An Introduction to the HIPAA Privacy Rule

Prepared for

covering kids & families

January 2005

An Introduction to the HIPAA Privacy Rule

Prepared for

Covering Kids & Families National Program Office
Southern Institute on Children and Families
500 Taylor Street, Suite 202
Columbia, SC 29201
(803) 779-2607
www.coveringkidsandfamilies.org

Prepared by

Joy Pritts, J.D.
Health Policy Institute
Georgetown University
Washington, D.C.

January 2005

Covering Kids & Families is supported by The Robert Wood Johnson Foundation with direction provided by the Southern Institute on Children and Families.

This guide is intended to give *Covering Kids & Families* participants a general overview of the Federal Health Privacy Rule. It should not be used as a substitute for legal or other expert professional advice. The author, Georgetown University, The Robert Wood Johnson Foundation and the Southern Institute on Children and Families specifically disclaim any personal liability, loss or risk incurred as a consequence of the use of any information in this guide.

TABLE OF CONTENTS

APPENDIX

CONTENTS: DOCUMENT DESCRIPTION 48

INTRODUCTION

The Robert Wood Johnson Foundation established *Covering Kids & Families* (CKF), a nationwide project, to help reduce the number of children in America who are uninsured. *Covering Kids & Families* is designed to help increase the number of children and families who benefit from Medicaid and the State Children's Health Insurance Program (SCHIP). The project does this through grants that support state and local coalitions' efforts to find, enroll and retain eligible children and families.

Covering Kids & Families statewide and local project participants (CKF participants) perform a number of different activities to help achieve the goal of the project. As part of general outreach, CKF participants educate people about Medicaid and SCHIP, identify people who may be eligible for the programs, and help people complete applications for Medicaid and SCHIP. In order to follow up on applications, CKF participants often obtain client-level data from Medicaid and SCHIP to help complete the enrollment process or to make sure the client remains enrolled. Some participants also request group data from Medicaid and SCHIP to conduct research and to monitor enrollment and retention rates.

THIS GUIDE

Covering Kids & Families participants are concerned that recent changes in federal law may interfere with their ability to perform crucial activities. They are particularly concerned about the Federal Health Privacy Rule (the Privacy Rule), also known as HIPAA.[1]

The purpose of this resource guide is to address those concerns. Part I of the guide gives a general overview of the HIPAA Privacy Rule that describes what the Privacy Rule is, who it covers and what information it protects. This part also explains the Privacy Rule's limits on how information related to health, health care and payment for health care can be used within an organization and disclosed to others. The guide then discusses HIPAA's impact on the Medicaid and SCHIP programs in the sections that explain the rules for "health plans."

HIPAA is very detailed. Its rules change depending on who is holding the information, to whom the information is being disclosed and the purpose for disclosing the information. It is likely that HIPAA will have an impact on most CKF participants because they interact with Medicaid and SCHIP programs that are covered by HIPAA. HIPAA's effect on any particular CKF participant is largely determined by whether its activities are covered by the Privacy Rule. As a community- or faith-based organization, a CKF participant is most likely to be covered by HIPAA, if at all, in the role of a health care provider. Part II, therefore, is designed to help CKF participants determine whether they are covered health care providers under HIPAA. Once an organization's status is determined, it can refer directly to the relevant section in Part III that explains HIPAA's potential impact on its CKF-related activities.

1. HIPAA stands for the Health Insurance Portability and Accountability Act of 1996.

Part III is designed to explain how the Privacy Rule may affect some CKF participants. This part of the guide focuses on the impact of the HIPAA Privacy Rule on two general categories of CKF participants: those who are *not* covered health care providers under HIPAA and those who *are* covered providers. It describes how HIPAA may affect some of the more common CKF activities. These sections of the resource guide are written as stand-alone discussions so that each can be reviewed separately. Because some areas of impact are common to both groups, there is some repetition in the two sections.

It is important to remember that the explanations in the guide are general in nature. The rules of HIPAA vary greatly depending on the particular circumstance for using and disclosing information related to health, health care and payment for health care. It is not possible for this resource guide to discuss all the different participants and activities related to the CKF project, nor can it address all the various procedures that Medicaid and SCHIP programs have adopted under the Privacy Rule.

This guide focuses on the Privacy Rule's limits for using and disclosing health-related information. There are also a number of other aspects to the Privacy Rule. For example, the Rule gives individuals the right to see and copy their own health information. It also imposes a variety of duties on those who are covered by it. Those who are interested in these other aspects of the Rule should read Appendix A: "Summary of the Privacy Rule's Additional Requirements." They should also consult the additional resources listed in Appendix C.

EXECUTIVE SUMMARY

The Health Insurance Portability and Accountability Act of 1996 Privacy Rule is a new federal law that governs the privacy of health-related information. The purpose of this resource guide is to explain the general requirements of the Privacy Rule and to describe how the Rule may impact CKF participants.

Overview of the HIPAA Privacy Rule

HIPAA contains a section called "Administrative Simplification" that is designed to help the health care system move to a uniform, computer-based information system. Because Congress was concerned about the vulnerability of health information when it is kept and transmitted electronically, it directed the United States Department of Health and Human Services (HHS) to write rules protecting the privacy of health information.[2] This set of rules is called the Federal Health Privacy Rule ("the Privacy Rule").

2. Congress also directed HHS to develop other rules to put this computerized health information system into place. These rules are in various stages of development and include rules covering transactions and code sets, unique identifiers and security. A summary of these Administrative Simplification rules is contained in Appendix B.

Scope of the Privacy Rule
Although many people have access to health information, the Privacy Rule directly covers only three core groups: health plans, health care clearinghouses and health care providers who use computer technology to send information related to certain administrative and financial transactions (such as claims for payment). These groups are collectively called "covered entities." Medicaid and SCHIP programs are covered by HIPAA because they are health plans.

The Privacy Rule protects information that relates to an individual's past, present and future: health, health care and payment for health care. Only information that identifies or can be used to identify the person is protected under HIPAA. The Privacy Rule lists a number of items ("identifiers") that can be used to identify a person, including some demographic information. The Rule also creates a subset of identifiable information called a "limited data set" that includes only the following identifying information: a person's city or town, state, ZIP code and coded information. Without permission being given by all the people included in the data set a limited data set can be disclosed only for research, public health and health care operations purposes. Information that has been "de-identified" is not protected by the Privacy Rule and can be freely disclosed. Information can be de-identified by removing all of the identifiers (such as names, Social Security numbers and addresses) listed in the Rule. It can also be de-identified by having a qualified statistician determine that there is only a very small risk that the information could be used to identify the person who is the subject of the information.

What Does the Privacy Rule Do?
The Privacy Rule is the first national law that controls how health information can be used within an organization and disclosed to others. Under the Privacy Rule, covered health care providers and health plans may not use or disclose protected health information unless: 1) There is a section of the Privacy Rule permitting that particular use or disclosure, or 2) they have the written permission (authorization) of the individual who is the subject of the information.

The Privacy Rule sets out some general principles that apply to using and disclosing information for most purposes. In general, the Rule permits disclosures for many health care-related purposes but does not *require* these disclosures. Additionally, when a covered health plan or provider discloses information under the Privacy Rule, it should disclose only the minimum amount of information necessary.

The Rule also permits covered providers and plans to share information without individual authorization with others who perform business-related activities on their behalf. In order to share information in this way, the covered plan or provider must have established a business associate contract with the recipient of the information.

In addition to these fairly general standards, the Privacy Rule permits covered providers and plans to disclose health information without the individual's authorization for a number of specific purposes. Covered plans and providers do not need authorization to use and disclose health information for purposes that are core to the health care system: treatment, payment and health care operations. The Rule also permits covered plans and providers to use and disclose information without the individual's authorization for a number of public priority purposes

including research, health oversight and public health. The covered plan or provider must meet certain conditions in order to disclose information for such public policy purposes.

HIPAA's impact on Medicaid/SCHIP is of particular interest to CKF participants who interact with these programs. Medicaid and SCHIP are health plans covered by HIPAA, and as such they must follow the Privacy Rule's requirements. The Rule protects Medicaid/SCHIP enrollment information because it is information related to the payment for health care. This means that Medicaid/SCHIP programs cannot disclose enrollment information unless one of the following conditions is met: the enrollment information has been de-identified; there is a section of the Privacy Rule that permits the programs to disclose identifiable information to the person who requested it for the recipient's intended purpose; or the programs have authorization from the people whose information is requested.

Is a CKF Participant a Covered Health Care Provider Under HIPAA?

The Privacy Rule affects CKF participants in a variety of ways depending on whether a particular CKF participant is directly covered by HIPAA. Many CKF participants are not directly covered by HIPAA but will be affected indirectly by the Rule because they interact with Medicaid/SCHIP programs; other CKF participants are directly covered by the Rule. As a community- or faith-based organization, if a CKF participant is covered by HIPAA at all, it is likely that it is as a covered health care provider. A CKF participant is a covered health care provider only if it carries on all three of the following activities:

- Provides health care in the regular course of business.
- Has "covered transactions" (such as filing claims for payment or obtaining authorization for treatment).
- Sends information for these covered transactions "electronically" (using computer technology such as the Internet or floppy diskettes).

Covering Kids & Families participants that are directly covered by HIPAA must follow all its requirements.

HIPAA's Potential Impact on *Covering Kids & Families* Statewide and Local Project Participants

The rules for sharing health information under the HIPAA Privacy Rule vary greatly according to the circumstances in which information is disclosed. They change depending on who discloses the information, to whom the information is disclosed and the purpose for which it is disclosed. The chart on the following pages gives a brief overview of HIPAA's potential impact on some common activities of CKF participants. Detailed explanations of the rules affecting various activities appear in the full text of the resource guide.

Summary of HIPAA's Impact on CKF Participants

	CKF Participants Covered by HIPAA		CKF Participants NOT Covered by HIPAA	
Activity	**Privacy Rule Requirement**	**Notes**	**Privacy Rule Requirement**	**Notes**
Awareness outreach (e.g., education about Medicaid and SCHIP programs)	None	Does not involve protected health information.	None	
Identifying clients who may be eligible for Medicaid/ SCHIP	None—if done in the context of identifying a potential source of payment.	A covered provider can use protected health information for payment activities without the authorization of the patient.	Not applicable	Not applicable
Outreach directed to individuals Collect information about or from potential applicants Help people in gathering information and filling out their applications Send application information to a Medicaid/SCHIP program	None	This assumes these activities are not done as part of making presumptive eligibility determinations. A covered provider can disclose protected health information to a covered plan for its payment activities (including eligibility determination) without the authorization of the patient.	None	This assumes these activities are not done as part of making presumptive eligibility determinations. Those who are not covered by HIPAA do not need an applicant's permission to disclose their information to Medicaid/SCHIP.
Presumptive eligibility determinations	Business associate contract	Obtaining and processing information on behalf of Medicaid/SCHIP requires a business associate contract. The contract can include other permitted activities.	Business associate contract	Obtaining and processing information on behalf of Medicaid/SCHIP requires a business associate contract. The contract can include other permitted activities.

	CKF Participants Covered by HIPAA		CKF Participants NOT Covered by HIPAA	
Activity	**Privacy Rule Requirement**	**Notes**	**Privacy Rule Requirement**	**Notes**
Presumptive eligibility determinations (continued)		Information can only be used and disclosed for the particular activities listed in the contract.		Information obtained under a business associate contract can only be used and disclosed for the particular activities listed in the contract. (Same as "Covered")
Disclosing patient information to Medicaid/SCHIP to ask follow-up questions to assist with application process	None	Disclosing information for payment (including determining eligibility) does not require patient authorization.	None	
Obtaining client-level application data from Medicaid/SCHIP to assist with application process	Could be any of the following: • No change • Authorization of client • Business associate contract with Medicaid/ SCHIP	It is not clear whether "application" data is protected under the Privacy Rule. *HHS needs to clarify*. In the meantime, expect various interpretations.	Could be any of the following: • No change • Authorization of client • Business associate contract with Medicaid/ SCHIP (Same as "Covered")	It is not clear whether "application" data is protected under the Privacy Rule. *HHS needs to clarify*. In the meantime, expect various interpretations. (Same as "Covered")
Verifying enrollment for payment purposes	None—if done within context of obtaining payment for health care.	Medicaid/SCHIP can verify whether patient is (or is not) enrolled for payment purposes without patient authorization. Does not include details of application/enroll-ment process since the provider does not need this for payment purposes.	Not applicable	Not applicable

	CKF Participants Covered by HIPAA		CKF Participants NOT Covered by HIPAA	
Activity	**Privacy Rule Requirement**	**Notes**	**Privacy Rule Requirement**	**Notes**
Obtaining client-level enrollment data from Medicaid/SCHIP to assist with the renewal process	Authorization of client (most likely) or Business associate contract (maybe)	Which document is required will depend on whether the Medicaid/SCHIP program sees CKF participant as acting on behalf of the client (most likely) or on behalf of the program.	Authorization of client (most likely) or Business associate contract (maybe)	Which document is required will depend on whether the Medicaid/ SCHIP program sees CKF participant as acting on behalf of the client (most likely) or on behalf of the program.
Obtaining Medicaid/SCHIP group data that includes only state and year for research	None	If the only identifying information that is included in data is the state where the enrollee lives and year related to the enrollment data, the information is not protected under HIPAA. Example: Number of children under the age of one enrolled in a state Medicaid program.	None (Same as "Covered")	If the only identifying information that is included in data is the state where the enrollee lives and year related to the enrollment data, the information is not protected under HIPAA. Example: Number of children under the age of one enrolled in a state Medicaid program. (Same as "Covered")
Obtaining group data that has been statistically determined to be "de-identified"	Must follow rules for statistically determining whether information is identified. Once data has been de-identified, it is not protected by Privacy Rule.	Data that includes identifying information may be de-identified by a qualified statistician who determines that there is a very small risk that the information (alone or with other reasonably available information) could be used to identify the individuals who are included in the data.	Must follow rules for statistically determining whether information is identified. Once data has been de-identified, it is not protected by Privacy Rule.	Data that includes identifying information may be de-identified by a qualified statistician who determines that there is a very small risk that the information (alone or with other reasonably available information) could be used to identify the individuals who are included in the data.

	CKF Participants Covered by HIPAA		CKF Participants NOT Covered by HIPAA	
Activity	**Privacy Rule Requirement**	**Notes**	**Privacy Rule Requirement**	**Notes**
Obtaining group data that has been statistically determined to be "de-identified" (continued)		Medicaid/SCHIP can, but is not required to, de-identify information.		Medicaid/SCHIP can, but is not required to. de-identify information.
Obtaining Medicaid/SCHIP group data in a "limited data set" for research	Information can only include the following identifiers: • City or town, state, ZIP code • Dates • Coded information Must have a data use agreement with Medicaid/ SCHIP.	Applies to identifiable information. Research must be for "generalizable" knowledge **(**knowledge that can apply to groups outside the particular Medicaid/SCHIP). Whether study is going to be published is one test to determine whether study counts as research.	Information can only include the following identifiers: • City or town, state, ZIP code • Dates • Coded information Must have a data use agreement with Medicaid/ SCHIP. (Same as "Covered")	Applies to identifiable information. Research must be for "generalizable" knowledge **(**knowledge that can apply to groups outside the particular Medicaid/SCHIP). Whether study is going to be published is one test to determine whether study counts as research. (Same as "Covered")
Obtaining identifiable Medicaid/SCHIP group data that includes additional data (e.g., name or telephone number) for research	Institutional Review Board or Privacy Board approval or Authorization of all individuals included in the data	Research must be for "generalizable" knowledge. Whether study is going to be published is one test to determine whether study counts as research.	Institutional Review Board or Privacy Board approval or Authorization of all individuals included in the data (Same as "Covered")	Research must be for "generalizable" knowledge. Whether study is going to be published is one test to determine whether study counts as research. (Same as "Covered")
Obtaining identifiable group data to monitor Medicaid/SCHIP	Authorization of all individuals included in the data.	Assumes that CKF participant is not doing this activity on behalf of the Medicaid/SCHIP program.	Authorization of all individuals included in the data. (Same as "Covered")	Assumes that CKF participant is not doing this activity on behalf of the Medicaid/SCHIP program.

	CKF Participants Covered by HIPAA		CKF Participants NOT Covered by HIPAA	
Activity	**Privacy Rule Requirement**	**Notes**	**Privacy Rule Requirement**	**Notes**
Obtaining identifiable group data to monitor Medicaid/SCHIP (continued)		Applies to group information that is identifiable. Rule permits disclosure without individual authorization for oversight purposes only to health oversight agencies. Health oversight agencies are government agencies or their contractors in charge of overseeing health care system. **Cannot** use limited data set for monitoring.		Applies to group information that is identifiable. Rule permits disclosure without individual authorization for oversight purposes only to health oversight agencies. Health oversight agencies are government agencies or their contractors in charge of overseeing health care system. **Cannot** use limited data set for monitoring. (Same as "Covered")

Conclusion

Overall, HIPAA should not prevent CKF participants from undertaking many of their important CKF-related activities. Participants may, however, be required to follow slightly different procedures for obtaining client-level information. The ease of obtaining group data will depend on the level of detail of the information requested. Participants should be able to obtain very general group data aggregated at the state level without any changes, as this information is not protected by the Privacy Rule. Participants may have a more difficult time obtaining group data that is aggregated at the county level. Medicaid/SCHIP programs can freely disclose this data if they have de-identified it, using approved statistical methods. When Medicaid/SCHIP programs are either unable or unwilling to conduct such de-identification, the programs are required to follow the Privacy Rule's detailed requirements for disclosure. In this case, participants might encounter problems in obtaining identifiable group data for research and monitoring. Because of HIPAA's limits on how identifiable information may be disclosed to others, Medicaid and SCHIP programs may be unable to provide certain types of group data to CKF participants for monitoring purposes.

PART I
OVERVIEW OF THE HIPAA PRIVACY RULE

BACKGROUND

In response to rising administrative health care costs, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[3] One part of HIPAA, called "Administrative Simplification," is intended to reduce the administrative costs of health care by encouraging the health care industry to adopt a uniform, computer-based system for storing and exchanging health information.[4] Using a single computerized format should make sending and processing health information easier, faster and less expensive.

But Congress also recognized that moving to a computer-based system increases concerns about the privacy and security of health information. Because of these concerns, Congress gave the Secretary of the United States Department of Health and Human Services (HHS) the power to make rules protecting the privacy of health information.

The United States Department of Health and Human Services issued the Privacy Rule in December 2000 and made major changes to it in August 2002. This Rule creates the first general federal protections for the privacy of health information. The Rule's core provisions restrict how health information may be used within an organization and how the information may be disclosed to others.[5] The Rule is still relatively new. Only since April 2003 have people and organizations that are covered by the HIPAA Privacy Rule had to comply with its requirements.

The Office for Civil Rights (OCR) within HHS is in charge of enforcing the Privacy Rule. In this role, OCR has the duty to help people figure out what they need to do to comply with the Privacy Rule. Additionally, OCR is responsible for receiving and responding to complaints about violations of the Privacy Rule.

This resource guide is intended to summarize only the portion of the Privacy Rule that limits the use and disclosure of health-related information and to highlight how the Rule may affect those involved in the *Covering Kids & Families* program. Those who are covered by the HIPAA Privacy Rule should become familiar with all of its requirements. The complete text of the Rule is available at: *http://www.hhs.gov/ocr/combinedregtext.pdf.* Appendix A of this guide gives a

---

3. Well over 10¢ of every health care dollar goes toward administrative expenses. See Steffie Woolhandler, Terry Campbell, David Himmelstein, "Costs of Health Care Administration in the United States and Canada," *The New England Journal of Medicine*, vol. 349, no. 8, pp. 768, 771 (August 21, 2003). Executive summary available free at *http://www.citizen.org/publications/release.cfm?ID=7271*.

4. Another primary purpose of HIPAA (the portability portion) is to make sure people are able to continue their health insurance when they change or lose their jobs.

5. The Privacy Rule also gives people new rights in managing their own health information, including the right to see, copy and correct their medical record. Appendix A summarizes these rights.

summary of some of its additional requirements. Other official resources that explain the Privacy Rule are listed in Appendix C.

SCOPE OF THE PRIVACY RULE

In order to understand the HIPAA Privacy Rule, it is necessary to know exactly who it applies to and what information it protects. The Rule does not cover everyone who holds health information — it only covers a select group of people and organizations who are known as "covered entities." Furthermore, while the Privacy Rule covers a broad range of medical record, billing and enrollment information, it does not cover all the information related to a person's health.

Who Is Directly Covered by the Privacy Rule?

Although many people and organizations have access to health information, not all of them are covered by the HIPAA Privacy Rule. The Rule directly covers only a core group of those in the health care system.[6] This core group includes:

- **Health plans**, including HMOs, fee-for-service insurers, Medicaid, Medicare, SCHIP and any other individual or group plan that provides or pays for health care.
- **Health care providers** who send certain administrative and financial information "electronically" (i.e., using computer technology).
- **Health care clearinghouses**, which are people or organizations that translate health information into and out of a uniform computerized format that health providers and health plans are required to use when they send information electronically for certain purposes.[7]

The HIPAA Privacy Rule calls these three groups "covered entities." Because most CKF participants will not need to interact with health care clearinghouses, this guide does not further discuss this third group of covered entities.

What Is Covered by the Privacy Rule?

The Rule covers only certain types of health information, called "protected health information." To be protected by the Rule, information must meet a three-part test. It must:

- Be "health information" as defined in the Privacy Rule.
- Identify (or be able to be used to identify) the person who is the subject of the information.
- Be created or received by a covered provider or health plan.

---

6. Congress determined that only this core group would be covered by HIPAA. HHS does not have the power to change who is covered by the rule.

