B. Disclaimer

{Comment: The purpose of the disclaimer is to attempt to avoid having a violation of these policies become the basis for a lawsuit. At the time this Resource Manual is written, it is not clear that this will be effective, but it certainly does not hurt to include it.}

All of the policies and procedures contained or referred to in these Privacy and Security Policies, or that may be added or otherwise established by XYZ in the future, represent the policies established by XYZ for the members of its workforce in relation to the particular subject addressed by the policy. It is the intention of XYZ that these Privacy and Security Policies be used by its employees, and other members of its workforce, in meeting their responsibilities to XYZ. Violation of a policy can be the basis for discipline or termination of employment; however, because these Privacy and Security Policies relate to the establishment and maintenance of high standards of performance, under no circumstances shall any policy or procedure be interpreted or construed as establishing a minimum standard, or any evidence of a minimum standard, of the safety, due care, or any other obligation which may be owed by XYZ, its employees, or its agents to another person.

II. PROTECTED HEALTH INFORMATION

A. What is "Protected Health Information?"

{Comment: Defining "protected health information" is important because that is the information these policies apply to. What is stated in this section is essentially from the Privacy Rule. The Privacy Rule excludes from the definition of "protected health information" records: (a) covered by the Education Rights and Privacy Act, 20 U.S.C. 1232g; (b) certain records maintained by an education agency or institution on students who are 18 years of age or older that are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional;(c) employment records held by a covered entity in its role as an employer, and, (d) regarding a person who has been deceased for more than 50 years. The first two are not important to most health care providers and, consequently, are not included in this template. However, those exclusions could be relevant to providers providing services where records are then maintained by an educational institution.}

"Protected health information" is any health information maintained by XYZ that is individually identifiable except: (a) employment records held by XYZ in its role as an employer; and, (b) information regarding a person who has been deceased for more than fifty (50) years. *{45 CFR §160.103}*

"Individually identifiable health information" means any health information, including genetic information, whether oral or recorded in any form or medium, including demographic information collected from an individual, that:

1. Is created or received by a health care provider, a health plan, employer, or health care clearinghouse;

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and,

3. That identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. *{45 CFR §160.103}*

{Comment: The following paragraph is an assumption on my part, but I suspect it will be true for many providers. Do not say it unless it is correct for your organization.}

All health information maintained by XYZ is individually identifiable unless and until it is de-identified as stated in Section II.B, below.

B. De-Identification of Health Information *{45 CFR §164.514}*

{"De-identification" is the process of removing all identifiers from individually identifiable health information so it is no longer "individually identifiable." Of course, once this is done, the information may not be useful to you.}

1. De-Identification *{45 CFR §164.514(a)}*

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

2. Requirements for De-Identification *{45 CFR §164.514(b)}*

{Comment: What is stated in the following paragraph is not required by the Privacy Rule, but it seems like a good idea to have someone with knowledge of the Privacy Rule confirm that information has, indeed, been de-identified. It does not have to be the Privacy Officer. You could choose someone else who is knowledgeable concerning HIPAA's requirements, such

as the Security Officer.}

Before any member of XYZ's workforce treats any information as being de-identified, it must be submitted to the Privacy Officer. Whether or not health information has been de-identified will be determined by the Privacy Officer.

{Comment: The two conditions stated below are established by the Privacy Rule. You cannot change them. I doubt that many providers will use Condition 1 due to its expense, but it seemed appropriate to include to be sure you are aware of it.}

The Privacy Officer may find that health information has been de-identified only if one of the following two conditions are met:

a. Condition 1: Statistical and Scientific Principles *{45 CFR §164.514(b)((1)}*

A person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually indentifiable:

(1) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject to the information; and,

(2) Documents the methods and results of the analysis that justify such determination. Such documentation shall be in accordance with the requirements stated in Section IV.N (see, Page II-22) and Section IV.O (see, Page II-23) of these Privacy and Security Policies.

b. Condition 2: Removal of Identifiers *{45 CFR §164.514(b)(2)}*

The following identifiers of the individual or of relatives, employers, or household members of the individual are removed and XYZ does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information:

(1) Names;

(2) All geographic subdivisions smaller than a State, includ-

ing street addresses, 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 people is 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) Telephone 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, except as permitted by Section II.B.3 (see, Page II-6) of these Privacy and Security Policies.

3. **Requirements for Re-Identification** *{45 CFR §164.514(c)}*

A code or other means of record identification may be assigned to allow information de-identified to be re-identified by XYZ provided:

a. The code or other means of record identification shall not be derived from or related to information about the individual and shall not otherwise be capable of being translated so as to identify the individual; and,

b. The code or other means of record identification shall not be used or disclosed for any other purpose and the mechanism for re-identification shall not be disclosed.

{Comment: In the following paragraph, it does not have to be the Privacy Officer. You can name someone else if you want.}

Whether or not information shall be coded for re-identification and be re-identified shall be determined by the Privacy Officer. If information is re-identified, the Privacy Officer shall oversee the process of doing so.

III. ELECTRONIC PROTECTED HEALTH INFORMATION

"Electronic Protected Health Information" is any protected health information maintained by XYZ that is transmitted by electronic media or maintained in electronic media. *{45 CFR §160.103}*

"Electronic Media" means:

"(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, Extranet or Intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission. *[45 CFR §160.103]*

IV. ADMINISTRATIVE POLICIES

{Comment: This Section IV, VIII.D.1.b.(4) reflects specific administrative requirements established by the HIPAA Privacy and Security Rules as well as several other matters that I felt were appropriate to include. Whether or not the provision is required by the Privacy or Security Rules is stated in the comments below.}

A. Organizational Policies

{Comment: This section concerning organizational policies is included simply to alert you to each of the following four kinds of arrangements. If you fall within one or more of these, you will need to adapt the wording of the template policies to reflect your situation. If you do not fall within any of these arrangements, this entire Section IV.A can be deleted. Legal advice should be sought in determining how these arrangements may impact your organization and how you want to proceed.}

1. Affiliated Covered Entity *{45 CFR §164.103 & §164.105(b)}*

{Comment 1: Legally separate covered entities that are under common ownership or control (as defined in the Privacy Rule, see, 45 CFR §164.103), may elect to designate themselves (including any health care component of such covered entity) as an "affiliated covered entity." This permits having one set of privacy policies, one Notice of Privacy practices, etc., rather than different ones for each entity. It may make things easier administratively. You need to look at your own situation to decide what is best for you. Becoming an affiliated covered entity requires an affirmative election to be one and that designation must be documented. See, the Chapter"Affiliated Covered Entities Versus Organized Health Care Arrangements" in Part I of this Resource Manual.

Examples of arrangements that could become affiliated covered entities are: a physician's practice and another health care provider that the physician owns; two home health agencies under common ownership.}