use of Human Subjects</u>

Limited data sets constructed from pharmacy and medical claims will be provided by DHCS for the purpose of this evaluation. All data elements that directly identify subjects will be removed. The data sets will be stored in a secure area. Analytical data will be stored on password protected files and accessed only by researchers. Upon completion of this research project, data will be destroyed as soon as it is no longer needed.

- Research population consisting of vulnerable populations (children, people with disabilities, pregnant women, prisoners, etc.)
- Level of risk for participants in research

Example 1:
The risk level of this research is: Minimal □ Moderate □ High □

The risks of this research are (check all that apply):
Physical □
Psychological □
Social □
Economic □
Data security and confidentiality □

Example 2:
Assessment of Risks:

No foreseeable risks to participants in this evaluation are anticipated.

Example 3:
"Protected Health Information" or "PHI" means any information, whether oral or recorded, in any form or medium that relates to the past, present, or future physical or mental condition of any individual, the provision of health and dental care to an individual, or the past, resent, or future payment for the provision of health and dental care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended from time to time.

12. COMMUNICATION PLAN

- Primary contacts

Example 1:
Dr. X will devote at least 4-8 hours per week to this project between approximately Month Year and Month Year 2. Drs. Y and X will communicate with the rest of the team by email or phone at least twice per month (ideally weekly) to ensure timely progress, and to direct further data collection.

Example 2:
Dr. X will come to the "Name Location here" for at least a one week period for training in tobacco documents research and analysis methodology. This training will include but is not limited to: training on the Legacy Tobacco Documents Library, search terms and strategy, proper research documentation, standard tobacco document citations format and EndNote citations. Dr. X will also have opportunities to meet with full time tobacco documents researchers at the Location. Dr. A will provide funding for Dr. X's travel to City; "Organization name here" will provide work space and a computer during Dr. X's stay. Dr. Y will devote most of her research time to working with Dr. X during this trip, and Drs. Y and B will oversee his training.

13. CONFLICTS OF INTEREST AND DISCLOSURE OF FINANCIAL OR TOBACCO COMPANY TIES

Many organizations will define what constitutes a conflict of interest. In many cases, a conflict of interest is limited to a situation where one of the parties would benefit financially from the execution of the agreement. Other organizations may define a conflict of interest more broadly. In some cases, disclosure of financial ties that might or might not be considered a conflict of interest is required of all parties. For some organizations, any relationship with the tobacco industry is explicitly included as a conflict of interest.

Example 1:
Conflict of Interest

This research project is funded by "State" HealthCare Foundation. Researchers and the institutions they are affiliated with have no financial or other relationships that could be perceived as affecting the objective conduct of this evaluation.

14. AMENDMENTS

Amendments can be made and should be anticipated for agreements, especially if the agreement spans more than 6 to12 months. Some amendments are required by law (i.e., agreements involving data covered by HIPAA will require that parties agree to automatically amend their agreement to include any changes to HIPAA law that occur during the term of their agreement). Other amendments result from changes that occur during the term of the agreement (i.e., the PI leaves an institution or the work is delayed and parties agree to change the end date or due date).

Example 1:
Amendment to Agreement**.** Upon the compliance date of any final regulation or amendment to a final regulation, promulgated by the U.S. Department of Health and Human Services pursuant to the Administrative Simplification provisions of HIPAA Title II, Subtitle F, that affects Limited Data Sets, this Agreement will automatically amend such that the obligations imposed on Recipient remain in compliance with the final regulation, unless either party elects to terminate this Agreement by providing written notice of termination to the other party at least 90 days before such compliance date. The obligations of Section x of this Agreement will apply to such termination and the obligations of Sections y and z of this Agreement will survive such termination.

Example 2 (non-legally mandated):
This agreement can be amended in writing at any time by mutual agreement of all parties.

- A change in the end date or an extension of the contract that is "mutually agreed to" by all parties involved

15. TERMINATION OF AGREEMENT

Agreements may be terminated for a variety of reasons. Most contracts specify the reasons that an agreement may be terminated "for cause." In such cases, one party may terminate without having to gain consent of the other party. Agreements also may include a term for agreement by "mutual consent." This usually requires that both parties agree in writing to terminate an agreement.

Examples of both are shown below:

Example 1:
This agreement shall remain in force until the earlier of <date> of either party provides notice of termination in writing. Notice of termination shall be at least 30 Days in advance of the termination date. However, the privacy protections set forth above shall survive the termination provisions of this Data Use Agreement.

Example 2:
The terms of this memorandum are agreed to by the undersigned, with the understanding that as the research progresses, details of these arrangements may require change. In addition, if the work does not progress as anticipated, or if other problems arise, this arrangement may be terminated by mutual agreement of the undersigned.

- Identify potential causes for early termination

Example 1:
Termination for Breach* . Data Provider may terminate this Agreement if it determines, in its sole discretion, that Recipient has breached any provision of this Agreement. Data Provider may exercise this termination right by providing Recipient written notice of termination that states the breach of this Agreement that provides the basis for the termination. Any such termination will be effective immediately or at such other date specified in Data Provider's notice of termination. The obligations of Sections 3 and 10 of this Agreement will survive termination of this Agreement.
** Breach means failing to perform any term of a contract. For example, not finishing a job, failure to make payment on time, or failure to deliver goods.*

Example 2:
Termination

A) ***Termination for Cause***. Upon DHCS' knowledge of a material breach of this Agreement by Business Associate, DHCS shall:

1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by DHCS;

2) Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

3) If neither cure nor termination is feasible, report the violation to the Secretary of the US Department of Health and Human Services.

B) ***Judicial or Administrative Proceedings.*** Business Associate will notify DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. DHCS may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. DHCS may terminate this Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceedings in which the Business Associate is a party or has been joined.

C) ***Effect of Termination***. Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from DHCS (or created or received by Business Associate on behalf of DHCS) that Business Associate still maintains in any form, and shall retain no copies of such PHI or, if return or destruction is not feasible, shall continue to extend the protection of this Agreement to such information, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.