7. Under HIPAA, HHS has issued rules called "Transaction Standards" that require health plans and health care providers to use certain computer coding formats when they send each other information for submitting health claims, paying health claims and other financial and administrative purposes. There is detailed information about "Transaction Standards" on CMS's Website, at http://www.cms.hhs.gov/hipaa/hipaa2/default.asp.

Health Information

HIPAA defines the term "health information" very broadly. Health information includes information that is about a person's past, present or future physical or mental health; the care that they receive; and the past, present or future payment for their care. Health information includes a doctor's notes, test results and similar material. It also includes enrollment information and billing records.

Is Medicaid Enrollment Data "Health Information"?

Yes. The fact that someone is enrolled in Medicaid is "health information" because it is related to the payment of their health care.

What About Medicaid Application Data?

This is an open question. Most people believe that applicant information fits in the definition of health information because it is related to the decision of Medicaid (a health plan) whether it will pay for an individual's health care. Some people believe that applicant information does not fit this definition because if the person's application is denied, their information will never be related to payment. (If a person is eventually enrolled, of course, their application information becomes covered.) We hope that HHS will clarify this issue in the near future.

Individually Identifiable Information

The HIPAA Privacy Rule protects "individually identifiable" health information. "Individually identifiable" means that the health information either identifies the person it is about (by using their name, for example) or contains information that could be used to identify the person (such as their Social Security number or their medical record number). The Rule contains a list of 18 items, called "identifiers," that can be used to identify a person. Many of these identifiers are items that when combined with other information can be used to identify a person (such as a person's age and where they live). For instance, cities, towns and ZIP codes associated with a person's health information are identifiers. Appendix D contains a complete list of the identifiers.

This broad definition of individually identifiable information could interfere with certain uses of group data that benefit the public (such as for research). To solve this potential problem, HHS created a subgroup of information called a "limited data set." A limited data set contains only a few identifiers that do not directly identify the person, including a city or town, state, ZIP code, dates and coded information.[8] The rules for when a limited data set may be used are discussed in more detail in *Obtaining Group or Aggregate Data*, in Part III. The Privacy Rule does not cover

8. Limited data sets are discussed in detail in Part III of the guide.

information that is “de-identified.” Information can be de-identified in two ways. One way to de-identify information is to remove all 18 of the listed identifiers from the data. Alternatively, data can be de-identified by having a qualified statistician determine that the risk is very small that the information can be used (alone or in combination with other reasonably available information) by the recipient to identify an individual who is the subject of the information. For example, a statistician could determine that the number of people eligible for Medicaid in a given county is de-identified information because there is little risk that the eligible individuals could be identified. Once information is de-identified, it is not covered by the Privacy Rule and can be disclosed for any purpose.

Is Group or Aggregate Data Individually Identifiable Information?

It depends on what information is included in the data group. Group data falls within one of three categories:

1. **De-identified Information:**
   - Generally, must have all 18 identifiers removed. It can contain the state the person lives in and their age expressed in years.
     - **Example**: The total number of people enrolled in a state's Medicaid program, grouped by age (years).
   - Is statistically de-identified. Information that includes some of the 18 identifiers can be de-identified if a qualified statistician determines the risk is very small that the information can be used (alone or in combination with other reasonably available information) by the recipient to identify an individual who is the subject of the information.
     - **Example**: A group of data aggregated by county that has been determined by a qualified statistician to pose a very small risk that the individuals included in it could be identified.

De-identified information is not covered by the Privacy Rule.

2. **Individually Identifiable Information**
   - Contains any one of the 18 identifiers listed in the Privacy Rule including name, address, city or town, ZIP code, Social Security number, etc.
     - **Example**: A list of people enrolled in a state's Medicaid program that includes their name or phone numbers.

This information is covered by the Privacy Rule and is subject to detailed rules about when it can be disclosed to others.

3. **Limited Data Set**
   - A subset of individually identifiable information. It can contain only the following identifiers: city or town, state, ZIP code, dates and coded information.
     - **Example**: The number of people enrolled in a state's Medicaid program, grouped by ZIP code and by age.

This information is covered by the Privacy Rule but may only be used for research, public health or health care operations. Information in a limited data set is subject to a less restrictive set of rules than other identifiable information.

Part III contains a full discussion of when group data is identifiable and whether it can be disclosed.

Information Created or Received by a Covered Health Provider or Health Plan

Health information is only protected under HIPAA if it was created or received by a covered health plan or health care provider. For example, medical records kept by hospitals are protected health information because health providers created the records. Similarly, enrollment data maintained by a Medicaid program is protected health information because it was created by a health plan.

HIPAA only protects information that meets all three of the tests listed above. The information must:

- Be about a person's health, the health care they receive or payment for their care.
- Identify the person who is the subject of the information (or be able to be used to identify that person).
- Be created or received by a covered health care provider or plan.

RULES FOR USING AND DISCLOSING HEALTH INFORMATION

One of the main purposes of the HIPAA Privacy Rule is to limit when and how health information can be "used" and "disclosed."[9] Both words have very specific meanings in the Privacy Rule. Under HIPAA, the word "use" means using health information within an organization. For example, a nurse in a doctor's office who reviews a patient's medical chart "uses" the patient's health information. In contrast, the word "disclose" means sharing health information outside an organization. For example, a doctor's office that sends a claim for payment to Medicaid "discloses" the patient's health information to the program. This distinction is important because at times the rules for using health information are different from those for disclosing the health information to others.

HIPAA contains some rules that apply generally to using and disclosing health information. It also has many rules that apply to using and disclosing health information for specific purposes.

General Rules

In general, covered providers and plans can use and disclose health information either 1) as specifically permitted or required by the Privacy Rule, or 2) as authorized (permitted in writing) by the person who is the subject of the information. This written permission is usually known as "individual authorization." There are a few circumstances where the Privacy Rule specifically requires an authorization.[10]

9. The HIPAA Privacy Rule also creates rights for patients and duties for covered entities. These portions of the Privacy Rule are briefly summarized in Appendix A.

10. For example, a provider *must* have a patient's authorization to use or share psychotherapy notes for most purposes other than directly treating the patient. Psychotherapy notes must be kept separate from the rest of the medical record to qualify for this increased protection.

1) Disclosing health information to others is often permitted but rarely required. HIPAA *requires* covered providers and plans to disclose health information only in two circumstances: 1) to the person who is the subject of the health information, when they request access to it, and 2) to HHS for purposes of enforcing the Privacy Rule. Other allowed uses and disclosures that are listed in the Rule are permitted, but are not mandatory. For example, HIPAA permits providers to disclose health information to a public health authority for public health purposes, but it does not *require* providers to furnish information to a public health authority.

2) The amount of information disclosed should be kept to the minimum amount necessary. Another overall principle of HIPAA is that covered health care providers or plans generally must limit the health information they use and disclose to the minimum amount necessary to accomplish the intended purpose. This principle is often called the "minimum necessary rule." In general, the minimum necessary rule requires providers and plans to decide as a matter of policy the amount of information necessary to accomplish routine activities. It does not require the provider or plan to decide how much information to use or disclose on a case–by-case basis.[11]

3) Sharing health information with "business associates" (those who perform activities on behalf of a covered health care provider or plan that health information). Health plans and providers routinely rely on others to provide activities that are essential to their business and that require the use and disclosure of health information. For example, many health care providers hire someone else to do their billing; health plans often hire others to process health insurance claims. HIPAA calls these people and organizations "business associates." Although business associates need access to health information to carry out their work, they are not directly covered by the Privacy Rule because they are not actual covered entities.

   The Privacy Rule attempts to fill this gap by requiring that covered providers and plans sign contracts with "business associates." These contracts require business associates to do many of the same things required by the Privacy Rule. For example, a business associate must promise to protect the confidentiality of the information that it receives. It must also promise that it will use and disclose the information only as permitted by the contract. The Rule contains many other requirements for these contracts. A sample business associate contract written by the HHS Office for Civil Rights is included in Appendix E.

11. There are a few exceptions to the minimum necessary rule. First, the minimum necessary rule does not apply when a provider asks for or discloses health information for treatment purposes. HHS does not want providers to have to second-guess what information is really necessary for treatment. Second, the rule does not apply when covered providers and plans must disclose information under another law. For instance, when a state requires a provider to report the names of patients with certain diseases, the provider is not required to decide what patient health information is the minimum necessary to accomplish the state's purpose—it only needs to comply with the state law.

Once a covered health care provider or plan has signed the required contract with the business associate, the provider or plan can disclose protected health information to the business associate for any purpose permitted by the Privacy Rule without obtaining individual authorization. They also can permit the business associate to create or receive protected health information on their behalf. However, the business associate contract only can permit the business associate to use and disclose information in the same manner that the covered plan or provider itself can use and disclose the information under the Privacy Rule. A covered plan or provider can authorize the business associate to perform multiple activities in a business associate contract, *so long as all activities are permitted under the Rule*. For example, a doctor can use a single business associate contract to permit a third-party administrator both to bill patients and to negotiate payments from a health insurance plan.

Even though business associates are indirectly required by their contracts to follow some of HIPAA's rules, they are not directly covered by the Privacy Rule. This means that HHS cannot force them to follow the terms of their business associate contracts. If a business associate violates its contract, there is nothing that HHS can do to punish it.

Rules for Using and Disclosing Health Information for Specific Purposes

In addition to these general rules, the Privacy Rule permits covered providers and health plans to use and disclose health information for a number of specific purposes *without* the permission of the person who is the subject of the information. In this area, the Rule sets different standards depending on:

- Who is using or disclosing the information.
- To whom the information is being disclosed.
- The purpose for using or disclosing the health information.

This section provides an overview of the rules that apply to some of the main purposes for using and disclosing health information.

Treatment, payment and health care operations

Health information is critical for the three core activities of the health care system: treatment, payment and health care operations. These activities are broadly defined under HIPAA. Treatment, for example, means providing, coordinating or managing health care. Payment includes any efforts to obtain or provide reimbursement for health care or premiums for health care. Payment includes functions such as billing, claims management, eligibility determinations and utilization review. The term "health care operations" is defined by a list of activities that includes quality assessment, business planning, customer service, training and similar functions. The Privacy Rule allows providers and plans to use and disclose health information for their treatment, payment and health care operations purposes *without* the individual's authorization. A hospital, for example, does not need a patient's authorization to submit a claim for payment to an insurance company.[12]

12. The standards for disclosing health information to other entities for *their* payment and health care operations purposes are slightly different. For example, some health plans request health information from doctors to assess the quality of care for which the plan has paid. In this circumstance, the doctor can share a person's health information

Footnote continued on the following page.

"Public priority" purposes

The Privacy Rule also permits providers to use and disclose health information for a wide variety of what HHS calls "public priority" purposes. These activities include:

- Any disclosure that is required by another law
- Public health
- Law enforcement
- Health oversight
- Research
- Workers' compensation
- Others

Health care providers and health plans are permitted to disclose health information for all of these purposes *without* the individual's authorization. For most of these activities, the Rule requires that additional conditions be met before the health information can be disclosed. These conditions can be quite detailed. For example, health care providers and plans can disclose health information for research purposes only when the researcher has either signed a data use agreement or has had their research project approved by an Institutional Review Board (IRB) or a Privacy Board. There is a detailed discussion on disclosing protected health information for research purposes in Part III, "Obtaining Group Data."

It is important to remember that while this part of the Privacy Rule *permits* health care providers and health plans to make disclosures for these public interest purposes, it does not *require* them to do so. For instance, the Rule does not require a health plan to disclose information to a researcher, even if the researcher has obtained approval from an IRB.

When individual authorization is required[13]

A covered health care provider or health plan must get an individual's authorization to use or disclose their health information for any purpose that is not expressly permitted or required by the Privacy Rule. To be valid, an authorization form must meet the detailed requirements specified in the Rule. Among other things, an authorization must be in writing and be signed and dated by the patient. The authorization must also state when it expires. The expiration can be based on a date (such as a month, day and year). Alternatively, the expiration can be based on an

---

with the health plan only if the person is both a patient of the doctor and enrolled in that health plan or has some other relationship with it.

13. For some purposes, the Privacy Rule permits plans and providers to disclose information without the individual's authorization as long as they give the individual a chance to say they do not want their information disclosed. For example, providers and plans do not have to get the patient's authorization for disclosures for facility directories and to family members and others involved in the individual's care or payment of care. Instead, they need to give patients an opportunity to say that they do not want the provider to share the information for these purposes. The Privacy Rule recognizes that there will be times when patients are not able to make these decisions, such as when they are unconscious. In these circumstances, the Rule encourages providers to use their professional judgment. Providers (such as hospitals) also are allowed to use patients' information for fund-raising purposes without their authorization provided they offer the patients the opportunity to have their names removed from the mailing list.

event. For example, a person can authorize a health plan to disclose their information to health care providers until that person is no longer enrolled with that insurance company. Appendix F contains a sample authorization form.

Interaction with Other Medical Privacy Laws

The HIPAA Privacy Rule is not the only law that controls the privacy of medical information. Every state has laws that restrict how health information is used and disclosed. In addition to HIPAA, the federal government has other laws that protect the privacy of medical information in certain contexts. For instance, federal regulations govern the privacy of substance abuse records kept by federally assisted alcohol or drug abuse programs. HIPAA sets rules for how the Privacy Rule interacts with these other privacy laws.

An Example of How Preemption Works: Disclosures for Research

HIPAA allows health plans to disclose information for any research purpose so long as certain conditions are met.

In contrast, many state Medicaid laws allow information to be shared for research only where the research is directly connected with the administration of Medicaid.

Because the Medicaid standard is stronger than the HIPAA standard, the Medicaid standard remains in place. Even if all the HIPAA standards are met, the Medicaid agency can release Medicaid information only if the research is directly connected with the administration of the program.

State laws

The interaction of the HIPAA Privacy Rule with state law is quite complicated. In very general terms, state laws that are contrary to the federal regulation and that are less protective are preempted (overridden) by HIPAA. HIPAA generally leaves in place parts of state laws that provide health care consumers with privacy protections that are equal to or greater than those contained in HIPAA.[14]

Federal laws

HIPAA's interaction with other federal laws is equally complex. If there are no conflicts between the laws, both laws stand. If there is a conflict between HIPAA's standards and those set by another federal law, HHS will determine whether Congress intended to override the older statute when it enacted HIPAA. HHS believes that because the uses and disclosures under HIPAA are often permissive (not required), few such conflicts should occur.

14. There are, of course, exceptions to this general rule. Most public health reporting laws remain in place even though they may be viewed as less protective of a patient's privacy. Additionally, state parental notification laws are *not* affected by HIPAA.

ENFORCEMENT OF THE PRIVACY RULE

The United States Department of Health and Human Services Office for Civil Rights (OCR) is in charge of enforcing the Privacy Rule. At this time, OCR does not audit health plans and providers to make sure they are complying with the Rule, but bases its investigations solely on the complaints it receives. This policy may change in the future.

Although those covered by HIPAA should not take compliance with the Privacy Rule lightly, they need not be over-concerned about severe punishment if they unintentionally violate the Rule. OCR first seeks voluntary compliance for violations of the Privacy Rule. If it is unable to resolve non-compliance issues informally, the agency can impose a $100 civil penalty, up to a maximum of $25,000 per year, for each rule violated. OCR also can seek criminal penalties up to a maximum of $250,000 for intentional wrongful disclosures of health information.

Key Points About Medicaid/SCHIP and Disclosures of Health Information

- Medicaid /SCHIP programs are health plans that must follow the Privacy Rule.
- The Privacy Rule protects Medicaid/SCHIP enrollment information because it is considered to be "health information."
- Medicaid/SCHIP programs cannot disclose enrollment information unless:
  - There is a section of the Privacy Rule that permits the programs to disclose the information to the person who requested it for the recipient's intended purpose.
    or
  - The programs have the authorization of the people whose information is requested.
- To the extent state Medicaid/SCHIP confidentiality laws are more restrictive than the Privacy Rule, the state laws remain in place.

PART II
IS A CKF PARTICIPANT A COVERED HEALTH CARE PROVIDER UNDER HIPAA?

The HIPAA Privacy Rule may have an impact on the activities of various CKF participants. Some may be directly affected by HIPAA because the Privacy Rule covers them. Others may be affected indirectly because they interact with Medicaid/SCHIP programs that are covered by HIPAA. How HIPAA affects a CKF participant depends largely on whether they are directly covered by the Privacy Rule.

Most of the governmental agencies that participate in CKF have already determined their status under HIPAA. This portion of the resource guide, therefore, focuses on those CKF participants who are community- and faith-based organizations and the volunteers who work with them. Such CKF participants are unlikely to be health plans or health care clearinghouses. It is probable that if they are covered by HIPAA at all it is as health care providers. This part of the guide is aimed at helping CKF participants determine whether they are a health care provider covered by HIPAA.

TEST TO DETERMINE WHETHER A CKF PARTICIPANT IS A COVERED HEALTH CARE PROVIDER

To be a covered health care provider under the HIPAA Privacy Rule, a CKF participant must do *all three* of the following activities:

1. Provide "health care" in the regular course of business.
2. Have certain administrative or financial transactions ("covered transactions").
3. Use computer technology to send information related to these covered transactions ("electronically" send information).

Each of these activities is described in detail below. If a CKF participant answers Yes to all ***three*** questions, it is a covered health care provider under HIPAA.

1. Provides "health care"

Under the HIPAA Privacy Rule, a health care provider is someone who regularly gives, bills or receives payment for health care, health services or health supplies in the normal course of business. "Health care" is broadly defined under the Rule as care, services or supplies related to the health of an individual. The term includes, but is not limited to, the following: "preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body." Health care also includes selling or dispensing drugs, devices or equipment with a prescription. Some examples of health care that a community- or faith-based organization might provide include:

- Vision or hearing tests
- Immunizations
- Mental health counseling

- Case management
- Family planning services
- Other types of care

Giving health care sporadically does not qualify as providing health care under HIPAA. This must be a regular activity. For example, an office administrator who occasionally hands out an aspirin or bandage does not qualify as a "health care provider" because this is not providing health care "in the normal course of business."

Does the CKF participant provide health care?

Yes **OR** **No**

---

2. Perform "covered transactions"
The HIPAA Privacy Rule covers only health care providers who have certain administrative costs because they have "covered transactions." In general, these transactions are related to health plans, including Medicaid and SCHIP.

Covered transactions include the following actions taken by health care providers:

- Requesting payment for health care from a health plan.
- Sending encounter information to an HMO to report health care provided to enrollees.
- Sending subscriber enrollment information to a health plan to establish or terminate insurance coverage.
- Asking a health plan for information about:
  - The enrollee's eligibility to receive health care under the health plan.
  - Coverage of health care under the plan.
  - Benefits associated with the health plan.
- Asking a health plan about the status of a health claim.
- Requesting a referral certification or authorization for treatment.
- Sending any information to a health plan for the purpose of determining the relative payment responsibilities of the health plan (coordination of benefits).

For example, submitting a claim for payment to Medicaid is a covered transaction. In contrast, sending a prescription to a pharmacy is not a covered transaction because it is not an administrative or financial transaction on the list.

Does the CKF participant perform covered transactions?

Yes **OR** **No**

3. "Electronically" send information in connection with covered transactions

The Privacy Rule only covers health care providers who "electronically" send information in connection with covered transactions. Electronically sending information means using computer technology to send it. Some examples of computer technology include:[15]

- Internet or other Web-based applications
- Private computer networks
- Direct data entry
- Computer diskettes and tapes
- "Faxback" systems
- Telephone voice response systems
- Other computer-based technology

For example, a clinic that sends claims information to Medicaid on a computer diskette is covered under HIPAA because it electronically sends the information. Providers who do not use computer technology are not covered by HIPAA. For example, a doctor who conducts all her financial and administrative activities in paper form is not covered by HIPAA.

HIPAA does not cover every provider who uses computer technology. In order to be covered, the provider must use computer technology *for a specific purpose*—to send information in connection with the covered transactions that were discussed above. For example, a doctor who submits claims for payment to a Medicaid program via the Internet meets this test because he electronically sends information related to a covered transaction. In contrast, a doctor who uses her computer solely to electronically send treatment advice to patients does not meet the test because advising patients is not a covered transaction.

A provider cannot escape being covered by the Privacy Rule by having someone else electronically conduct a covered transaction on their behalf. For example, if a billing firm sends claims for payment to health insurers on behalf of a provider, the provider still meets this last test.

Most health care providers will be covered by the HIPAA Privacy Rule. Under the Administrative Simplification Compliance Act, many health care providers now must submit Medicare claims electronically in order to receive payment. Thus the Act essentially requires

15. For purposes of HIPAA, using computer technology does not include using the telephone or a regular fax machine.

such health care providers to conduct the types of electronic transactions that automatically bring them within the scope of HIPAA.[16]

Does the CKF participant electronically send information related to covered transactions?

Yes **OR** **No**

Key Points about Health Care Providers Covered by HIPAA

- A CKF participant is a covered health care provider under HIPAA only if it answers Yes to *all three* of these questions:
  1. Does the participant provide health care in the normal course of business?
  2. Does the participant have "covered transactions"?
  3. Does the participant electronically send information related to these covered transactions?

(The questions can be answered in any order.)

16. The Administrative Simplification Compliance Act (Public Law No. 107-105, December 27, 2001) prohibits CMS from paying Medicare claims that are not submitted electronically after October 16, 2003, unless the Secretary of HHS grants a waiver from this requirement. It further provides that the Secretary must grant such a waiver if there is no method available for the submission of claims in electronic form or if the entity submitting the claim is a small provider of services or supplies. A "small provider" is one with fewer than 10 full-time equivalent employees. More information on the Administrative Simplification Compliance Act can be found at *http://cms.hhs.gov/providers/edi/*.

PART III
HIPAA'S POTENTIAL IMPACT ON *COVERING KIDS & FAMILIES* STATEWIDE AND LOCAL PROJECT PARTICIPANTS

The rules for sharing health information under the HIPAA Privacy Rule vary greatly depending on the particular circumstances under which information is disclosed. They change depending on who discloses the information, to whom the information is disclosed and the purpose for which the information is disclosed. This guide addresses a few of the more common activities of CKF participants. Once CKF participants have determined whether they are a covered health care provider under HIPAA, they can refer to the appropriate section in this part to learn more about how HIPAA may have an impact on their CKF activities**.** Those who are *not* directly covered by HIPAA should refer to the first section of Part III. Those who *are* covered by HIPAA may want to proceed directly to the second section of Part III. Because several issues apply both to those who are covered and those who are not covered by HIPAA, some of the information appears in both sections.

IMPACT ON CKF PARTICIPANTS WHO ARE NOT COVERED BY THE HIPAA PRIVACY RULE

This section focuses on CKF participants who are *not* directly covered by the Privacy Rule.[17] It describes how HIPAA may affect some of the typical activities of these participants.

As discussed in Part I, HIPAA directly covers only three categories of people and organizations that have access to information related to health care and the payment of health care:

- Health plans
- Health care clearinghouses
- Health care providers who send health information related to covered transactions using computer-based technology.

Covering Kids & Families participants who do not fall within one of these categories are not covered by HIPAA and do not need to follow its detailed rules.

Outreach

Covering Kids & Families participants that are not covered by HIPAA can continue performing many CKF activities without any changes. For example, HIPAA does not change how they can:

- Do general awareness outreach (e.g., education about Medicaid and SCHIP programs).
- Collect information about or from potential applicants.
- Help people in gathering information and filling out their applications.
- Send application information to a Medicaid/SCHIP program.

17. This section does not address governmental agencies that participate in the CKF Initiative.

However, HIPAA will have an impact on CKF activities that involve interacting with Medicaid/SCHIP programs. Some of these activities are discussed in the sections that follow.

Presumptive Eligibility Determinations

Some CKF participants make presumptive eligibility determinations for Medicaid/SCHIP programs. Under these programs, certain health care providers and community-based organizations are qualified to make preliminary determinations that individuals are eligible for Medicaid/SCHIP. Generally, the health care provider or community-based organization must sign a document (for example, an application or an agreement) to become qualified to make presumptive eligibility determinations.

In making presumptive eligibility determinations, the qualified provider or organization obtains income and other eligibility information from the client. After reviewing the information, the provider or organization determines whether the individual is eligible to immediately receive Medicaid or SCHIP benefits on a temporary basis (Medicaid or SCHIP ultimately decides whether the person is eligible for permanent coverage). Technically, preliminary eligibility determinations and permanent enrollment are separate procedures. Even if Medicaid/SCHIP determines that a person is not eligible for permanent enrollment, the program still pays for care received during the period the client was temporarily enrolled by a presumptive eligibility determination.

Under the Privacy Rule, a person or organization that performs activities using client information on behalf of a health plan is classed as a business associate of that health plan. Because making presumptive eligibility determinations requires obtaining and using client information on behalf of Medicaid/SCHIP, those who do this activity are considered "business associates" of the specific program and must sign a business associate contract with it.[18] The business associate contract can be a separate document, but can also be incorporated in other documents (such as an agreement to make presumptive eligibility determinations).

The contract can only permit the business associate to use and disclose information the same way that Medicaid/SCHIP, itself, could use and disclose the information under the Privacy Rule.[19] Other than this limitation, the individual Medicaid/SCHIP programs can decide which activities to include in a business associate contract. They can write the contract narrowly, so that it permits the business associate to perform only one function, such as making presumptive eligibility determinations, or they can write it more broadly and permit the business associate to perform more than one activity. For example, SCHIP could use one business associate contract to authorize a person or organization to both make presumptive eligibility determinations and assist in the permanent application process.[20] Under HIPAA, it is up to the Medicaid/SCHIP

18. A sample business associate contract is included as Appendix E.

19. For example, the business associate contract could not permit the business associate to sell the information that it collects on behalf of the program.

20. Only authorized state Medicaid staff can make eligibility determinations for Medicaid.

program to decide which activities to include in their business associate contracts. State law, however, may limit which activities Medicaid/SCHIP may include in such a contract.

A business associate can only use or disclose health information for the activities that are listed in the business associate contract. For example, if the contract only permits a person or organization to collect information on behalf of the Medicaid program to make presumptive eligibility determinations, the business associate may not use the information collected for other purposes. Should the associate want to use this information for other purposes, authorization to do so must be obtained from the client.

Key Point about Presumptive Eligibility Determinations

- People and organizations that make presumptive eligibility determinations should expect to sign some form of business associate contract with the Medicaid/SCHIP program.

Obtaining Client-Level Information from Medicaid or SCHIP

The HIPAA Privacy Rule has a limited impact on Medicaid/SCHIP programs' ability to disclose client-level information to CKF participants. Medicaid and SCHIP programs have always been required by state law to protect the confidentiality of information about both applicants and people who are formally enrolled in the program.[21] Under these laws, Medicaid and SCHIP generally can release applicant and enrollee information only in two cases: 1) with the permission of the individual, or 2) to persons who are required to follow the same confidentiality requirements of the program. The procedures for complying with these requirements vary depending on the state. Some Medicaid/SCHIP programs continue to use their established procedures. Other programs have changed their procedures for disclosing client-level information in response to the Privacy Rule. Because some of these programs treat application and enrollment information differently under the Rule, this resource guide discusses these types of information separately.

Obtaining Application Information Before Enrollment

A CKF participant might request information about the status of a client's application to ensure that things are proceeding smoothly and that no additional documents are needed. It is not clear whether this application information is covered by HIPAA if the client is not yet enrolled in Medicaid or SCHIP. Due to this uncertainty, CKF participants may encounter any one of a variety of procedures for obtaining this type of data.

21. Federal regulations require state Medicaid and SCHIP programs to have safeguards that restrict the use and disclosure of information concerning people who apply for and receive benefits under these programs. See 42 C.F.R. § 431.300 etc.

The HIPAA Privacy Rule protects information related to "health information," which is defined as including the past, present or future payment for health care. It is an open issue whether the *application* information fits within this definition. Some Medicaid/SCHIP programs take the position that application information is not protected by the HIPAA Privacy Rule because it may never be related to the payment of health care. For instance, a client's application could be rejected and their application information would never be related to payment. Programs that take this position have not changed their procedures for disclosing application information because, in their view, the HIPAA Privacy Rule does not apply to this information.

Other Medicaid/SCHIP programs take the position that application data is covered by HIPAA because it relates to a Medicaid/SCHIP program's decision whether it will pay for the client's health care. These programs have generally put in place new procedures for obtaining application information and require either the client's authorization or a business associate contract to disclose information to CKF participants, depending on the program's perspective on the CKF participant's activities. Some of these Medicaid/SCHIP programs view CKF participants as acting on a client's behalf when they request information to assist the client in the application process. When this is the case, the program requires an authorization form to disclose the information to the CKF participant. As discussed in "Individual Authorization," in Part I of this resource guide, the authorization must meet very specific requirements. Among other things, it must name who can share the information, state with whom the client's information can be shared and what information can be shared and include the client's signature. There is a sample patient authorization form in English and Spanish in Appendix F.

Some Medicaid/SCHIP programs that treat application information as protected health information under HIPAA view CKF participants as assisting their program in processing applications. In this case, the CKF participant is a business associate of the program, and Medicaid/SCHIP will only disclose client-level data to CKF participants who sign a business associate contract. As discussed in Part I of this guide, the requirements for business associate contracts are quite detailed (A sample business associate contract is included as Appendix E). Under the Privacy Rule, a business associate contract can include more than one purpose for sharing information. For example, a Medicaid/SCHIP program can have a business associate contract that authorizes a CKF participant to collect information to make presumptive eligibility determinations *and* to receive information to assist with follow-through on permanent applications. The decision on what activities to include in a business associate contract is largely up to the Medicaid/SCHIP program.

In sum, there is currently no uniform approach to disclosing Medicaid/SCHIP application information. Some programs treat application information as protected health information and others do not. Of those that treat application information as covered by HIPAA, some require the client's authorization to disclose information while others require a business associate contract. Ultimately, HHS will need to resolve this issue.

Key Points about Obtaining Application Information Before Enrollment

Different Medicaid/SCHIP programs use different procedures for disclosing application information. To disclose application information, a Medicaid/SCHIP program may do any of the following:

- Continue to follow its pre-Privacy Rule procedures.
- Require the client's authorization to disclose information.

  or
- Require a CKF participant to sign a business associate contract.

Obtaining Information After Enrollment

Some CKF participants request information about people who are already enrolled in Medicaid/SCHIP so that they can make sure that the client remains enrolled in the program. Client-level data about people who are formally enrolled in Medicaid/SCHIP is information related to payment for health care, and as such is clearly protected under HIPAA. Most Medicaid/SCHIP programs view a CKF participant as acting on a client's behalf when they ask for enrollment information to make sure the client remains enrolled in the program. In this case, the Medicaid/SCHIP program will require the client's authorization (written permission) to share this information with the CKF participant.

Some Medicaid/SCHIP programs view a CKF participant's activities to ensure that clients remain enrolled in a program as being done on behalf of their program. If this is the case, the CKF participant is Medicaid/SCHIP's business associate and is required to sign a business associate contract. As discussed earlier in "Presumptive Eligibility Determinations," Medicaid/SCHIP programs can use a single business associate contract to authorize numerous activities. A sample business associate contract is included in Appendix E.

Medicaid/SCHIP programs have some discretion in how they view activities that CKF participants take to ensure that clients re-enroll. Ensuring re-enrollment can be seen as an activity that is performed on behalf of the client or on behalf of the program. In either case, Medicaid/SCHIP programs will require an authorization or a business associate contract to disclose client-level enrollment data. Which particular document Medicaid/SCHIP requires depends on the program's interpretation of the Privacy Rule and its perception of the CKF participant's activities as being on behalf of the program or on behalf of the client.

Key Points about Obtaining Information After Enrollment

To disclose enrollment information to a CKF participant, Medicaid/SCHIP programs require either:

- The client's authorization to disclose information to the CKF participant
  or
- A signed business associate contract.

Obtaining Group or Aggregate Data

Many CKF participants request group (aggregate) data from Medicaid/SCHIP programs for research or monitoring purposes. For example, a CKF participant might request data on the number of people under 18 who are enrolled in a state Medicaid program by county. How easy it is to obtain this data depends on two factors:

- Whether the information requested is "protected health information" under the Privacy Rule.
- The purpose for requesting the information.

The section that follows first discusses whether group data constitutes protected health information under the Privacy Rule. It then discusses the rules for obtaining protected health information for research and monitoring purposes. Finally, it addresses the issue of whether Freedom of Information Act requests can be used to avoid potential problems under the Privacy Rule.

Does the Group Data Requested Include Protected Health Information?

In order to be protected under the HIPAA Privacy Rule, the information must be information related to health, health care or the payment for health care that can identify the subject of the information. It also has to be created or received by a health provider or plan. Information about enrollment in Medicaid/SCHIP is related to the payment of health care.[22] Furthermore, Medicaid/SCHIP group enrollment data clearly was created by health plans. Therefore, the central issue with respect to requests for Medicaid/SCHIP group enrollment data is whether it includes information that can be used to identify the subject of the information.

If the data includes identifiable information, it is protected health information and is subject to the Privacy Rule. However, if the data has been de-identified it is not protected health information under the Rule and can be disclosed without restrictions.

The easiest method for obtaining group data is to request information that has been de-identified, because it is not protected by the Privacy Rule. Information can be de-identified in two ways.

22. As discussed in "Obtaining Application Information before Enrollment," it is an open issue whether application information is protected health information.

First, if all 18 of the items that the Privacy Rule lists as potentially identifying a person ("identifiers") are removed.[23] Alternatively, if a qualified statistician determines that the risk is very small that the information can be used (alone or in combination with other reasonably available information) by the recipient to identify an individual who is the subject of the information.

Unless otherwise noted, this discussion assumes that the data requested includes only the person's age, enrollment status and the geographic area where the person lives. It also assumes that the CKF participant is not performing these activities at the request of or on behalf of the Medicaid/SCHIP program.

Data that includes enrollee's age and state of residence
Requesting data that includes only enrollment (or eligibility) status, age and state of residence may be one way to obtain group data easily. This type of information is considered to be de-identified because all 18 of the items listed as identifiers in the Privacy Rule have been removed. Medicaid/SCHIP programs can freely disclose data grouped by age and expressed in terms of years (for instance, "18 and younger"). They can also disclose data grouped at the state level. Neither a person's age nor their state of residence is on the list of identifiers. The Privacy Rule does not place any restrictions on Medicaid or SCHIP disclosing information aggregated at this level.

Data that includes the county in which enrollee lives
It may be more difficult to obtain data that includes counties. Counties, towns, ZIP codes and other geographic areas smaller than a state are on the Privacy Rule's list of 18 identifiers.

De-identified county-level information
County-level data can be de-identified by having a qualified statistician determine that the risk is very small that the information can be used (alone or in combination with other reasonably available information) by the recipient to identify an individual who is the subject of the information. Medicaid/SCHIP programs can, but are not required to, de-identify information using this statistical method. The Privacy Rule does not place any restrictions on Medicaid/SCHIP disclosing information that has been de-identified in this manner.

23. A list of the 18 identifiers is in Appendix D.

Key Points about Obtaining De-Identified Group Data

- A data group that only includes the enrollees' enrollment or eligibility status, ages (in years) and state(s) of residence is de-identified information.
- County level data can be de-identified if a qualified statistician determines that the risk is very small that the information can be used (alone or in combination with other reasonably available information) by the recipient to identify an individual who is the subject of the information.
- De-identified data can be freely disclosed and is not subject to the restrictions of the Privacy Rule.
- Medicaid/SCHIP programs may, but are not required to, de-identify data.

Identifiable county-level information

It is possible that county-level data will not be available as de-identified information through some Medicaid/SCHIP programs. Medicaid/SCHIP programs are not required to statistically de-identify information. Furthermore, a statistician may conclude that there is a real risk of identifying individuals from a data set that is based on a sparsely populated geographic area. When this is the case, county-level data constitutes individually identifiable information and is protected by the Privacy Rule. This means that, absent individual authorization, Medicaid/SCHIP programs only can disclose individually identifiable county-level enrollment data for purposes that are expressly permitted in the Privacy Rule. It may be difficult to obtain this individually identifiable group data for research and monitoring purposes.

Rules for Obtaining Protected Health Information for Research and Monitoring Purposes

This section discusses obtaining county-level data that is individually identifiable and therefore is protected health information under the Privacy Rule.[24] Usually, CKF participants request this type of group data for research and monitoring purposes. The Privacy Rule considers these to be distinct activities. The Rule defines "research" as a systematic investigation that is designed to develop knowledge to be applied to groups outside the covered entity.[25] In contrast, monitoring a government program, such as ensuring that a particular program is fulfilling its duties properly, is more similar to a health oversight activity.

It can be difficult to distinguish between these activities. However, the Privacy Rule treats disclosures for generalizable research very differently from disclosures for monitoring the

24. Or other geographic area smaller than a state.

25. One test for research is whether the person conducting the research intends to publish the results of the study.

performance of a particular program. Because the rules in these areas are fairly complex, we discuss research and monitoring activities separately here. The discussion that follows assumes that the information requested is protected health information (for example, enrollment information that is grouped by county), and that the person or organization requesting the information does not obtain the authorization of all the people whose data is requested.[26] Additionally, the discussion assumes that the organization is not performing these activities at the request of or on behalf of Medicaid/SCHIP.[27]

Research

A CKF participant may request Medicaid/SCHIP data for research purposes. For example, they may want to conduct research to determine whether the adoption of a certain enrollment policy leads to increased rates of enrollment. There are two methods for obtaining group enrollment data for research without individual authorization. The method that can be used depends on the information requested.

A researcher can obtain information with a few key identifiers included as a "limited data set." As discussed in Part I of this guide, a limited data set has had all identifiers removed except: town or city, state, ZIP code, dates and other coded information. For example, data on Medicaid enrollees in a particular state grouped by age and ZIP code constitutes a limited data set. The Privacy Rule permits Medicaid/SCHIP programs to disclose a limited data set without individual authorization to researchers who have signed a data use agreement with the program. In the data use agreement, the researchers promise to use the information only for research and that they will not attempt to re-identify the individuals.[28] There are additional content requirements for data use agreements.

The limited data set does not expressly include counties. However, a good argument can be made that a limited data set implicitly includes counties. The limited data set includes cities and towns on the basis that this information does not directly identify individuals. Because counties, which are larger geographic areas, are even less likely to identify individuals, they may be implicitly included in the limited data set. The United States Department of Health and Human Services needs to clarify this issue.

For some research, the information contained in a limited data set is not sufficient. For example, a researcher may want to survey people. In such a project, the researcher needs more data (such as telephone numbers) than is permitted to be disclosed in a limited data set. Researchers who request this level of information must have their research project approved by an Institutional Review Board (IRB) or a Privacy Board. Generally, researchers must either be affiliated with an

26. Covered health providers and plans are permitted to disclose protected health information if they have the authorization (written permission) of all the people whose information is included in the set of data. This procedure generally is not practical for disclosing group data.

27. Any CKF participant who is performing these activities at the request of or on behalf of Medicaid/SCHIP would be a business associate of the Medicaid/SCHIP program and would be subject to different rules.

28. Unfortunately, HHS has not yet developed a model data use agreement.

institution (such as a university) that has an IRB or must establish a special privacy board. Many CKF participants will be unable to meet this requirement.

Monitoring a program
Covering Kids & Families participants may request group data in order to monitor the performance of their state's Medicaid/SCHIP program. The Privacy Rule does not permit Medicaid/SCHIP programs to disclose protected health information to private parties for this purpose without individual authorization. The Rule permits disclosures for "health oversight," which can include monitoring. However, this type of disclosure can be made only to governmental agencies (or their contractors) authorized by law to oversee the health care system. It is unlikely that a community- or faith-based organization would qualify as a health oversight agency. It is therefore unlikely that Medicaid/SCHIP programs will provide CKF participants with data for monitoring purposes.

Key Points about Obtaining Individually Identifiable Group Data for Research and Monitoring Without Individual Authorization

These points only apply where the group data requested contains individually identifiable information (i.e., it contains at least one of the 18 listed identifiers, such as the enrollees' counties, and it has not been de-identified by a statistician).

Research

- Researchers can obtain general group data if they request a limited data set that includes only the following identifiers: city or town, state, ZIP code and dates.
- County-level data may be implicitly included in the data that may be disclosed in a limited data set.
- A researcher must sign a data use agreement to obtain a limited data set without the authorization of all of the people whose information is included in the data set.
- Data that includes more identifiers (such as names or telephone numbers) may be disclosed only to researchers who have the approval of an IRB or Privacy Board.

Monitoring

- A Medicaid/SCHIP program cannot disclose enrollment data for "monitoring" purposes unless the recipient is a governmental agency (or a contractor of such an agency) that is responsible for overseeing the health care system.

HIPAA and Freedom of Information Act Requests
Covering Kids & Families participants have asked whether submitting requests for group data under the Freedom of Information Act (FOIA) would avoid these potential problems with

obtaining data under HIPAA. There is no simple answer to this question. It depends on the FOIA laws of the particular state where the Medicaid/SCHIP program is located.[29]

The federal FOIA applies only to federal agencies. The federal law does not control requests to Medicaid /SCHIP programs because they are state, not federal, agencies. Rather, state law governs data requests to Medicaid/SCHIP programs. Virtually every state has an FOIA law. Some of these state laws are very similar to the federal FOIA; other states have adopted FOIA laws that are very different from the federal FOIA. As it is impossible to address all these variations, this guide discusses some general principles that may be used in analyzing state FOIAs.

The Privacy Rule permits disclosures that are required by other laws. Because state FOIAs require disclosure of information held by the government, such disclosures generally appear to be permitted by the Privacy Rule. Every state FOIA, however, has some exemptions which permit the government to withhold information. The critical question is whether a request for group data falls within one of these exemptions.

For example, some state FOIA laws include an exemption that affords a state agency discretion not to disclose medical or other information where such disclosure would constitute a clearly unwarranted invasion of personal privacy. The United States Department of Health and Human Services takes the position that when a state has this type of law the disclosure of such records is not "required by law," and therefore is not permissible under HIPAA.[30] It is possible that a Medicaid/SCHIP program would adopt a similar position and refuse to disclose group data that includes "protected health information" under HIPAA. There are a number of potential challenges to the position that all protected health information should be withheld under this exemption. For example, in deciding whether to disclose information under this exemption, an agency is supposed to balance the individual's right to privacy against the public's right to disclosure.

States with different exemptions to their FOIA laws may respond differently to a request for group data. For example, the Texas Attorney General determined that the HIPAA Privacy Rule does not change how the state will respond to requests for information under the Texas Public Information Act (PIA).[31] Therefore, if a Texas Medicaid/SCHIP agency could disclose group data pursuant to a PIA request prior to the Privacy Rule, it will be able to continue to do so.

---

29. Although the states have given these statutes various names (such as FOIA, Open Records Act, and Right to Know Act) this guide refers to them collectively as FOIA.

30. Office for Civil Rights, *Frequently Asked Questions*, response to "How does the HIPAA Privacy Rule relate to state public record laws?" Available at http://www.hhs.gov/ocr/hipaa/ under the category "Disclosures Required by Law."

31. Texas Attorney General Open Records Decision No. 681 (February 13, 2004), available at: http://www.oag.state.tx.us/opinions/ord/ord-681.pdf. The Texas Public Information Act exempts from disclosure "information considered to be confidential by law, either constitutional, statutory, or by judicial decision." Tex. Govt. Code § 522.101. The Texas Attorney General reasoned that the Privacy Rule does not make confidential information that is required to be disclosed by law. Therefore, state agencies will continue to evaluate requests for

Footnote continued on the following page.

Key Points about FOIA Requests

- Whether a CKF participant can obtain information under a FOIA request depends on a number of factors including the state's FOIA, its exemptions and how the state program interprets the law.
- Even if a state Medicaid/SCHIP program initially denies a request for group data, there may be good legal grounds for challenging the denial.

IMPACT ON CKF PARTICIPANTS WHO *ARE* COVERED HEALTH CARE PROVIDERS UNDER THE PRIVACY RULE

This section focuses on CKF participants who *are* covered health care providers under the Privacy Rule and how some of their typical CKF-related activities may be affected by HIPAA. (Those who are *not* directly covered by HIPAA will find information in the previous section specifically addressing HIPAA's impact on CKF participants who are *not* covered entities.) For those who *are* covered by HIPAA, the Privacy Rule will have an impact on many, but not all, of their CKF-related activities. As the rules vary with the activity, different activities are discussed separately.

Outreach

Education

HIPAA should not affect general outreach such as general education about Medicaid and SCHIP. Informing people about the existence of these programs and educating them about the programs' general requirements generally do not involve using or sharing protected health information.

Identifying Potential Applicants

A covered health care provider may use information about patients to identify those who might be eligible for Medicaid/SCHIP programs. HIPAA permits covered providers to use health information for payment activities without the authorization of the patient. Payment activities include those that are done to obtain payment for care. Because identifying a source of payment for care is a payment activity, covered providers may continue to do this activity without obtaining the patient's authorization.

Presumptive Eligibility Determinations

Some CKF participants make presumptive eligibility determinations for Medicaid/SCHIP programs. Under these programs, certain health care providers and community-based organizations are qualified to make preliminary determinations that individuals are eligible for Medicaid/SCHIP. Generally, the health care provider or community-based organization must

---

information under the PIA solely on the basis of whether there is a law (other than the Privacy Rule) that makes the information confidential.

sign a document (for example, an application or an agreement) to become qualified to make presumptive eligibility determinations.

In making presumptive eligibility determinations, the qualified provider or organization obtains income and other eligibility information from the client. After reviewing the information, the provider or organization determines whether the individual is eligible to immediately receive Medicaid or SCHIP benefits on a temporary basis (Medicaid or SCHIP ultimately decides whether the person is eligible for permanent coverage). Technically, preliminary eligibility determinations and permanent enrollment are separate procedures. Even if Medicaid/SCHIP determines that a person is not eligible for permanent enrollment, the program still pays for care received during the period the client was temporarily enrolled by a presumptive eligibility determination.

Key Point about Presumptive Eligibility Determinations

- *Covering Kids & Families* participants that make presumptive eligibility determinations should expect to sign a Business Associate Contract with the Medicaid/SCHIP program.

Under the Privacy Rule, people and organizations who perform activities using client information on behalf of a health plan are classed as business associates of that health plan. Because making presumptive eligibility determinations requires obtaining and using information on behalf of Medicaid/SCHIP, those who do these activities are business associates of that Medicaid/SCHIP program and must sign a business associate contract with it.[32] The business associate contract can be a separate document, but it can also be incorporated in other documents (such as an agreement to make presumptive eligibility determinations).

The contract can only permit a business associate to use and disclose information in the same way that Medicaid/SCHIP, itself, could use and disclose the information under the Privacy Rule.[33] Other than this limitation, the Medicaid/SCHIP program can decide which activities to include in a business associate contract. The program can write the contract narrowly, so that it only permits a business associate to perform one function, such as making presumptive eligibility determinations, or they can write it more broadly and permit the business associate to perform more than one activity. For example, SCHIP can use one business associate contract to authorize a business associate to both make presumptive eligibility determinations and assist in the

32. A sample business associate contract is included in Appendix E.

33. For example, the business associate contract could not permit the business associate to sell the information that it collects on behalf of the program.

permanent application process.[34] Under HIPAA, it is up to the Medicaid/SCHIP program to decide which activities to include in their business associate contracts. State law, however, may limit which activities Medicaid/SCHIP may include in such a contract.

A business associate can only use or disclose health information for the activities that are listed in the business associate contract. For example, if the contract only permits the business associate to collect information on behalf of the Medicaid program to make presumptive eligibility determinations, the business associate may not use that information for other purposes. Should the associate want to use this information for other purposes, authorization to do so must be obtained from the client.

Application Assistance

When a covered health care provider asks a Medicaid/SCHIP program for information about a client's application there are two sides of the process under the Privacy Rule. First, the provider discloses the patient's information in order to ask the question. Second, the Medicaid/SCHIP program discloses the applicant's information in response to the inquiry. The following sections discuss these two sides of the process as "requesting application information" and "obtaining application information."

Requesting Application Information Before Enrollment

A covered health care provider might wonder whether they can use information that a patient gave to them to ask Medicaid/SCHIP follow-up questions about the status of the patient's application for enrollment. Information a patient gives a health care provider to help the provider obtain payment for care is protected by the Privacy Rule.[35] The Privacy Rule permits providers to disclose protected health information without the individual's authorization for the payment activities of others. Because Medicaid/SCHIP actions to determine a person's eligibility are considered payment activities, a covered provider does not need the patient's authorization to ask this kind of follow-up question.

Obtaining Application Information

From the perspective of the Medicaid/SCHIP program, the issue is whether the HIPAA Privacy Rule impacts their ability to disclose information to a CKF participant. Medicaid and SCHIP programs have always been required by state law to protect the confidentiality of information about applicants and people who are enrolled in the program.[36] Under these laws, Medicaid and SCHIP generally can release applicant and enrollee information only in two cases: 1) with the permission of the individual, or 2) to persons who are required to follow the same confidentiality requirements of the program. The procedures for complying with these requirements vary depending on the state. Some Medicaid/SCHIP programs have changed their procedures for

34. Only authorized state Medicaid staff can make an eligibility determination for Medicaid.

35. A covered provider who received this information only in their capacity to make preliminary eligibility determinations is limited by the terms of their business associate contract in how they can use and disclose the information. See the previous discussion," Presumptive Eligibility Determinations."

36. Federal regulations require state Medicaid and SCHIP programs to have safeguards that restrict the use and disclosure of information concerning people who apply for and receive benefits under these programs. See 42 C.F.R. § 431.300 etc.

obtaining client-level information in response to the Privacy Rule. Others have not. Because some programs treat application and enrollment information differently under the Privacy Rule, this guide discusses these types of information separately.

Obtaining Application Information Before Enrollment

A CKF participant might request information about the status of a client's application to ensure that things are proceeding smoothly and that no additional documents are needed. It is not clear whether this application information is covered by HIPAA if the client is not yet enrolled in Medicaid or SCHIP. Due to this uncertainty, CKF participants may encounter any one of a variety of procedures for obtaining this type of data.

The HIPAA Privacy Rule protects information related to "health information" which is defined as including the past, present or future payment for health care. It is an open issue whether the *application* information fits within this definition. Some Medicaid/SCHIP programs take the position that application information is not protected by the HIPAA Privacy Rule because it may never be related to the payment of health care. For instance, a client's application could be rejected and their application information would never be related to payment. Programs that take this position have not changed their procedures for disclosing application information because, in their view, the HIPAA Privacy Rule does not apply to this information.

Other Medicaid/SCHIP programs take the position that application data is covered by HIPAA because it relates to a Medicaid/SCHIP program's decision whether or not it will pay for the client's health care. These programs have generally put in place new procedures for obtaining application information and require either the client's authorization or a business associate contract to disclose information to CKF participants, depending on the program's perspective on the CKF participant's activities. Some of these Medicaid/SCHIP programs view CKF participants as acting on a client's behalf when they request information to assist the client in the application process. When this is the case, the program requires an authorization form to disclose the information to the CKF participant. As discussed in Part I of this guide, the authorization must meet very specific requirements. Among other things, it must name who can share the information, state with whom the client's information can be shared, clarify what information can be shared, and include the client's signature. There is a sample patient authorization form in English and Spanish in Appendix F.

Some Medicaid/SCHIP programs that treat application information as protected health information under HIPAA view CKF participants as assisting their program in processing applications. In this case, the CKF participant is a business associate of the program, and Medicaid/SCHIP will only disclose client-level data to CKF participants who sign a business associate contract. As discussed in Part I of this guide, the requirements for business associate contracts are quite detailed. (A sample business associate contract is included in Appendix E. Under the Privacy Rule, a business associate contract can include more than one purpose for sharing information. For example, a Medicaid/SCHIP program can have a business associate contract that authorizes a CKF participant to collect information to make presumptive eligibility determinations *and* to receive information to assist with follow-through on permanent applications. The decision on what activities to include in a business associate contract is largely up to the Medicaid/SCHIP program. Currently, there is no uniform approach to disclosing

Medicaid/SCHIP application information. Some programs treat application information as protected health information and others do not. Of those that treat application information as covered by HIPAA, some require the client's authorization to disclose information while others require a business associate contract. Ultimately, HHS will need to resolve this issue.

Key Points about Obtaining Application Information Before Enrollment

Different Medicaid/SCHIP programs use various procedures for disclosing application information. To disclose application information, a Medicaid/SCHIP program may do any of the following:

- Continue to follow its pre-Privacy Rule procedures.
- Require the client's authorization to disclose information.

  or
- Require a CKF participant to sign a business associate contract.

Verifying Enrollment

A covered provider may want to verify that a patient is enrolled in a Medicaid/SCHIP program. To the extent that the provider does so in relation to obtaining payment for health care, this inquiry would be considered to be a "payment" activity under HIPAA. In this case, the covered provider can make this inquiry without the authorization of the patient. Similarly, the Privacy Rule allows the Medicaid/SCHIP program to release information about whether a person is enrolled without the client's authorization for payment purposes.

Obtaining Information After Enrollment

Some CKF participants request information about people who are already enrolled in Medicaid/SCHIP so that they can make sure that the client remains enrolled in the program. Client-level data about people who are formally enrolled in Medicaid/SCHIP is information related to payment for health care, and as such is clearly protected under HIPAA. Most Medicaid/SCHIP programs view a CKF participant as acting on a client's behalf when they ask for enrollment information to make sure the client remains enrolled in the program. In this case, the Medicaid/SCHIP program requires the client's authorization (written permission) to share this information with the CKF participant.

Some Medicaid/SCHIP programs view a CKF participant's activities to ensure that clients remain enrolled in a program as being done on behalf of their program. If this is the case, the CKF participant is Medicaid/SCHIP's business associate and is required to sign a business associate contract. As discussed earlier in "Presumptive Eligibility Determinations." Medicaid/SCHIP programs can use a single business associate contract to authorize numerous activities. A sample business associate contract is included as Appendix E.
Medicaid/SCHIP programs have some discretion in how they view activities that CKF participants take to ensure that clients re-enroll. Ensuring re-enrollment can be seen as an activity

that is done on behalf of the client or on behalf of the program. In either case, Medicaid/SCHIP programs require an authorization or a business associate contract to disclose client-level enrollment data. Which particular document Medicaid/SCHIP requires depends on the program's interpretation of the Privacy Rule and its perception of the CKF participant's activities as being on behalf of the program or on behalf of the client.

Key Points about Obtaining Information After Enrollment

To disclose enrollment information to a CKF participant, Medicaid/SCHIP programs require either:

- The client's authorization to disclose information to the participant
  or
- A business associate contract signed by the CKF participant.

Obtaining Group or Aggregate Data

Many CKF participants request group (aggregate) data from Medicaid/SCHIP programs for research or monitoring purposes. For example, a CKF participant might request data on the number of people under 18 who are enrolled in a state Medicaid program by county. How easy it is to obtain this data depends on two factors:

- Whether the information requested is "protected health information" under the Privacy Rule.
- The purpose for requesting the information.

The section of the guide that follows first discusses whether group data constitutes protected health information under the Privacy Rule. It then discusses the rules for obtaining protected health information for research and monitoring purposes. Finally, it addresses the issue of whether Freedom of Information Act requests can be used to avoid potential problems under the Privacy Rule.

Does the Group Data Requested Include Protected Health Information?

In order to be protected under the HIPAA Privacy Rule, the information must be information related to health, health care or the payment for health care that can identify the subject of the information. It also has to be created or received by a health provider or plan. Information about enrollment in Medicaid/SCHIP is related to the payment of health care.[37] Furthermore, Medicaid/SCHIP group enrollment data clearly was created by health plans. Therefore, the central issue with respect to requests for Medicaid/SCHIP group enrollment data is whether it includes information that can be used to identify the subject of the information.

37. As discussed in "Obtaining Application Information before Enrollment," it is an open issue whether application information is protected health information.

If the data includes identifiable information, it is protected health information and is subject to the Privacy Rule. However, if the data has been de-identified it is not protected health information under the Rule and can be disclosed without restrictions.

The easiest method for obtaining group data is to request information that has been de-identified, because it is not protected by the Privacy Rule**.** Information can be de-identified in two ways. First, if all 18 of the items that the Privacy Rule lists as potentially identifying a person ("identifiers") are removed.[38] Alternatively, if a qualified statistician determines that the risk is very small that the information can be used (alone or in combination with other reasonably available information) by the recipient to identify an individual who is the subject of the information.

Unless otherwise noted, this discussion assumes that the data requested includes only the person's age, enrollment status and the geographic area where the person lives. It also assumes that the CKF participant is not performing these activities at the request of or on behalf of the Medicaid/SCHIP program.

Data that includes enrollee's age and state of residence
Requesting data that includes only enrollment (or eligibility) status, age and state of residence may be one way to obtain group data easily. This type of information is considered to be de-identified because all 18 of the items listed as identifiers in the Privacy Rule have been removed. Medicaid/SCHIP programs can freely disclose data grouped by age and expressed in terms of years (for instance, "18 and younger"). They can also disclose data grouped at the state level. Neither a person's age nor their state of residence is on the list of identifiers. The Privacy Rule does not place any restrictions on Medicaid/SCHIP disclosing information aggregated at this level.

Data that includes the county in which enrollee lives
It may be more difficult to obtain data that includes counties. Counties, towns, ZIP codes and other geographic areas smaller than a state are on the Privacy Rule's list of 18 identifiers.

De-identified county-level information
County-level data can be de-identified by having a qualified statistician determine that the risk is very small that the information can be used (alone or in combination with other reasonably available information) by the recipient to identify an individual who is the subject of the information. Medicaid/SCHIP programs can, but are not required to, de-identify information using this statistical method. The Privacy Rule does not place any restrictions on Medicaid/SCHIP disclosing information that has been de-identified in this manner.

38. A list of the 18 identifiers is in Appendix D.

Key Points about Obtaining De-Identified Group Data

- A data group that only includes the enrollees' enrollment or eligibility status, ages (in years) and state(s) of residence is de-identified information.
- County-level data can be de-identified if a qualified statistician determines that the risk is very small that the information can be used (alone or in combination with other reasonably available information) by the recipient to identify an individual who is the subject of the information.
- De-identified data can be freely disclosed and is not subject to the restrictions of the Privacy Rule.
- Medicaid/SCHIP programs may, but are not required to, de-identify data.

Identifiable county-level information

It is possible that county-level data will not be available as "de-identified" information through some Medicaid/SCHIP programs. Medicaid/SCHIP programs are not required to statistically de-identify information. Furthermore, a statistician may conclude that there is a real risk of identifying individuals from a data set that is based on a sparsely populated geographic area. When this is the case, county-level data is individually identifiable information and is protected by the Privacy Rule. This means that, absent individual authorization, Medicaid/SCHIP programs only can disclose individually identifiable county-level enrollment data for purposes that are expressly permitted in the Privacy Rule. It may be difficult to obtain this individually identifiable group data for research and monitoring purposes.

Rules for Obtaining Protected Health Information for Research and Monitoring Purposes

This section discusses obtaining county-level data that is individually identifiable and therefore is protected health information under the Privacy Rule. Usually, CKF participants request this type of group data for research and monitoring purposes.[39] The Privacy Rule considers these to be distinct activities. The Rule defines "research" as a systematic investigation that is designed to develop knowledge to be applied to groups outside the covered entity.[40] In contrast, monitoring a government program, such as ensuring that a particular program is fulfilling its duties properly, is more similar to a health oversight activity,.

It can be difficult to distinguish between these activities. However, the Privacy Rule treats disclosures for generalizable research very differently from disclosures for monitoring the

39. Or other geographic area smaller than a state.

40. One test for research is whether the person conducting the research intends to publish the results of the study.

performance of a particular program. Because the rules in these areas are fairly complex, we discuss research and monitoring activities separately here. The discussion that follows assumes that the information requested is protected health information (for example, enrollment information that is grouped by county), and that the person or organization requesting the information does not obtain the authorization of all the people whose data is requested.[41] Additionally, the discussion assumes that the organization is not performing these activities at the request of or on behalf of Medicaid/SCHIP.[42]

Research

A CKF participant may request Medicaid/SCHIP data for research purposes. For example, they may want to conduct research to determine whether the adoption of a certain enrollment policy leads to increased rates of enrollment. There are two methods for obtaining group enrollment data for research without individual authorization. Which method can be used depends on the kind of information being requested.

A researcher can obtain information with a few key identifiers included as a "limited data set." As discussed in Part I of this guide, a limited data set has had all identifiers removed except: town or city, state, ZIP code, dates and other coded information. For example, data on Medicaid enrollees in a particular state grouped by age and ZIP code constitutes a limited data set. The Privacy Rule permits Medicaid/SCHIP programs to disclose a limited data set without individual authorization to researchers who have signed a data use agreement with the program. In the data use agreement, the researchers promise to use the information only for research and that they will not attempt to re-identify the individuals.[43] There are additional content requirements for data use agreements.

The limited data set does not expressly include counties. However, a good argument can be made that a limited data set implicitly includes counties. The limited data set includes cities and towns on the basis that this information does not directly identify individuals. Because counties, which are larger geographic areas, are even less likely to identify individuals, they may be implicitly included in the limited data set. The United States Department of Health and Human Services needs to clarify this issue.

For some research, the information contained in a limited data set is not sufficient. For example, a researcher may want to survey people. In such a project, the researcher needs more data (such as telephone numbers) than is permitted to be disclosed in a limited data set. Researchers who request this level of information must have their research project approved by an Institutional Review Board (IRB) or a privacy board. Generally, researchers must either be affiliated with an

41. Covered health providers and plans are permitted to disclose protected health information if they have the authorization (written permission) of all the people whose information is included in the set of data. This procedure generally is not practical for disclosing group data.

42. Any CKF participant conducting these activities at the request of or on behalf of Medicaid/SCHIP would be a business associate of the Medicaid/SCHIP program and would be subject to different rules.

43. Unfortunately, HHS has not yet developed a model data use agreement.

institution (such as a university) that has an IRB or must establish a privacy board. Many CKF participants will be unable to meet this requirement.

Monitoring a program

Covering Kids & Families participants may request group data in order to monitor the performance of their state's Medicaid/SCHIP program. The Privacy Rule does not permit Medicaid/SCHIP programs to disclose protected health information to private parties for this purpose without individual authorization. The Rule permits disclosures for "health oversight," which can include monitoring. However, this type of disclosure can be made only to governmental agencies (or their contractors) authorized by law to oversee the health care system. It is unlikely that a community- or faith-based organization would qualify as a health oversight agency. It is therefore unlikely that Medicaid/SCHIP programs will provide CKF participants with data for monitoring purposes.

Key Points about Obtaining Individually Identifiable Group Data for Research and Monitoring Without Individual Authorization

These points only apply where the group data requested contains individually identifiable information (i.e., it contains at least one of the 18 listed identifiers, such as the enrollees' county, and it has not been de-identified by a statistician).

Research

- Researchers can obtain general group data if they request a limited data set that includes only the following identifiers: city or town, state, ZIP code and dates.
- County-level data may be implicitly included in the data that may be disclosed in a limited data set.
- A researcher must sign a data use agreement to obtain a limited data set without the authorization of all of the people whose information is included in the data set.
- Data that includes more identifiers (such as names or telephone numbers) may be disclosed only to researchers who have the approval of an IRB or Privacy Board.

Monitoring

- A Medicaid/SCHIP program cannot disclose enrollment data for "monitoring" purposes unless the recipient is a governmental agency (or a contractor of such an agency) that is responsible for overseeing the health care system.

HIPAA and Freedom of Information Act Requests

Covering Kids & Families participants have asked whether submitting requests for group data under the Freedom of Information Act (FOIA) would avoid these potential problems with obtaining data under HIPAA. There is no simple answer to this question. It depends on the FOIA laws of the particular state where the Medicaid/SCHIP program is located.[44]

The federal FOIA applies only to federal agencies. The federal law does not control requests to Medicaid /SCHIP programs because they are state, not federal, agencies. Rather, state law governs data requests to Medicaid/SCHIP programs. Virtually every state has a FOIA law. Some of these state laws are very similar to the federal FOIA; other states have adopted FOIA laws that are very different from the federal FOIA. As it is impossible to address all these variations, this guide discusses some general principles that may be used in analyzing state FOIAs.

The Privacy Rule permits disclosures that are required by other laws. Because state FOIAs require disclosure of information held by the government, such disclosures generally appear to be permitted by the Privacy Rule. Every state FOIA, however, has some exemptions that permit the government to withhold information. The critical question is whether a request for group data falls within one of these exemptions.

For example, some state FOIA laws include an exemption that affords a state agency discretion not to disclose medical or other information where such disclosure would constitute a clearly unwarranted invasion of personal privacy. The United States Department of Health and Human Services takes the position that when a state has this type of law the disclosure of such records is not "required by law," and therefore is not permissible under HIPAA.[45] It is possible that a Medicaid/SCHIP program would adopt a similar position and refuse to disclose group data that includes "protected health information" under HIPAA. There are a number of potential challenges to the position that all protected health information should be withheld under this exemption. For example, in deciding whether to disclose information under this exemption, an agency is supposed to balance the individual's right to privacy against the public's right to disclosure.

States with different exemptions to their FOIA laws may respond differently to a request for group data. For example, the Texas Attorney General determined that the HIPAA Privacy Rule does not change how the state will respond to requests for information under the Texas Public Information Act (PIA).[46] Therefore, if a Texas Medicaid/SCHIP agency could disclose group data pursuant to a PIA request prior to the Privacy Rule, it will be able to continue to do so.

---

44. Although the states have given these statutes various names (such as FOIA, Open Records Act, and Right to Know Act) this guide refers to them collectively as FOIA.

45. Office for Civil Rights, *Frequently Asked Questions*, response to "How does the HIPAA Privacy Rule relate to state public record laws?" Available at http://www.hhs.gov/ocr/hipaa/ under the category "Disclosures Required by Law."

46. Texas Attorney General Open Records Decision No. 681 (February 13, 2004), available at: http://www.oag.state.tx.us/opinions/ord/ord-681.pdf. The Texas Public Information Act exempts from disclosure "information considered to be confidential by law, either constitutional, statutory, or by judicial decision." Tex. Govt. Code § 522.101. The Texas Attorney General reasoned that the Privacy Rule does not make confidential information that is required to be disclosed by law. Therefore, state agencies will continue to evaluate requests for

Footnote continued on the following page.

Key Points about FOIA Requests

- Whether a CKF participant can obtain information under a FOIA request depends on a number of factors including the state's FOIA, its exemptions and how the state program interprets the law.
- Even if a state Medicaid/SCHIP program initially denies a request for group data, there may be good legal grounds for challenging the denial.

CONCLUSION

The HIPAA Privacy Rule creates new rules for how covered health care providers and health plans such as Medicaid and SCHIP can use and disclose health information. These rules are broad enough to cover client-level data as well as much group data. Overall, HIPAA should not prevent CKF participants from undertaking many of their important CKF related activities. They may be required, however, to follow different procedures for obtaining information.

Medicaid and SCHIP programs will still be able to share client level information with CKF participants. In many cases, however, the Privacy Rule will require the programs to use different procedures for sharing this information. It is likely that many Medicaid and SCHIP programs will begin to require either the client's authorization or a business associate contract in order to share client level information.

It may be more difficult to obtain group data, particularly for monitoring purposes. The ease of obtaining group data will depend on the level of detail of the information requested. Participants should be able to obtain very general group data aggregated at the state level without any changes, since this information is not protected by the Privacy Rule. Participants may have a more difficult time obtaining group data this is aggregated at the county level. Medicaid/SCHIP programs can freely disclose this data if they have de-identified it using approved statistical methods. When Medicaid/SCHIP programs are either unable or unwilling to conduct such de-identification, the programs are required to follow the Privacy Rule's detailed requirements for disclosure. In this case, participants might encounter problems in obtaining identifiable group data for research and monitoring. Due to HIPAA's limits on how identifiable information may be disclosed to others, Medicaid and SCHIP programs may be unable to provide certain types of group data to CKF participants for monitoring purposes without the authorization of all the individuals in the data group.

---

information under the PIA solely on the basis of whether there is a law (other than the Privacy Rule) that makes the information confidential.

APPENDIX
LIST OF CONTENTS

Because *Covering Kids & Families* participants serve as a resource, not only to their clients but also to their local agencies, we are providing some additional resources that may be helpful in understanding HIPAA and making some of the forms that are required by the HIPAA Privacy Rule more user-friendly.

We have listed the resources below and explained why we think they may be useful. The actual documents follow this list.

Appendix A **Additional Requirements of the HIPAA Privacy Rule**
In addition to the restrictions that HIPAA places on using and disclosing health information, the Privacy Rule creates a number of other duties and rights. This is a brief summary of these additional requirements.

Appendix B **Summary of All Administrative Simplification Rules**
The Privacy Rule is only one of a number of sets of rules that are intended to govern the computerized health information system that is being developed under HIPAA's Administrative Simplification Provisions. This is a brief summary of the existing and planned Administrative Simplification Rules.

Appendix C **General HIPAA Privacy Resources**
A list of official resources for obtaining additional information about HIPAA.

Appendix D **HIPAA Identifiers**
HIPAA protects only individually identifiable information that is related to health, health care or payment for health care. This appendix lists the items ("identifiers") that could be used to identify the person who is the subject of the information. To de-identify data, a health plan or provider is required to remove all of these identifiers. Alternatively, a plan or provider could keep some of these identifiers in the data set if it has a statistician determine that there is only a small risk that the persons in the data set could be identified.

Appendix E **Model Business Associate Contract**
Persons or organizations covered by HIPAA need to have a contract or a memorandum of understanding with their "business associates," people who use health information to act on behalf of the covered entity. In response to frequent requests from the public, HHS published this sample business associate contract.

Appendix F **Authorization Forms**
There are times when persons and organizations covered by HIPAA must get the patient's or client's written permission (authorization) to use or share their health information with others. We have included MassHealth's version of an authorization form as a sample. It has all of the required elements and is easy to read. We give both the English and Spanish versions.

Notice of Privacy Practices: Every person or organization that is covered by HIPAA must provide a notice to their clients or patients explaining their privacy practices under HIPAA. These notices must be written in plain language and must explain not only the duties of the covered entity but also the rights of the person who is the subject of the information.

Appendix G -1 **Plain Language Principles and Thesaurus for Making HIPAA Privacy Notices More Readable**
Published by the Office of Civil Rights, HHS, this document explains how to make notices of privacy practices more consumer-friendly and gives a list of terms that can be used to explain HIPAA in plain language.

Examples of Notices of Privacy Practices: We have provided some examples of notices of privacy practices currently being used by state Medicaid departments. Below, we note the elements of each notice that we think are particularly effective.

Appendix G-2 **New York**
We included this notice because it is specifically tailored to show the interaction of HIPAA and state law. It is much shorter than some of the other notices because New York state law prohibits using and sharing information in many cases where HIPAA would allow it. This approach is consistent with HIPAA's requirement that if a use or disclosure permitted by HIPAA is prohibited or materially restricted by another law, the privacy notice must reflect the law that is more stringent.

Appendix G-3 **New Mexico**
New Mexico uses what is called a "layered notice." This format has a cover page that summarizes the major points of HIPAA. It then includes a more detailed description in the following pages. HHS encourages the use of this consumer-friendly style.

Appendix G-4 **Alabama**
Alabama's notice is written in language that is especially easy to read. It also highlights the fact that the document is important in order to make sure that people actually read it.

Appendix G-5 **Wisconsin**
Like many states, Wisconsin demonstrates a sense of cultural sensitivity by making its notice available in a number of different languages. Wisconsin's notice also stands out because it contains specific details on how patients can use their rights, such as getting a copy of their medical information for themselves. Including these details goes beyond the minimum required by HIPAA.

APPENDIX A
ADDITIONAL REQUIREMENTS OF THE HIPAA PRIVACY RULE

HIPAA creates a detailed framework that addresses a number of different aspects of protecting health information. As discussed in Part I of the resource guide, HIPAA establishes rules on how covered health care providers and health plans can use and share health information. In addition, the HIPAA Privacy Rule creates:

- Rights for patients with respect to their own health information.
- Administrative duties for covered health care providers and health plans.
- Penalties for violations of the Rule (found in the Enforcement Standards).

The HIPAA Privacy Rule is very detailed in each of these areas.

Duties of Covered Health Care Providers and Health Plans

The HIPAA Privacy Rule also places a number of duties on those covered by the rule. Some of these duties are tied to the rights that people have in their health information; others are more administrative in nature.

Duties Related to People's Rights

HIPAA gives people a number of rights with respect to their health information. It also requires covered plans and providers to honor those rights. This rule can be thought of as two sides of the same coin, with people's rights on one side of the coin and the related duties of covered providers and plans on the flip side. Under HIPAA, people have the right to:

- **A notice of privacy practices**. Health care providers and health plans are required to give a copy of their notice of privacy practices to all their patients or clients. This notice is supposed to tell people, in plain language, how the health care provider or plan uses and discloses their health information. It is also supposed to explain, in general terms, the rights that people have to their own health information. Plain-language principles for making notices readable are contained in Appendix G-1. Some sample notices of privacy practices are contained in Appendixes G-2 through G-5.
- **See, copy and correct their health information**. When a person asks, a health care provider or health plan must let that person review their health information. The person also has a right to get a copy of the information. The provider can charge a reasonable fee for providing the copy. If the person believes that their health information is inaccurate or incomplete, they can ask the provider or plan to correct this information by adding new information. There are times, however, when a person's request can be denied.
- **Obtain a list of disclosures**. An individual has the right to get a list of when and to whom their health information has been disclosed. This right is somewhat more limited than might at first appear. The right only applies to health information that has been "disclosed" (i.e., shared with someone who is not part of the health care provider or health plan). It does not apply when health information has been "used" internally. For example, a patient does not have the right to see a list of all hospital employees who reviewed their medical record, because an employee's review is a "use," not a "disclosure."

- **Request restrictions on how their health information is used and shared for treatment, payment and health care operations activities.** A person has the right to ask health care providers and plans to limit how their health information is used and disclosed for treatment, payment and health care operations. People with sensitive medical conditions such as mental health problems or sexually transmitted diseases might be most inclined to use this right. Note that it is only a right to ask—the provider or plan does not have to say yes to the request.
- **Direct that they be contacted only in a certain manner or place.** A patient has the right to ask a provider to communicate with them by certain means or at certain locations. If the request is reasonable, the provider must accommodate it. For example, a patient might ask a doctor not to leave a message on his home voice mail.

Who Has Rights with Respect to Minors' Health Information?

Most of the time the parent is the one who has these rights with respect to their child's health information.

If a minor is able to consent to health care under state law without their parent's consent, then the child has the right of access to health information related to that treatment. It is up to state law whether the parent also has the right to the health information. If state law is silent on this issue, the health care provider is supposed to use its professional judgment.

The Privacy Rule contains detailed procedures for providing all of these rights. For example, a health care provider must try to get a patient's signature on a form saying that the person received the notice of information practices. The provider must keep these forms for a number of years. The other rights have similarly detailed requirements. This portion of the resource guide provides only a brief overview of the requirements associated with these rights.

Administrative Duties of Covered Providers

To make sure that covered providers and health plans follow these rules, the Privacy Rule requires them to take a number of administrative steps. Some of these administrative duties are discussed below.

Most important, covered health care providers and plans are required to develop and put into place written policies and procedures for protecting health information. With respect to using health information within an organization, health care providers and plans must set policies to implement the minimum necessary rule's requirements. For instance, a doctor's office must make a policy decision about the minimum amount of information necessary for different employees to use within the office. After deciding which employees need access to health information and what information the employees need to access, the office must set policies and

procedures that reflect these decisions. The doctor's office may, for example, adopt a policy that a scheduling clerk is not supposed to have access to patients' medical records.

Health care providers and plans also must train their employees in these privacy policies and procedures to ensure that they are followed. Providers and plans must select a "privacy officer" in their office who is in charge of being familiar with the Privacy Rule. They must also appoint a person to receive complaints. This may or may not be the same person as the privacy officer.

In addition, providers and plans are required to take reasonable steps to safeguard protected health information from improper uses and disclosures. This might mean using keywords to gain access to computers or locking a file room.

The Privacy Rule also requires providers and plans to keep certain documents such as their written privacy policies and authorizations that people have signed. Generally, these documents must be kept for at least six years.

The administrative requirements usually do not require a plan or provider to take a specific action. Instead, the requirements are fairly general. This allows organizations to comply with the Rule by taking action that is appropriate to their size and structure. For example, the Privacy Rule requires training, but does not specify the type of training required. A sole practitioner's office can meet the training requirement by giving new employees a pamphlet that explains who is allowed access to health information and what information they are permitted to review. Training should be more detailed at a large hospital that has many departments with different levels of need for health information.

APPENDIX B
SUMMARY OF ALL ADMINISTRATIVE SIMPLIFICATION RULES

In order to encourage the health care industry to adopt computer technology, Congress enacted the Administrative Simplification Provisions of HIPAA. This gave the Secretary of the United States Department of Health and Human Services (HHS) the power to make rules for how this new computer-based health information system will work. These rules, often called "standards," are in different stages of development. Some rules have been issued in final form and currently are in effect; others are still being developed. The United States Department of Health and Human Services' current and planned rules governing computer-based health information include the following:

- **Transactions and Code Sets:** This rule creates uniform computer-based formats and codes for sending health information. This rule went into full effect in October 2003.
- **Unique Identifiers:** Under this rule, every health care provider, employer and health plan covered by HIPAA will be given a unique identifier, like a tax identification number. These unique identifiers will be used for processing all health claims and similar administrative activities. The rules for provider and employer identifiers have been finalized, but rules for health plan identifiers are still in development. There are also plans to give each person in the United States a unique health identifier that would be used for all health care purposes, such as a medical record number and an insurance identification number. The development of the personal health identifier is currently on hold.
- **Privacy of Individually Identifiable Health Information:** Known as the Privacy Rule, this rule creates the first general federal protections for the privacy of health information. It sets standards for using health information and sharing it with others. It also gives people new rights in managing their own health information, including the right to see, copy and correct their medical record. This rule has been in effect since April 2003. The Privacy Rule is discussed in detail in Part I of this resource guide.
- **Security:** The Security Rule is related to the Privacy Rule. While the Privacy Rule controls *who* can see and use health information, the Security Rule sets standards for *how* to protect the confidentiality of the information. This rule includes administrative, physical and technical requirements for protecting health information. It is designed to make sure that health information stored and sent by computers remains confidential, is not tampered with and is available when needed. The Security Rule is in effect.
- **Enforcement:** This rule sets out the procedures that HHS must follow to penalize those people or organizations that violate the HIPAA rules. It also describes the various levels of penalties that HHS can impose for different kinds of violations. HHS has issued the final rule on civil penalties but has not yet issued the rule addressing criminal penalties.

Those who are covered by the administrative simplification provisions of HIPAA will need to comply with all of these sets of rules once they are in effect.

APPENDIX C
GENERAL HIPAA PRIVACY RESOURCES

- **HHS, Office of Civil Rights**
  http://www.hhs.gov/ocr
    Text of Privacy Rule
    Guidance
    FAQs

  http://www.hhs.gov/ocr/hipaa/smallbusiness.html
    Helpful links for small providers

- **HHS, Centers for Medicare & Medicaid Services (CMS)**
  http://www.cms.hhs.gov/hipaa/hipaa2/default.asp
    Covered entity evaluation tool
    Focuses on transaction and code standards

  http://www.cms.hhs.gov/medicaid/hipaa/adminsim
    Medicaid and HIPAA Administrative Simplification Issues
    Letters from CMS to state officials

- **HHS, Office of the Assistant Secretary for Planning & Evaluation (ASPE)**
  http://aspe.hhs.gov/admnsimp/
    Administrative Simplification history

- **State professional associations**
    For example, state medical or hospital associations

APPENDIX D
HIPAA IDENTIFIERS

(Items that may be used either directly or indirectly to identify the person who is the subject of the information)

45 CFR Sec. 164.514

1. Names;
2. All geographical subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of a ZIP code, if according to the current publicly available data from the Bureau of the Census:
    a. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
    b. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer peoples changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full-face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (With the exception of codes assigned to allow information to become de-identified and re-identified. Such codes cannot be derived from information about the individual. Furthermore, the covered entity cannot use or disclose the code and cannot disclose the mechanism for re-identification.)

APPENDIX E
MODEL BUSINESS ASSOCIATE CONTRACT

Medical Privacy - National Standards to Protect the Privacy of Personal Health Information

SAMPLE BUSINESS ASSOCIATE CONTRACT PROVISIONS

(Published in FR 67 No.157 pg.53182, 53264 (August 14, 2002))

Statement of Intent

The Department provides these sample business associate contract provisions in response to numerous requests for guidance. This is only sample language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy Rule. However, use of these sample provisions is not required for compliance with the Privacy Rule. The language may be amended to more accurately reflect business arrangements between the covered entity and the business associate.

These or similar provisions may be incorporated into an agreement for the provision of services between the entities or they may be incorporated into a separate business associate agreement. These provisions only address concepts and requirements set forth in the Privacy Rule and alone are not sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that are required or typically included in a valid contract. Reliance on this sample is not sufficient for compliance with State law and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Furthermore, a covered entity may want to include other provisions that are related to the Privacy Rule but that are not required by the Privacy Rule. For example, a covered entity may want to add provisions in a business associate contract in order for the covered entity to be able to rely on the business associate to help the covered entity meet its obligations under the Privacy Rule. In addition, there may be permissible uses or disclosures by a business associate that are not specifically addressed in these sample provisions, for example having a business associate create a limited data set. These and other types of issues will need to be worked out between the parties.

Sample Business Associate Contract Provisions[1]

Definitions (alternative approaches)

Catch-all definition:

Terms used, but not otherwise defined, in this Agreement shall have the same

meaning as those terms in the Privacy Rule.

Examples of specific definitions:

a. Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].

b. Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].

c. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

d. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

e. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

f. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

g. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate

a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.

b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]

d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such

information.

f. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

g. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]

h. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available [to the Covered Entity, or] to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

i. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

j. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms], information collected in accordance with Section [Insert Section Number in Contract Where Provision (i) Appears] of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Permitted Uses and Disclosures by Business Associate

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

a. Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:
[List Purposes].

b. Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose

Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions [only necessary if parties wish to allow Business Associate to engage in such activities]

a. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

d. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions [provisions dependent on business arrangement]

a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

Term and Termination

a. Term. The Term of this Agreement shall be effective as of [Insert Effective Date], and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. [Term may differ.]

b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

    1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

    2. Immediately terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or

    3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

    [Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c. Effect of Termination.

    1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

    2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and

disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

c. Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

[1] *Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions and are not intended to be included in the contractual provisions.*

APPENDIX F
AUTHORIZATION FORMS

Fill out the following section if this form is being filled out by someone who has the legal authority to act on behalf of the applicant/member (such as the parent of a minor child, an eligibility representative, or a legal guardian).

Print name of person filling out this form:

_____

Signature of person filling out this form:

_____

Date: _____/_____ /_____

Address: _____

_____

Telephone number: _____- _____- _____

*Authority of person filling out this form to act on behalf of the applicant/member:

_____

*If this form is being filled out by someone who has been appointed by a court as a legal guardian or conservator, or who has power of attorney or health-care proxy, **a copy of the applicable legal document must be attached.**

Send the filled-out MassHealth Permission to Share Information (PSI) Form to the MassHealth Enrollment Center (MEC) closest to you:

Revere MEC
300 Ocean Ave.
Suite 4000
Revere, MA 02151

Springfield MEC
333 Bridge St.
Springfield, MA 01103

Taunton MEC
21 Spring St.
Suite 4
Taunton, MA 02780

Tewksbury MEC
367 East St.
Tewksbury, MA 01876

MassHealth Permission to Share Information (PSI) Form

Use this form if you want MassHealth to share the information we have about you with another person or organization, such as:

- a family member, friend, or other relative;
- someone who helps take care of you;
- someone who helps you fill out MassHealth forms; or
- a social worker, lawyer, or health-care advocacy group.

Do not use this form if you want:

- information about yourself;
- information about your children under age 18 (You can usually get this without filling out any forms.); or
- your eligibility and payment information to be shared with your health-care provider. (Your health-care provider can get information about your MassHealth eligibility and payment for services provided to you without you filling out any forms.)

Important: If you decide that you **do** need to fill out this form, **you must fill out all sections completely. Please print clearly.**

Section 1: Name of MassHealth Applicant or Member

Permission is given for MassHealth and its representatives to share information listed in **Section 2** about:

_____

(Name of applicant or member whose information is to be shared)

Address: _____

_____

Date of birth: _____/_____ /_____

Telephone number: _____ - _____ - _____

Social security number: _____- _____ - _____

with the person or organization listed in **Section 3**.

Please Note: The applicant's or member's social security number is required if one has been issued, unless he or she is applying for or getting only MassHealth Limited, Children's Medical Security Plan (CMSP), or Healthy Start benefits.

Section 2: What Information Do You Want Shared?

Check the box or boxes that apply. Please read carefully.

I am giving MassHealth permission to share:

- ❑ **eligibility notices and information about eligibility for, and access to, MassHealth benefits with the person or organization listed in Section 3.** (Check this box only if you want the person or organization in **Section 3** to be able to contact MassHealth to get eligibility information and copies of your eligibility notices.)

  Please Note: Eligibility notices include information about all members of a household. If you check this box, a separate PSI Form must be submitted and signed by each member of your household who is 18 years of age or older. If we do not get forms signed by each member of your household who is 18 years of age or older, we will not be able to honor your request.

- ❑ **information about the status of my disability determination and notices about my disability determinations.** (Check this box only if you have submitted a MassHealth Disability Supplement and are waiting for a determination of your disability.)

- ❑ **only the following information (please be specific)**:

  _____

  _____

By giving MassHealth this permission to share information, are you *also* giving MassHealth permission to share any drug and alcohol treatment information it has about the applicant or member?

- ❑ **Yes, share drug and alcohol treatment information.**
- ❑ **No, do not share drug and alcohol treatment information.**

Section 3: Whom Do You Want Us to Share Information With?

List the name of **ONLY ONE person or organization** in this section. You must fill out another PSI Form if you want to name more than one person or organization.

MassHealth may share the information listed in **Section 2** with:

Name of person or organization:

_____

In care of (name of person in organization to whom mail should be sent):

_____

Address: _____

_____

Telephone number: _____ - _____ - _____

Fax number: _____- _____- _____

Section 4: Why Do You Want Us to Share Your Information?

Tell us why you want to share the information listed in **Section 2**. If you do not want to list reasons, write: "at my request." If you leave this section blank, we will assume you mean "at my request."

I am giving MassHealth my permission to share the information listed in Section 2 because:

_____

_____

Section 5: End of Permission

This Permission to Share Information is good until:

_____/_____/_____

If you do not put a specific end date, this permission will end 12 months from the date we get this form.

Section 6: Signature

I understand that:

- when the person or organization named in **Section 3** gets this information from MassHealth, that person or organization may be able to share it with others without my permission. If they do so, federal and state privacy laws may not protect the information;
- I need to send this PSI Form to the MassHealth Enrollment Center (MEC) (listed on the back of this form) closest to where I live;
- I may cancel this permission at any time by sending a letter to:

  MassHealth
  Privacy and Security Office
  600 Washington Street
  Boston, MA 02111;

- if I cancel this permission, MassHealth cannot take back any information that it shared when it had my permission to do so;
- if I do not give MassHealth permission to share information, or if I cancel my permission to share information with the person or organization named in **Section 3**, the applicant's or member's MassHealth benefits will not be affected in any way; and
- in certain circumstances, MassHealth may not honor my request to share information.

Signature of applicant/member:

_____

Date: _____/_____/_____

(See other side.)

Si este formulario lo llena una persona con la autoridad jurídica para actuar en nombre del solicitante/afiliado (p. ej., el padre o la madre de un menor de edad, un representante para la determinación del cumplimiento de requisitos o un tutor legal) sírvase completar la siguiente sección:

Nombre de la persona que llena el formulario (en letra de molde):

_____

Firma de la persona que llena este formulario:

_____

Fecha: _____/_____/_____

Dirección: _____

_____

Teléfono: _____ - _____ - _____

*Autoridad de la persona que llena el formulario para actuar a nombre del solicitante/afiliado:

_____

*Si este formulario lo llena una persona designada judicialmente para actuar como tutor o apoderado legal, o una persona con poder firmado, o representante para efectos de atención médica, **se deberá adjuntar una copia del documento correspondiente.**

Envíe este Formulario MassHealth: Autorización para compartir información (PSI) llenado al Centro de inscripción de MassHealth (MEC) más cercano a su domicilio:

Revere MEC
300 Ocean Ave.
Suite 4000
Revere, MA 02151

Springfield MEC
333 Bridge St.
Springfield, MA 01103

Taunton MEC
21 Spring St.
Suite 4
Taunton, MA 02780

Tewksbury MEC
367 East St.
Tewksbury, MA 01876

Formulario MassHealth: Autorización para compartir información (PSI)

Use este formulario si desea que MassHealth comparta información sobre usted con otras personas o entidades, por ejemplo:

- un familiar, amigo u otro pariente;
- alguien que cuide de usted;
- alguien que lo ayude a completar los formularios MassHealth; o
- un trabajador social, abogado o un grupo asesor de asistencia médica.

No use este formulario si desea:

- información sobre usted;
- información sobre sus hijos menores de 18 años (Podrá obtenerla sin completar formularios.); o
- que se comparta con su proveedor de atención médica la información sobre sus beneficios y pagos por los servicios que usted recibe. (El proveedor de atención médica podrá obtener esta información de MassHealth sin que usted complete ningun formulario.)

Importante: Si considera que si **necesita** llenar este formulario, **sírvase llenar todas las secciones en letra de molde legible**.

Sección 1: Nombre del solicitante o afiliado a MassHealth

Se autoriza a MassHealth y a sus representantes a compartir la información que se detalla en la **Sección 2** acerca de:

_____

(Nombre del solicitante o afiliado cuya información se ha de compartir)

Dirección: _____

_____

Fecha de nacimiento: _____/_____/_____

Teléfono: _____ - _____ - _____

Número de seguro social: _____ - _____ - _____

con la persona o entidad que se detalla en la **Sección 3**.

Nota: Se exige el número de seguro social del solicitante o afiliado si tal número se ha expedido, a menos que la persona sólo esté solicitando los beneficios de MassHealth Limited, del Plan de Seguridad Médica para Niños (CMSP), o de Healthy Start.

Sección 2: ¿Qué información desea compartir?

Marque todos los casilleros que correspondan. Lea atentamente.

MassHealth puede compartir la siguiente información:

❑ **notificación sobre el cumplimiento de requisitos e información sobre requisitos para recibir y tener acceso a los beneficios de MassHealth con la persona o entidad que se detallan en la Sección 3.** (Marque esta opción sólo si desea que la persona o entidad indicada en la **Sección 3** pueda comunicarse con MassHealth para obtener información sobre el cumplimiento de requisitos y copias de sus notificaciones sobre el cumplimiento de requisitos.)

Nota: Las notificaciones sobre el cumplimiento de requisitos incluyen información sobre todos los miembros del mismo hogar. Si marca esta opción, cada miembro afiliado de su familia que tenga 18 años o más deberá firmar y entregar un Formulario PSI por separado. Si no recibimos los formularios firmados por cada miembro de su familia que tenga 18 años o más, no podremos darle curso a su solicitud.

❑ **situación y notificaciones sobre la determinación de mi discapacidad.** (Marque esta opción sólo si presentó un Suplemento de Discapacidad de MassHealth y está esperando una determinación sobre ella.)

❑ **sólo la siguiente información (favor de especificar):**

_____

_____

Al autorizar a MassHealth a que comparta la información indicada arriba, autorizo asimismo que se comparta cualquier dato sobre tratamiento por drogas o alcohol que exista en dicha información?

❑ **Sí, autorizo que se comparta información sobre tratamiento por drogas o alcohol.**

❑ **No, no autorizo que se comparta información sobre tratamiento por drogas o alcohol.**

Sección 3: ¿Con quién desea Ud. que compartamos la información?

Indique aquí el nombre de **SÓLO UNA persona o entidad**. Deberá llenar otro Formulario PSI si desea nombrar más de una persona o entidad.

MassHealth puede compartir la información indicada en la **Sección 2** con esta persona o entidad:

Nombre de la persona o entidad:

_____

A cargo de (nombre de la persona de contacto dentro de la entidad a quien se le debe enviar la información):

_____

Dirección: _____

_____

Teléfono: _____ - _____ - _____

Fax: _____ - _____ - _____

Sección 4: ¿Porqué desea que compartamos su información?

Indique el motivo por el que desea compartir la información detallada en la **Sección 2**. Si no desea enumerar motivos específicos, basta con que escriba: "según lo solicité yo." Si no completa esta sección, supondremos que ha indicado "según lo solicité yo."

Doy autorización para que MassHealth comparta la información indicada en la Sección 2 por el siguiente motivo:

_____

_____

Sección 5: Fecha de expiración del permiso

La presente autorización para compartir información es válida hasta: _____/_____/_____

Si no indica una fecha determinada, esta autorización tendrá una validez de 12 meses a partir de la fecha en que recibamos el presente formulario.

Sección 6: Firma

Entiendo que:

- una vez que la persona o entidad indicada en la **Sección 3** reciba la información de MassHealth, esta persona o entidad puede a su vez compartir la información con otros sin mi permiso. Si lo hace, puede que las leyes federales y estatales de confidencialidad no protejan esta información;
- debo enviar este Formulario PSI al MassHealth Enrollment Center (MEC) más cercano a mi domicilio (ver al dorso);
- puedo cancelar esta autorización en cualquier momento, enviando una nota a:

  MassHealth
  Privacy and Security Office
  600 Washington Street
  Boston, MA 02111;

- si cancelo mi autorización, MassHealth no se puede retractar de la información que divulgó cuando tenía mi autorización;
- si no autorizo a MassHealth para que comparta la información o si anulo mi autorización para compartir la información con la persona o entidad indicada en la **Sección 3**, los beneficios MassHealth del solicitante o afiliado no se verán afectados de ningun modo; y
- en ciertas circunstancias, es posible que MassHealth no pueda cumplir con mi solicitud de compartir la información.

Firma del solicitante/afiliado:

_____

Fecha: _____/_____/_____

(Sigue al dorso.)

APPENDIX G
PLAIN LANGUAGE PRINCIPLES AND THESAURUS FOR MAKING HIPAA PRIVACY NOTICES MORE READABLE

EXAMPLES OF NOTICES OF PRIVACY PRACTICES

Plain Language Principles and Thesaurus

for Making HIPAA Privacy Notices More Readable

Prepared for the Health Resources and Services Administration,

in consultation with the Office for Civil Rights, and other offices and agencies

within the U.S. Department of Health & Human Services, Washington, D.C.,

and plain language specialists.

Section I - Principles for Writing HIPAA Notices of Privacy Practices in Plain English

Principles for Plain Language Privacy Notices

Introduction

You are writing a HIPAA Privacy Notice. Your dilemma is: It's a legal document that must meet the intent and letter of the law, but it also has to be in Plain Language. If you use these Principles you will:

- be able to write it more quickly and easily,
- have fewer revisions and editions.

These Principles are intended as an aid to writers of Privacy Notices and are not necessarily a guarantee to meet all of the legal requirements of HIPAA. This guidance is intended solely to provide some helpful hints for making a notice of privacy practices more readable. It does not create any binding requirements for how a notice of privacy practices must be phrased or structured.

The Principles are presented in a "progressive format." That is, the Plain Language process is arranged to flow from the most general to the more detailed. There are advantages to using the same format in your Privacy Notice. Sections in the Principles are:

Section 1. Introduction and preamble (an overview)
Section 2. Principles (Individual principles)
Section 3. Examples for each principle using HIPAA content. (Details)
Section 4. Appendices (Very specific details)

The Privacy Rule encourages, but does not require, writers to develop a "layered" notice. The Preamble to the Final Modification of August 14, 2002, Federal Register page 53243, says that a two layered notice would satisfy notice requirements. The first layer would be a short notice that summarizes individual's rights and other information. The second layer would be longer and include all the elements required by the Rule.

It is possible to combine the "layered" format with the "progressive" format, by using the elements of the "progressive" approach in the second, longer, layer.

It is important to remember that the Notice must include all the elements that the Rule requires. You can find the details in the Rule. If you are using the progressive approach the required elements can be integrated in the relevant parts. The required elements are:

- Header with specific language
- Uses and disclosures
- Separate statements for certain uses and disclosures
- Individual rights
- Covered entity's duties
- Complaints
- Contact

The basis for the Principles is a mix of well known advice for Plain Language. This "mix" is outlined in Suitability Assessment of Materials (SAM).[1] Other resources in health care communication can be found at most State Health Departments.

Principles:

1. The Content of the Notice:

The HIPAA rules tell us the topics that must be in the Notice. A special highlighted header on the purpose is also required. But the Notice writer is free to arrange the order of the topics. And the rules allow and encourage that other topics may be added. You may want to place topics in the order of your patients' interest - with the most interesting topic first. After the required statement, the order may be:

a) A preamble, including "What good is this Notice to me?" (Examples)
b) What is a health care record? (Examples.)
c) Patient Rights. (Examples)

d) Who can see your record without asking you? (Examples)
e) Who can't see your record unless you give a written OK? (Examples)

A. Preamble:

A preamble is helpful before giving the HIPAA content. The reasons:

- Many won't see any personal benefits of the Privacy policy.
- The *very concept* of health care records and privacy may not be familiar. (An explanation and visual may be needed to clarify.)
- Many won't grasp why and what they are asked to sign and what use they can or should make of the Privacy Notice.

Appendix A gives an example of a preamble that covers these points.

Appendix B gives the text of the rules that describes in detail what to include, how to deliver, and other things about the notice.

2. Making the Notice easy to read and understand:

The HIPAA rules do not set a goal for readability level, but many States have set goals for health care print materials.[2] These range from 4th to 6th grade levels. In comparison, many draft Privacy Notices written to date are about 16th grade (college grad level). (Note: The average readability of this Principles document is at the 8th grade level.)

You would like the readability of your Notice to be compatible with the reading skill level of your patient population. The average reading skill of adult Americans is about 9th grade level. For people over 65, and for most

minority groups, the average skill levels are lower than 9th grade. (See Ref. 5 for reading skills by age, gender, ethnic set.)

It is clearly the intent of the rules that patients be able to read and understand the Notice. A suitable readability level is essential, but that is only one of the necessary factors for understanding. Because of the complexity of the Notice content, examples are needed to explain what is meant by many of the privacy statements. In fact, Section 164.520(b) of the rules requires that at least one example be given for certain types of disclosures.

A. To make the Notice easier to read:

- *Use a conversational style*. It is almost always easier to read narrative than more formal styles of writing. (The rules are written in formal/legal style: you must translate them.) For the first draft, write it as you would say it. Tip: If you find it hard to do this, try running a tape recorder while you tell a person the Notice content as best you can from memory or from a simple list of topics. Then transcribe and edit the tape. For example:

More Formal Language	Conversational Style
Covered entities must describe the right of patients to make amendment of a protected health record if patient believes the health information is incorrect or incomplete.	If you think there is something wrong or missing in your health record, you can ask that it be changed.

- *Use common words*. Common words are better known to the public and are often shorter. (Common words are used in the example, above right.) A Thesaurus of more common words for those found in HIPAA is in Section II. (For these Principles we use OK vs authorization, rules vs regulations, health care records vs protected medical records, etc.)

- *Use shorter sentences*. Keep the *average* sentence to about 15 words or less. Try bullets for short lists. (For example, in these Principles the average sentence length is between 15 and 20 words.)

- *Avoid hyphens and compound words*. These increase readability level. For example: self insured vs self-insured; any one vs anyone.

- *Give examples to explain "problem" words*. Problem words - if you use them -are often those that describe *a concept*, *a category*, or a *value judgment* (CCVJ). Some words and phrases may be both a category and concept depending on the context. If you use these kinds of words, add an explanation or example to define them. Here are just a few of the problem CCVJ words found in HIPAA:

Concept	Category	Value Judgment
disclosures	disclosures required by law	*adequate* notice
access	business associates	*material* changes
authorization	covered entity	*significant* number
activities	self-insured groups	*reasonable* effort

For example: "disclosures" usually means showing your health care records to someone outside this organization. This can be to another doctor treating you, or those paying for your treatment, and others.

For example: "disclosures required by law" means "When the law demands that we show your health record to other people we will do so. For example, we will report communicable diseases to the appropriate health authorities as required by law. When the law allows us to show your health record to other people, we will show it when there are good reasons to do so. For example, to assist those conducting worthwhile research."

For example: "significant number" means -% or more of the population speaks only some other language.

- *Use lower case rather than all capital letters* . Research tells us that text in all CAPS is harder and slower to read, and harder to understand. The reason: Besides looking at the letters in a word, we recognize words by their shape. For example, " try" and "medical" are easier to recognize and read than TRY AND MEDICAL.

With all CAPS the height of the letters is the same, so we lose "shape of the words" as a reading cue. This slows reading speed. For many, by the time they get to the end of a sentence, they may have forgotten what they read earlier in that sentence. Suggested remedy: To give emphasis or prominence, use bold and larger font size with lower case letters (except where grammar calls for a capital letter).

- *Assessing readability*: After drafting your Notice, assess its readability level using one of the many formulas available.

B. To improve understanding and to make it "look" easier to read:

The rules do not specify layouts, fonts, and other factors that can make the Notice look easy to read. But if it looks hard to read, many patients won't want to read it, won't bother to read it. And they won't understand it. Many draft Notices written to date have long lists of items. These look hard to grasp and to remember - and they are. Here are ways to make it look easy to read and easier to understand:

- *Allow more white space by using wider margins*. Double column of text (like a newspaper format) can also give a more open look. These layout devices will also shorten the line lengths to be closer to 50 to 60 letters and spaces. That is easiest to read.

- *"Chunk" long lists into smaller bites.* Chunking makes the information look less formidable, and helps the reader better understand and remember. Look for logical

groupings within the long list. Then place these items under suitable descriptive sub headers. Appendix C gives an example of chunking of one group of HIPAA topics.

- *Consider visuals as well as text in your Notice*. The legal nature of the HIPAA content and the absence of visuals in the rules do not in any way limit the use of visuals - especially for examples. Visuals can be used to explain a number of the HIPAA concepts. For example, consider the stated HIPAA concept phrase: "a health care record." Rough sketches of visuals that might be included for explanation are:

Figure 1. Your health care record can be all of these:

(Show a doctor holding up an x-ray to a light box.)	(A file folder with lots of papers in. A slot for "Name"___ on the cover.)	(Two sketches of desk-top computers, with image on screens. Show lightning flash between computers to show linkage.)
An x-ray	**A folder of papers**	**A computer file**

-*Use large fonts and high contrast*. Older readers tend to need larger font sizes. Use at least 12 point font for your Notice. And they need high contrast between ink and paper. For example, black ink on white paper, or black on light yellow paper. Do not use high gloss paper. It has a higher glare.

- *Give the context first, before giving the new information*. With the context first, it is easier to associate the information with things we already know. If the context is last, we must carry in short term memory all of the preceding information until we get to the end of the sentence. By then, we may have forgotten much of the information that went before.

Original: Context **last** - Harder to read: (in italics)

"We will also provide your physician or a subsequent health care provider with copies of various reports that should assist with your treatment *once you are discharged from this hospital."*

Rewritten: Context **first** - Easier to read:

"*Once you are discharged from this hospital*, your physician or other health care providers will be treating you. We will give copies of your health records to doctors and other health providers to help them in treating you."

C. Use Visuals that explain and clarify:

Readers should be aware that the Privacy Rule does not require the use of visuals, however, the research tells us that visuals help us understand, and they are a great help to memory. (We remember the face - a visual, but not the name - words). Visuals also "lighten" the page appearance and make it more inviting. For the Privacy Notice, simple visuals could be the examples that clarify the meaning of:

- sharing of your record by doctors and nurses treating you
- paying for treatment
- running the hospital or clinic
- telling about other health benefits and services
- reminding you of appointments
- telling you about treatment choices
- including you in the hospital directory
- telling family and friends
- others

- *Use simple line drawings*. These work best because they convey the image without background clutter. They are also less costly to make and can be made and revised quickly. Even stick figure icons can greatly improve memory.

- *Cue the viewer*: The patient needs to quickly grasp what to look at in the picture. For example, if the visual is to show one doctor disclosing a patient record to another for treatment, consider adding an arrow pointing to the folder they are both sharing. The words, "talking about your record" might be added to the arrow.[3]

- *Use action captions*: A short, action caption tells what the visual is all about - its key point. For example, if a visual showed an appointment slip, a caption might say something like, "To remind you when to come back."

With few exceptions, it is best to include a caption with each visual and always locate the caption in the same place with respect to the visual. If the layout of the text and visuals on the page clearly associates the two, then the adjacent text may serve as the caption.

3. Make it suitable for the culture:

First impressions: First impressions do count on how we accept new things. The rules say nothing about a cover page for the Notices. This gives you, the writer, a chance to create a cover that projects a culture friendly image. Although this is not required by the Privacy rule, you will find it helpful to make sure that your notice responds to the culture of the readers. For example, for a Native American population, consider a cover visual showing a Native American patient. The cover might also show a doctor holding or using a health care record. For a mix of ethnic groups (often the case) show a mix of people from ethnic groups on the cover.

- Match the logic, language, experience of the culture: Write your Notice with these three factors in mind. (But to really know if your draft notice is culturally suitable, you will need to pretest your Notice with a small sample of typical adults from that culture. One-to-one pretesting is recommended. Appendix D outlines a pretesting protocol.)

- *Logic*: Each culture has its own logic with respect to health. For example: It is the logic of many ethnic groups that "the doctor knows best" and their logic and belief is never to question such an authority figure - even if they think their record is wrong. One remedy: The Notice may have to take pains to make such questioning easy for the patient (perhaps by modeling some questions) and/or show by example (a visual?) that it is OK to do so.

It is logical to think in the here and now, rather than future possibilities. Thus, it may be hard to grasp the logic of showing a patient's health record to a funeral director, or to law enforcement. (Does it mean I'm going to die, or be arrested?) For these, and other less likely disclosures, consider grouping them under a sub-header and adding a short explanation. For example: "When law demands or allows us to we would show your health record to other people. Sometimes when there are good reasons to do so, we could show them."

- *Language*: Although many words and terms used in regulations such as HIPAA need translation for any culture, care must be taken so that terms are correctly used. Many words are best explained by an example. For example: "Health Oversight Authorities" such as health inspectors, and other government people who check our hospitals and clinics."

Metaphors can be misleading in any culture. For example, one draft Notice says that the health record serves "as a tool for education of health care professionals." But in millions of minds, tools are things like hammers, saws, drills. They may think, how could the pieces of paper be like those?

- *Experience*: The content of the Notices presupposes a number of special skills in literacy, problem solving, and experience. That is, the reader has *to be able to do certain tasks* or have some *prior knowledge or experience*.

For example, the tasks and experience needed for patients to exercise their right to limit disclosure of some part of their health care records include:

1. Understanding that they have a right to do this, and the limits of that right.
2. Have experience with the process and carry out the required actions. (Write a request, know who to send it to, etc.)
3. Know how to verify that their request was honored, and protest if it was not.

For each of the Patient Rights, consider doing a simple task analysis similar to that shown above. That will help you to see if your patient population is likely to have the needed experience and skills to exercise those rights. If they do not, then we suggest that additional helpful advice be included. This may be in the Notice itself or in a supplementary piece. Insight into the skills of the US population as a whole, as well as that of several minority groups can be obtained from the National Adult Literacy Survey (NALS).[4]

4. For those with very limited reading skills

Even the most carefully prepared Privacy Notices are likely to be over the heads of about twenty percent of the adult American population. A copy of the Notice may be given to the patient with the hope that someone at home will read and explain it. Another option is to "tell" the Notice content or use another media. This might be a talk, an audio tape, a pictorial series, or a video tape. For some, an interactive web site may be suitable.[5] This is not a requirement of the rule, but is something you may want to consider.

In all these media, many of the Principles in the pages above will apply. Some new principles must be added:

- For factual content, limit the audio tape or video to no more than about eight minutes. Five minutes is better. Otherwise listeners forget most of the facts.

- Use a story as the fabric to allow you to over-weave the factual HIPAA content. People can remember the factual information better in the context of a story.

- In the audio or video, refer to the written Privacy Notice document. Tell or show how it is a key document, and how to use it.

Conclusion: There is no really easy way to produce a highly suitable Privacy Notice for all populations. The cultures and the subjects are too complex for it to be easy. But you can use the above Principles to make the work less frustrating and more effective. Also, your Privacy Notice will be understood by a greater number of your patient population.

Section II - Thesaurus of Plain Language Words and Phrases for HIPAA Notices of Privacy Practices

This thesaurus of plain language privacy words and phrases is designed to help you write HIPAA notices that will be more readable and understandable. This document identifies technical and legal language that might be hard for most people to understand, and suggests more common words and phrases. But because the same word may have different meanings, not every plain language word or phrase will work for every writer.

You have to deal with both regulatory and language issues in writing your privacy notices. These suggested words and phrases do not give you legal protection, so you should have a lawyer review your final version. While this Thesaurus does not provide a legal safe harbor, it will help you comply with HIPAA's plain language requirements.

Privacy notice words and phrases	***Plain language words and phrases***
A	
...abide by...	...agree to...
We will *accommodate* all reasonable requests.	We will meet/agree to all reasonable requests.
The information on or *accompanying* the bill will include information...	Your bill will include information...
accrediting agency agency...	...reviewing agency; licensing
acknowledged	accepted; recognized; approved
adverse events	injuries; bad reactions
...after the delivery of treatment...	...after you've been treated...
alternative	choice
amend	change
...appropriate government authority...	...government department...
assist	help
...as soon as reasonably practicable...	...as soon as we can...

Privacy notice words and phrases	*Plain language words and phrases*
attorney	lawyer
audit	review; inspect; look at
authorization	your written permission; your written approval
...authorized public or private entity to assist in disaster relief...	...government agency or charity authorized to help with disaster relief...
...authorizing disclosures	...allowing us to share information...
B	
...before any costs are incurred...	...before we do anything that has a cost attached...
C	
certify	confirm in writing
...collaborating with...	...working with...
...collect and maintain...	...get and keep...
committed	promised
...communication source...	...source of information...
communicates	tells; let you know
The use or disclosure will be made in compliance with the law.	Your health information will be used or shared according to the law.
comply with the rule us to do...	obey the rule; doing what it tells
...coordination or management of care...	...coordinating your care; making sure you get the care you need...

Privacy notice words and phrases	*Plain language words and phrases*
correctional institution	jail or prison
...contact you at work instead of at home or vice versa...	...contact you at work or home...
...court order, subpoena, warrant, summons or similar process...	...court order; legal demand...
covered entities	Health plans, health care clearinghouses that process your health information and your health care providers (such as doctors, hospitals and clinics) that have to comply with these privacy rules.
D	
...deceased person...	...dead person; someone who died...
...de-identified information...	...information that does not identify you or tell who you are...
demographic	personal statistics; personal information
...designee of this facility...	...employee who has been identified; employee that we have identified
determine(s)	decide(s)
...disclose information...	...share information; give; tell...
...disclosures we will make...	...information we will share...
E	
effective date	...takes effect on...
...employee review activities...	... employee review (evaluations)...

Privacy notice words and phrases	*Plain language words and phrases*
...employees, staff and other hospital work personnel...	...hospital personnel; people who work at the hospital...
enable	...allow; make possible...
ensure	...make sure...
entities	facilities; institutions; organizations
...established protocols...	...has rules...
evaluate	measure; rate
examination	exam
...exercise your rights...	...use your rights...
...except as described...	...except...
...exceptions, restrictions, and limits...	...limits...
...experienced adverse events...	...been injured or hurt...
F	
...facility planning and marketing...	...business planning...
...family can be notified about your condition, status and location...	...your family can be told about your health and where you are...
...family member or personal representative	...family member who is your legal representative for health care...
...file a written complaint...	...write or e-mail a letter of complaint...
...filing a complaint...	...complaining...

Privacy notice words and phrases	*Plain language words and phrases*
...for the purpose...	...to...
G	
...governmental entity or agency...	...to (from, for, etc., as appropriate) the government...
H	
...health care operations...	...health care operations, including management of organization or facility...
health care professionals	...people who care for you; doctors, nurses; and others who care for you
..health information we have is incorrect...	...health information is wrong...
We may disclose protected health information to a *health oversight agency* for activities authorized by law, such as audits, investigations, and inspections.	We can share your health information with agencies that audit, investigate, and inspect health programs for the public's health.
...health record is physical property...	...health record belongs to...
hereby	**Do Not Use**
honor	follow, abide by
We may use and disclose medical information about you for *hospital operations*.	We may share your medical information to run the hospital.
I	
...identifiable information...	...personal information that can identify you...

Privacy notice words and phrases	*Plain language words and phrases*
...identify or locate a suspect, fugitive, material witness or missing person...	...to identify or find someone who is a suspect, fugitive, material witness, or missing person
...in an emergency situation...	...in an emergency...
incomplete	lacking
incorrect	wrong
...Indian Health Service facility...	...Indian Health Service/IHS clinic or hospital...
indicate	tell us
...individually identifiable health information...	...information about your health care that identifies you...
individual(s)	patient(s)
...individual right...	...a person's right...
...information is kept by or for the hospital...	...hospital keeps the information...
...information on or accompanying the bill...	...information with your bill...
...inmate of a correctional institution...	...prisoner...
inspect and receive a copy	get a copy...ask for a copy...see and get a copy
...in the following instances...	...in these cases...

Privacy notice words and phrases	*Plain language words and phrases*
J	
...judicial administrative proceeding... case...	...legal proceeding such as a court
K	
L	
law enforcement	police, FBI Officers, and others who enforce laws
legal options	legal choices
legal requirements	the law
Licensure	being licensed
M	
maintained	kept
...make new provisions effective...	...make changes effective...
material change	significant change
...may otherwise be at risk for... contracting or spreading the disease or condition.	...might catch your disease or spread it... .
medications	drugs; medicines
...members of the clergy...	clergy, for example, priest, minister or rabbi...
monitor	review; track

Privacy notice words and phrases	*Plain language words and phrases*
N	
...next of kin...	...close relatives
notify	tell you/tell us
...not required to agree...	...don't have to agree...
O	
..obligations we have...	...our responsibilities...
observations	...reports...
obtain a paper copy	get a copy
obtaining	getting
...other duties authorized by law... them to	...other duties that the law allows perform...
...other purposes permitted or required by law...	...other purposes that the law allows or requires...
otherwise	if not
P	
...past, present or future physical or mental health and related health care services...	...all your health services...
...pertaining to victims of a crime...	...being a crime victim...
physical property	property of; belongs to
physician	doctor

Privacy notice words and phrases	*Plain language words and phrases*
...plan for future care or treatment...	...care plan...
...policies, procedures, practices...	...our rules and standards...
...post marketing surveillance information...	...study drug safety...
...potentially endangering...	...possibly hurting...
...private insurance payers...	...insurance company...
procurement	getting
...protected health information...	...personal medical information that is protected by the rule...
...protect the privacy of your health information...	...protect your health information...
protocols	rules
...provide your treatment...	...treat you...
...provided consent...	...given consent/permission...
provider	doctor, nurse, or other provider of health care
...providing assistance with your health care...	...helping you (with your health care)...
provisions	...arranging for...
...psychotherapy information compiled in a reasonable, or use in, reasonable anticipation, or use in a civil, criminal, or administrative proceeding...	...psychotherapy notes that might be used in a court case or another legal proceeding...

Privacy notice words and phrases	*Plain language words and phrases*
Q	
R	
rebuttal	response; answer; contradict
regulation	rule
...release information...	...give out your information...
religious affiliation	religion
...request a correction/amendment...	...ask us to change; ask us to correct...
...request a restriction...	...ask us not to ...
...we are required to abide...	...we must...
restrictions	limits
revised	new; changed
revision	change
...revoke your written authorization...	...withdraw; take back; tell us not to...
S	
...submit your request in writing...	...write a letter...
...substantial communication barrier...	...communication problem...
...suspected violation...	..possible violation...

Privacy notice words and phrases	*Plain language words and phrases*
T	
thereof	**Do Not Use**
...to support business activities services; of your doctor's practice...	...for your doctor's business business services your doctor buys to run his practice...
...training of medical students...	...training medical students...
...treatment alternatives and options...	...treatment choices...
...treatment and services you receive...	...care you receive; your care...
...types of uses and disclosures...	...how we share; with whom we share; and how the information is used
U	
...unable to agree to a requested restriction...	...can't agree with your request...
...understanding utilization review activities...	...reviewing health services...
...under the custody of law enforcement...	...in legal custody...
...unless otherwise permitted or required by law as described below...	...unless allowed or required by law...
...upon your request...	...if you ask...
...use or disclose...	...use or give out; share; release...
...undertaking *utilization review* activities..	...reviewing our work...

Privacy notice words and phrases	*Plain language words and phrases*
V	
W	
...when required to do so by federal, state, or local law...	...when required by law; when the law requires...
...where we can make improvements in our care and services...	...how we can improve our care...
written complaint	a letter or e-mail
...you must do so in writing...	...write a letter or e-mail...
X, Y, Z	

Appendix A - Example of a Preamble for a Direct Treatment Provider

This Privacy Notice tells you about your rights about your health care records. You get a copy of this Privacy Notice to keep for yourself. You can look at this copy anytime to see what use is made of your health care records and who gets to see them. A new government rule requires that we give you this Privacy Notice to sign.

Our policy has always been to keep your records safe. Your records are usually kept in a folder of papers with your name on it. Your records can also be stored in a computer. Your records tell what treatments and tests you have had, and what decisions the doctors have made.

(Note: A figure could be inserted here to graphically show what the health care records may look like.)

This Privacy Notice is in four parts:

1. What your health care records are, and Your Rights about those records,
2. Who **can** see them without your written OK.
3. Who **can not** see them unless you give a written OK.
4. Our policies to protect health care records.

Appendix B

Section 164.520 - Notice of Privacy Practices for Protected Health Information

Standards for Privacy of Individual Identifiable Information

(45 CFR Part 160 and 164)

Appendix C - Chunking of long lists

Long list from Privacy Rule
(Allowable Disclosures)

- provide for your treatment
- information for payment
- health care operations
- business associates
- directory
- notifications
- communicate with family
- interpreters
- research
- funeral director
- procurement organizations
- marketing
- appointment reminders
- treatment alternatives
- Food and Drug Administration
- workers compensation
- public health
- correctional institutions
- law enforcement
- member of the military
- health oversight authorities
- non-violation notices
- disclosures by whistle blowers
- investigation, audits

Revised list with chunking
(Allowable Disclosures)

For your medical treatment and payment
- provide for your treatment
- tell you of treatment alternatives
- appointment reminders
- evaluate your care
- information for payment
- business associates

For your personal reasons
- communicate with your family
- notify people
- be listed in a directory
- for workers compensation
- get an interpreter for you
- notify a funeral director

For other reasons that help improve health
- research
- procurement organizations
- marketing
- public health
- Food and Drug Administration

Other special uses
- law enforcement request
- correctional institutions
- members of the military
- non-violation of notice
- disclosure by whistle blower
- investigation or audits

Appendix D - A simple protocol for Pretesting draft Privacy Notices

The purpose of pretesting is to find any problem areas in the draft Privacy Notice while it is still in draft form. The problems can then be addressed before wide use of the Notice.

The following steps outline how to pretest on an individual basis. These steps can be carried out in less than one week time.

1. Decide what are the most important concepts and pieces of information in your draft Privacy Notice. What is most important for the reader to know and understand how to do? (For some, that might be to understand the concept of their medical record, and the fact that they can have a say in who sees it.)

2. Write open ended questions that would show that readers understand these key concepts and pieces of information. For example, "Tell me what you understand your medical record to be. What is it?" (At least 5 questions, but not more than 10.) Prepare a sheet(s) that lists the questions and spaces to record - verbatim - the readers' responses.

3. Write a brief description that explains to the test givers the purpose and process of the pretest. Test givers might start out by explaining that the writers of the Notice are trying to make the Privacy Notice easy to understand. "We'd like you to read the Notice, and then we will ask you a few questions about what you have read. It will take only a few minutes. There is no right or wrong, we want to know what you understand about the Notice."

4. Sample size and recording responses: Select a sample size of at least 30 individuals. Ideally, they would consist of 10 each from three different parts of your patient population.

5. Analyze the responses, and make appropriate changes in the draft Notice and/or provide supplementary instruction as needed.

References

1. Doak, Doak, Root. Teaching patients with low (*or any*) literacy skills. J.B.Lippincott Co., Philadelphia, Pa. 1996, pp 49-58.

2. Matthews TL, Sewell JC. State Official's Guide to Health Literacy. 2002. The Council of State Governments, PO Box 11910, Lexington, Ky. 40578-1910.

3. Wileman RE, Visual Communicating. Educational Technology Publications, Englewood Cliffs, NJ, 07632, 1993, p. 24. Also, Ref. 1, Ch. 7.

4. Kirsch IS, Jungeblut A, Jenkins l, Kolstad A. Adult Literacy in America. National Center for Educational Statistics, US Dept. Of Educ. Wash D.C., Sept. 1993.

5. Beyond the Brochure: Alternative approaches to effective health communication. 1993. AMC Cancer Research Center, 1600 Pierce St., Denver, CO, 80214. (In cooperation with the Centers for Disease Control and Prevention. Agreement No. U50/CCU806186-03)

STATE OF NEW YORK
DEPARTMENT OF HEALTH

Corning Tower The Governor Nelson A. Rockefeller Empire State Plaza Albany, New York 12237

Antonia C. Novello, M.D., M.P.H., Dr.P.H.
Commissioner

Dennis P. Whalen
Executive Deputy Commissioner

Privacy Notice

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Effective April 14, 2003, the New York Medicaid program must tell you how we use, share, and protect your health information. The New York Medicaid program includes regular Medicaid, Medicaid Managed Care, Family Health Plus, and Child Health Plus A. The program is administered by the New York State Department of Health and the Local Departments of Social Services.

Your Health Information is Private.
We are required to keep your information private, share your information only when we need to, and follow the privacy practices in this notice. We must make special efforts to protect the names of people who get HIV/AIDS or drug and alcohol services.

What Health Information Does the New York Medicaid Program Have?
When you applied for Medicaid, Family Health Plus, or Child Health Plus A, you may have provided us with information about your health. When your doctors, clinics, hospitals, managed care plans and other health care providers send in claims for payment, we also get information about your health, treatments and medications.

If you enrolled in Child Health Plus B, the New York Medicaid program does not have your health information. You should contact your Child Health Plus B plan with questions about your health information.

How Does the New York Medicaid Program Use and Share Your Health Information?
We must share your health information when:

- ***You or your representative requests your health information.***
- ***Government agencies request the information as allowed by law such as audits.***
- ***The law requires us to share your information.***

In your Medicaid application, you gave the New York Medicaid program the right to use and share your health information to pay for your health care and operate the program. For example, we use and share your information to:

- ***Pay your doctor, hospital, and/or other health care provider bills.***
- ***Make sure you receive quality health care and that all the rules and laws have been followed.*** We may review your health information to determine whether you received the correct medical procedure or health care equipment.
- ***Contact you about important medical information or changes in your health benefits.***
- ***Make sure you are enrolled in the right health program***.
- ***Collect payment from other insurance companies.***

We may also use and share your health information under limited circumstances to:

- ***Study health care.*** We may look at the health information of many consumers to find ways to provide better health care.
- ***Prevent or respond to serious health or safety problems for you or your community as allowed by federal and state law.***

We must have your written permission to use or share your health information for any purpose not mentioned in this notice.

What Are Your Rights?

You or your representative have the right to:

- Get a paper copy of this notice.
- See or get a copy of your health information. If your request is denied, you have the right to review the denial.
- Ask to change your health information. We will look at all requests, but cannot change bills sent by your doctor, clinic, hospital or other health care provider.
- Ask to limit how we use and share your information. We will look at all requests, but do not have to agree to do what you ask.
- Ask us to contact you regarding your health information in different ways (for example, you can ask us to send your mail to a different address).
- Ask for special forms that you sign permitting us to share your health information with whomever you choose. You can take back your permission at any time, as long as the information has not already been shared.
- Get a list of those who received your health information. This list will not include health information requested by you or your representative, information used to operate the New York Medicaid program or information given out for law enforcement purposes.

See the New York State Department of Health web site for a copy of this notice: www.health.state.ny.us.

1. **For more privacy information, to make a request or to report a privacy problem/complaint*, please contact the Medicaid Help Line Office at: (518) 486-9057 or 1-800-541-2831. TTY users should call 1-800-662-1220. The Help Line will direct your calls to the correct state and local department of social services office.**

2. You may also report a complaint* to: The Office for Civil Rights, Department of Health and Human Services, Jacob Javits Federal Building, 26 Federal Plaza, Suite 3312, New York, New York 10278; (Telephone) (212) 264-3313 or 1-800-368-1019; (Fax) (212) 264-3039; or (TDD) (212) 264-2355.

***You will not be penalized for filing a complaint**.*

If we change the information in this notice, we will send you a new notice and post a new notice on the New York State Department of Health web site.

The New Mexico Medicaid Program
Notice of Privacy Practices Summary

Effective Date April 14, 2003

What types of information does NM Medicaid collect?

In order to assist you, NM Medicaid may collect certain information about you. This may include your:

- name
- address
- birth date
- financial information
- information about your health

NM Medicaid may ask you for your medical history or medications you may be taking. NM Medicaid may also ask you if you have any health problems.

What does NM Medicaid do with this information?

- shares information about you with people who provide treatment for you
- discusses your information with other people who are also involved in your health care or who pay for your care
- shares your information with other government agencies
- shares some of your information to collect payment from others

When else can NM Medicaid release your information?

- if it is needed to prevent or control the spread of a disease
- to the courts or law enforcement if NM Medicaid is ordered by a court to do so

What are your rights?

- to see any medical information we may have about you
- to get a copy of any medical information we may have about you
- to ask us to make corrections if you think there are mistakes in any health information we may have about you
- to know with whom NM Medicaid has shared your information
- to ask us not to share parts of your medical information

What do you do if you have a complaint?

If you want to file a complaint, you may write to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer at NM Medicaid at the address below.

New Mexico Medical Assistance Division
HIPAA Privacy Officer
P.O. Box 2348
Santa Fe, NM 87504-2348
1-888-997-2583
1-505-476-6800 (Santa Fe area only)

You may also file a complaint with the U.S. Department of Health and Human Services at the address below.

Secretary of the United States Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

If you file a complaint, it will not be held against you or any member of your family. More information is included on this form. Please read the "Notice of Privacy Practices".

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you are a person with a disability and you require this Notice in a different format or require assistance to understand this form, you may ask for help from the HIPAA Privacy Officer.

How the New Mexico Medicaid Program May Use or Disclose Your Health Information

Treatment

The people who provide health care services to you will use information about you to decide how best to care for you. We may share health information about you to provide the services you may need, such as physical examinations, nutritional services, medications and prescriptions or hospitalization. We also may share health information about you with people outside the New Mexico Medicaid Program who may be involved in your medical care, such as family members, physicians or others who provide part of your care.

Payment

NM Medicaid may share information about you to get payment for our services from your health plan or insurance company. For example, we may need to give your health plan information about a clinical exam or immunizations you received (or your child received) so your health plan will pay us or pay you back for the treatment or services we provided. We may also tell your health plan or insurance company about a treatment you are going to receive so they can approve it and agree to pay for the treatment.

Health Care Operations

We may use your health information to review the treatment and services you received and to evaluate the care given to you. We may combine health information about many recipients to decide whether additional services should be offered, what services are needed and whether certain new treatments and services are working. NM Medicaid may share information with doctors, nurses, technicians, medical interns, other NM Medicaid staff, and other government agencies or divisions for review purposes. NM Medicaid may combine the health information NM Medicaid has with health information from other health care providers to compare how we are doing and to see where we can make improvements in the care and services we offer. We may also share your information for reviews and grievances. Sometimes NM Medicaid will remove your name from information so others may use that information to study our health care services. We may release part of your information to follow workers' compensation rules.

Appointment Reminders and Information

NM Medicaid may call or write to you to remind you that you have an appointment for treatment or medical care. NM Medicaid may tell you about health-related benefits or services that may be of interest to you.

Individuals Involved in Your Care or Payment for Your Care

NM Medicaid may give information about you to a friend or family member who is involved in your medical care. NM Medicaid may also give information to someone who helps pay for your care.

Veterans and Specialized Government Functions

If you were a member of the armed forces, NM Medicaid may release health information about you as required by the Veterans' Administration. NM Medicaid may also release information about you for security or military reasons.

As Required by Law

NM Medicaid must share health information about you when required to do so by federal, state or local law.

Public Health Risks

NM Medicaid must share health information about you for public health reasons as required by federal or state law:

- To prevent or control disease, injury or disability;
- To report child abuse or neglect;
- To report reactions to medications or other problems with products;
- To notify people of recalls and defects about products they may be using;
- To notify a person who may have been exposed to a disease or may be at risk for catching or spreading a disease or condition;
- To notify the appropriate government authority if NM Medicaid believes a patient or client has been the victim of abuse, neglect or domestic violence;
- To prevent a serious threat to health or safety.

Health Oversight Activities

NM Medicaid may share health information for accreditations, audits, investigations, inspections, and licensing. This is necessary for the state and federal government to monitor the health care system, government programs and laws.

Lawsuits and Other Disputes

If you are involved in a lawsuit or other legal dispute, NM Medicaid may share health information about you in response to a court order or for a fair hearing. NM Medicaid may also share health information about you in response to a subpoena or other lawful process by someone else involved in the dispute.

Law Enforcement

NM Medicaid may share information about you if asked to do so by a law enforcement official, subject to federal and state laws and regulations. NM Medicaid may also share information in response to a court order, following a subpoena, warrant, summons or similar legal process.

Other Uses of Health Information

NM Medicaid will not use or share health information about you for any reason other than those listed above without your written permission. If NM Medicaid shares information about you *with your permission*, NM Medicaid cannot take back the information already shared. NM Medicaid also must keep records of the services you received which NM Medicaid either paid or denied.

Your Rights Regarding Your Health Information

Right to Inspect and Copy

You have the right to see and receive copies of the health information NM Medicaid has about you. To inspect and request copies of your health information, you may contact the HIPAA Privacy Officer. If you want to see your health information that may be in more than one location or if you have any questions about your information, you must write to the HIPAA Privacy Officer. If you ask for copies, NM Medicaid may charge you for the costs of copying and mailing the information to you. NM Medicaid may deny your request as permitted by the HIPAA Privacy Rule. If NM Medicaid denies your request to see your health information, you may ask us why and ask for a review of our decision. A licensed health care professional chosen by us will review your request and the denial. The person who reviews the denial will not be the same person who originally denied your request. NM Medicaid will do whatever the reviewer recommends.

Right to Request a Correction to Misinformation

If you believe that health information NM Medicaid has about you is not correct or is incomplete, you may ask us to correct it. You have the right to ask for a correction for as long as the information is kept by NM Medicaid. To ask for a correction, you must write to the HIPAA Privacy Officer who will review your request. You must give us a reason that supports your request. NM Medicaid may deny your request for a correction if it is not in writing or does not include a reason to support the request. NM Medicaid may also deny your request if you ask us to correct information that:

- was not created by NM Medicaid
- is not part of the health information kept by NM Medicaid
- is correct and complete
- was created by a business agent whose records cannot be obtained.

Right to a Record of Information We Have Shared

NM Medicaid keeps a record of your health information that has been shared. You may ask for a copy of the record of information that has been shared by writing to the HIPAA Privacy Officer. The HIPAA Privacy Officer will write to you about the results of your request. You cannot ask for any information that was shared *before April 14, 2003*. NM Medicaid will give you one free copy per year. NM Medicaid may charge you for the copy if you ask for more than one copy in a 12-month period. If there is a charge, NM Medicaid will tell you what it is and if you do not want to pay, you can take back your request.

Right to Ask for Limits on Shared Health Information

You have the right to ask NM Medicaid to limit the health information about you that NM Medicaid shares with someone who is involved in your care or who pays for your care. For example, you could ask that NM Medicaid not use or share information about a treatment or prescription you received. NM Medicaid may not be able to agree to your request, for example, if required by law. If NM Medicaid does agree, NM Medicaid will do what you ask us to do unless the information is needed to provide you emergency treatment. To ask for limits or restrictions on your health information, you may ask for assistance from the HIPAA Privacy Officer. If you ask for limits or restrictions on your health information that may be at more than one location or if you have any questions about your information, you may write to the HIPAA Privacy Officer telling NM Medicaid:

- ·what information you want to limit and
- ·to whom you want the limits to apply (for example, to your spouse).

If you have asked to limit the health information NM Medicaid uses or shares and if NM Medicaid has agreed, you have the right to change your mind by writing to the HIPAA Privacy Officer.

Right to Request Private Communications

You have the right to ask that NM Medicaid communicate with you about your health information other than by mailing. You may also ask that NM Medicaid send communications to you about your health information to the address you choose. NM Medicaid will grant your request if possible.

Right to a Paper Copy of This Notice

You have the right to a paper copy of this notice at any time by writing the HIPAA Privacy Officer. You may also get a copy of this notice at our website. http://www.state.nm.us/hsd/mad

Complaints

If you believe NM Medicaid has violated your privacy rights, you may complain to the HIPAA Privacy Officer, or you may file a complaint with the Secretary of the United States Health and Human Services Department at **200 Independence Avenue, SW, Washington, DC 20201**. If you file a complaint, it will not be held against you or any member of your family.

Additional Information

If you have questions about this notice, or if you need more information, write to the HIPAA Privacy Officer at:

New Mexico Human Services Department
HIPAA Privacy Officer
P.O. Box 2348
Santa Fe, New Mexico 87504-2348

Information About This Notice

NM Medicaid may change this notice at any time. NM Medicaid will post a copy of the current notice in our main office. The notice will show the effective date on the first page. Each time you go to an HSD County Office, you may ask for a copy of our current Notice of Privacy Practices. If NM Medicaid changes the notice, NM Medicaid will send you a copy of the revised notice. The revised notice will be available at the HSD County Offices and on the NM Medicaid web site. www.state.nm.us/hsd/mad.

Alabama Medicaid Agency

501 Dexter Avenue
P.O. Box 5624
Montgomery, AL 36103-5624
www.medicaid.state.al.us
e-mail: almedicaid@medicaid.state.al.us
Telecommunication for the Deaf: 1-800-253-0799
1-800-362-1504 (334) 242-5000

Bob Riley
Governor

Mike Lewis
Acting Commissioner

April, 2003

There is a new law that protects you by keeping your medical information private. Read this notice to find out what you need to know!

Alabama Medicaid Agency

NOTICE OF PRIVACY PRACTICES - Effective April 14, 2003

FOR YOUR PROTECTION

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

You do not need to do anything with this notice or call Medicaid unless you have a problem or concern about the law. This notice is being sent to you so you will know about this new law.

MEDICAID PROMISES TO KEEP YOUR INFORMATION PRIVATE

Your health information is personal. However, there are times when Medicaid must share information with others to help you get the health care you need**.** When this must be done, Medicaid promises to follow the law so that your information is kept private. This notice tells you how Medicaid uses and shares information about you and what your rights are under the law. It tells the rules Medicaid must follow when using or sharing your information.

UNDERSTANDING THE TYPE OF INFORMATION THAT MAY BE SHARED

There are many good reasons for your information to be shared. If you apply for Medicaid through another agency (such as the Department of Human Resources or the Social Security Administration), that agency must send information about you to Medicaid. Information that may be sent to us includes your name, address, birth date, phone number, Social Security number, health insurance policies and health information. When your health care providers send claims to Medicaid for payment, the claims must include your diagnosis and the medical treatments you received. In order for Medicaid to pay for some medical treatments, your health care providers must also send extra medical information such as doctor's statements, x-rays, or lab test results.

HOW MEDICAID USES AND SHARES HEALTH CARE INFORMATION

Medicaid contracts with others outside of the agency for some services. For example, Medicaid contracts with a company to process the claims sent in by your health care provider. Medicaid may need to share some or all of your information with that company so your health care bills can be paid. When this is done, Medicaid requires that company to follow the law and keep all of your information safe.

Here are the ways Medicaid uses and shares your health information. For each category, we will say what we mean and give an example.

For Payment: Medicaid may use and share information about you so that it can pay for your health services. For example, when you get a Medicaid service, your health care provider asks Medicaid to pay for that service by filing a claim. On the claim form, your provider must identify you and say what your diagnoses and treatments are.

For Medical Treatment: Medicaid may use or share information about you to make sure that you get needed medical treatment or services. For example, your Patient 1st doctor may receive information about you from Medicaid.

To Run the Medicaid Program: Medicaid may use or share information about you to run the Medicaid program. For example, Medicaid may contract with a company that looks at hospital records to check on the quality of care given to you and the outcome of your care.

To Other Government Agencies Who Provide Benefits or Services To You: Medicaid may share information about you to other government agencies that are giving you benefits or services. For example, Medicaid may be asked to give the Alabama Department of Public Health information so you can qualify for benefits or services.

To Keep You Informed: Medicaid may use your information to send you materials to help you live a healthy life. For example, Medicaid may send you a brochure about an illness or condition you have or about your managed care choices.

To Check On Health Care Providers: Medicaid may share information about you to the government agencies that license and inspect medical facilities. An example is the Alabama Department of Public Health who inspects nursing homes.

For Research: Medicaid may share information about you for an approved research project. A review board must approve any research project and its rules to make sure your information is kept private.

As Required by Law: When requested, Medicaid will share information about you with the U.S. Department of Health and Human Services.

YOUR HEALTH INFORMATION

You have the following rights about the health information that Medicaid has about you:

- You have the right to see and get a copy of your health information with certain exceptions.
- You have the right to ask Medicaid to change health information that is incorrect or incomplete. Medicaid may deny your request in some cases.
- You have the right to ask what items and who Medicaid has shared your health information with after April 14, 2003.
- You have the right to ask that certain uses or disclosures of your health information be restricted. Medicaid is not legally required to agree with your request, but will agree if possible.
- You have the right to ask that Medicaid talk with you about your health in a way or at a place that will help you keep your health information private.

- You have the right to get a paper copy of this notice. You may ask Medicaid to give you another copy of this notice, or you may print a copy from Medicaid's web site, **www.medicaid.state.al.us**

MEDICAID'S REQUIREMENTS

Medicaid is required by law to:

- Keep your information private
- Give you this notice that tells the rules Medicaid must follow when using or sharing your information with others.
- Follow the terms of this notice.
- Except for the reasons given in this notice, Medicaid may not use or share any information about you unless you agree in writing. You may take away your permission at any time, in writing, except for the information that Medicaid disclosed before you stopped your permission. If you cannot give your permission due to an emergency, Medicaid may release the information if it is in your best interest. Medicaid must notify you as soon as possible after releasing the information.

In the future, Medicaid may change its privacy practices and may apply those changes to all health information we have. Should Medicaid's privacy practices change, Medicaid will mail a new notice to you within 60 days. Medicaid will also post the new notice on its web site, **www.medicaid.state.al.us**

TO FIND OUT MORE

If you have questions or would like to know more, you may call our Privacy Officer toll-free at 1-800-362-1504 or Telecommunication for the Deaf at 1-800-253-0799.

TO REPORT A PROBLEM

If you believe your privacy rights have been violated, you may:

- File a complaint with Medicaid by calling the Office of General Counsel toll-free at 1-800-362-1504 or Telecommunication for the Deaf: 1-800-253-0799 or by writing to the Office of General Counsel, Alabama Medicaid Agency, P.O. Box 5624, Montgomery, AL 36103-5624.
- File a complaint with the Secretary of Health and Human Services by writing to Secretary of Health and Human Services, 200 Independence Ave. SW, Washington, D.C. 20201. For additional information you may call toll-free 1-877-696-6775.
- File a grievance with the United States Office of Civil Rights by calling toll-free 1-866-OCR-PRIV (1-866-627-7748) or Telecommunication for the Deaf: 1-866-788-4989.

We will not get back at you for filing a complaint or grievance.

REMEMBER:

You do not need to do anything with this notice or call Medicaid unless you have a problem or concern about the law. This notice is being sent to you so you will know about this new law.

Por favor, llame por teléfono 1-800-362-1504 para esta información en español.

IMPORTANT NOTICE

There is a new law that protects you by keeping your medical information private. Read this notice to find out what you need to know!

Alabama Medicaid Agency
P.O. Box 5624
Montgomery, AL 36103

Jim Doyle
Governor

Helene Nelson Secretary

State of Wisconsin
Department of Health and Family Services

DIVISION OF HEALTH CARE FINANCING
WISCONSIN MEDICAID AND BADGERCARE
RECIPIENT SERVICES
6406 BRIDGE ROAD
MADISON WI 53784
Telephone: 800-362-3002
TTY: 800-362-3002
FAX: 608-221-8815
www.dhfs.state.wi.us/badgercare
www.dhfs.state.wi.us/medicaid

PHC 13040 (03/03)

Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

THIS NOTICE DOES NOT AFFECT YOUR BENEFITS OR ELIGIBILITY

Effective Date: April 14, 2003

This notice is being sent to enrollees of the following Medicaid (MA, Medical Assistance, T-19) programs including BadgerCare; Family Care; Healthy Start; Medical Assistance Purchase Plan (MAPP); Program for all Inclusive Care for the Elderly (PACE); Partnership; Community Options Program-Waiver; Community Integration Program II; Community Integration Program 1A; Community Integration Program 1B; Brain Injury Waiver; Community Supportive Living Arrangement.

Spanish –	Si necesita ayuda para traducir o entender este texto, por favor llame al teléfono 1-800-362-3002 (V/TTY)
Russian –	Если вам не всё понятно в этом документе, позвоните по телефону 1-800-362-3002 (V/TTY)
Hmong –	Yog xav tau kev pab txhais cov ntaub ntawv no kom koj totaub, hu rau 1-800-362-3002 (V/TTY)
Laotian –	ເພື່ອຊ່ວຍໃນການແປ ຫລື ເຂົ້າໃຈເນື້ອຫາໃນນີ້, ກະຣຸນາໂທຣະສັບຫາ 1-800-362-3002 (V/TTY)

PRIVACY RESPONSIBILITY

Wisconsin's Department of Health and Family Services (DHFS) Medicaid program is committed to protecting the privacy of your medical information. Your privacy is already protected under Medicaid and Wisconsin law. In addition, federal law now requires health plans, such as Medicaid, to protect your medical information and to let you know how your medical information may be used and released to others. This notice tells you what Medicaid may do with your medical information and what your privacy rights are under the law. Medical information described in this notice may include information about you that appears on enrollment, claims, or other records used to make decisions about your health care services.

If you are in an HMO or other managed care plan you may get a privacy notice from them describing their privacy policies, as well.

Medicaid Privacy responsibilities include:

- Protecting the privacy of any medical information created or received about you.
- Sending you this notice describing Medicaid's medical information privacy policies and the legal reason for those policies.
- Using or sharing medical information only as described in this notice.

- Sending you a new notice, if Medicaid privacy policies change.

WHEN YOUR MEDICAL INFORMATION MAY NOT BE USED

Medicaid will not use or disclose your medical information for any reason other than those described on page 2 of this notice, without your written authorization. You may withdraw an authorization at anytime by submitting a completed request form to the address listed in the "To Use Your Rights" section of this document. If you withdraw your authorization, Medicaid will no longer be able to use or disclose health information about you for those purposes covered by your written authorization. If authorization is withdrawn, Medicaid will be unable to take back any previous disclosures made with your authorization. In the event of an emergency, information may be released without your permission if, medically, it is in your best interest. You will be told as soon as possible after the information is released.

HOW YOUR MEDICAL INFORMATION IS USED OR DISCLOSED WITHOUT WRITTEN PERMISSION

Your medical information may be used or disclosed for treatment, payment, and health care operations, without your written permission. For examples of these functions, see below. Some services are provided through contracts with other state agencies or private companies. Some or all of your information may be disclosed, without written permission, to the other agency or company so they can do the job we have asked them to do. The other agency or company must also keep your information confidential.

Not all types of uses and releases are listed in this notice. Following are some common ways medical information is used or disclosed without written permission for treatment, payment, and health care operations. For each category we will explain what we mean and give an example.

Treatment – Medical information may be used or disclosed to make sure that needed medical treatment is received. For example, your medical information may be given to a pharmacist when you need a prescription filled.

Payment – Your medical information may be used and disclosed to others to bill and collect payment for the treatment and services you received. Medical information may also be shared with other government programs such as Worker's Compensation, Medicare, or private insurance to manage your benefits and payments. For example, your doctor sends a claim form to Medicaid for payment. This claim form includes information identifying you, your diagnosis, and treatment.

Health Care Operations – Medical information may be used or disclosed in order to carry out necessary benefit or service related activities. For example, these activities may include quality and cost improvement functions such as conducting or arranging for medical review, quality improvement studies, audit services, management, or general administration.

Other ways your medical information may be used or disclosed without written permission include:

Informing You – Your information may be used in order to let you know about health and wellbeing services. Examples of this may include contacting you for appointment reminders, telling you about treatment alternatives or giving you information about health related benefits or services.

Public Health – Information may be reported to a public health authority or other appropriate government authority authorized by law to collect or receive information to help prevent or control disease, injury, disability, infection exposure, and child abuse or family violence. The authorities could include local, state or federal governmental agencies. For example, your medical information may be shared if you are exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease.

Health Oversight Activities – Information may be shared with other government agencies to provide oversight of the health care system. Examples of this include licensing and inspecting of medical facilities, audits or other proceedings related to oversight of the health care system.

Coroners, Medical Examiners, or Funeral Directors – Your medical information may be released to a medical examiner, coroner, or funeral director as needed to carry out duties authorized by law. For example, this may be necessary to identify a deceased person.

For Organ Donations – If you are an organ donor, information may be given to the organization that finds or transplants organs for the purpose of an organ transplantation or donation.

Worker's Compensation – Your information may be disclosed to comply with Worker's Compensation or similar laws.

Public Safety – Your information may be disclosed to prevent or lessen a serious threat to your health or safety, to another person, or the general public.

Specialized Government Functions – Your information may be used or disclosed to the government for specialized government functions. For example, your information may be disclosed to the appropriate military authorities if you are or have been a member of the U.S. armed forces.

Law Enforcement – Your information may be disclosed to fulfill a requirement by law or law enforcement agencies. As an example, medical information may be used to identify or locate a missing person.

Court or Other Hearings – Your information may be disclosed to comply with a court order.

Required by Law – In addition to the ways listed above in which your medical information may be disclosed, Medicaid may share your information when required by law.

YOUR MEDICAL INFORMATION PRIVACY RIGHTS
You have the right to:

See or Copy Your Medical Information – To see or copy enrollment, claim, or other records used to make decisions about your health plan services, send in a completed request form to the address listed in the "To Use Your Rights" section of this document. Medicaid will not include information prepared for legal actions or proceedings. A fee may be charged to cover the processing cost of your request.

Correct Information You Believe to be Incorrect or Incomplete – To ask for a correction to enrollment, claim, or other records used to make decisions about your health plan services, send in a completed request form, to the address listed in the "To Use Your Rights" section of this document. Your request will be reviewed. If the change is not allowed, you will be told in writing why and how you can disagree.

Request a List of Who Was Given Your Information and Why – Such a list will not include information used for payment of your treatment, for our health care operations, or for any information already provided on a previous list, national security, law enforcement/corrections, or certain health oversight activities. Information given to you will include the release date, the name of the person or organization, a brief description, and the reason for the disclosure. The list will not include dates before April 14, 2003, or go back more than six years. Medicaid will provide one list

per year free of charge. There may be a charge for additional lists. To obtain such a list, send a completed request form to the address listed in the "To Use Your Rights" section of this document.

Request Restrictions on Using or Sharing Your Medical Information For Treatment, Payment or Health Care Operations – You have the right to request restrictions on how your information is used or disclosed. Medicaid is not required to agree to your requested restrictions. After sending a completed request form to the address listed below, your request will be evaluated. We will let you know if we can comply with the restriction or not.

Request That You Be Informed About Your Health in a Way or at a Location That Will Help Keep Your Information Private – You have the right to request how and where Medicaid contacts you about your medical information. After sending a completed request form to the address listed in the "To Use Your Rights" section of this document, your request will be evaluated and Medicaid will let you know if it can be done.

Receive a Paper Copy of This Notice – If you received this notice on the DHFS Internet site or by electronic mail (e-mail), you have the right to ask for and receive a paper copy of this notice by calling Recipient Services at (800) 362-3002.

TO USE YOUR RIGHTS
To use any of these rights or to obtain a copy of the correct privacy request form for inspecting, copying, amending, making restrictions, or obtaining an accounting of your health information, call Recipient Services at (800) 362-3002. Send your completed privacy request form to the DHCF Privacy Officer, Wisconsin Medicaid and BadgerCare Recipient Services, P.O. Box 6678, Madison, WI 53716-0678.

CHANGES TO THIS NOTICE
This notice may be changed or amended at any time. The changes are effective for all medical information including what is on file. A new notice will be sent to you when policy changes are made. Wisconsin Medicaid will also post the new notice on the Recipient page of the Internet at http://www.dhfs.state.wi.us/medicaid/. **Until a change happens, Medicaid will comply with the current version of this Notice.**

FOR MORE INFORMATION
If you have questions about any part of this notice or would like additional information about our privacy practices, please write to Wisconsin Medicaid and BadgerCare Recipient Services, P.O. Box 6678, Madison, WI 53716-0678, or telephone (800) 362-3002 (V/TTY).

COMPLAINTS
You will not lose benefits or eligibility or otherwise be retaliated against for filing a complaint. Please send written complaints about this notice, about how Medicaid handles your medical information, or if you believe your privacy rights have been violated to the DHCF Privacy Officer at Wisconsin Medicaid and BadgerCare Recipient Services, P.O. Box 6678, Madison, WI 53716-0678.

You may also file a complaint directly with the Secretary of the U.S. Department of Health and Human Services by writing to the Privacy Officer, Office of Civil Rights, Department of Health and Human Services, 200 Independence Avenue SW, Washington, D.C. 20201. For additional information, call (866) 627-7748.

If you have no questions about this notice, you do not have to do anything. Remember this notice has no effect on your health care benefits or eligibility.