



225 Varick Street • New York, NY 10014 • (212) 243-1313

Fax: (212) 675-0286 • E-mail: lacinfo@lac.org

**NEW YORK STATE’S HIV CONFIDENTIALITY LAW
AND
THE FEDERAL HEALTH INSURANCE PORTABILITY
AND ACCOUNTABILITY ACT (HIPAA)**

A Summary For HIV/AIDS Providers

(March 2008)

TABLE OF CONTENTS

I. INTRODUCTION 1

 A. What is New York State’s HIV Confidentiality and Testing Law?..... 1

 B. What is HIPAA? 2

 C. HIPAA's Relationship with State Law..... 3

 D. Other Confidentiality Laws 4

II. WHO MUST COMPLY 4

 A. Who Must Comply with Article 27-F..... 4

 B. Who Must Comply with HIPAA 5

 C. Are You Covered by HIPAA? 7

 D. What To Do If You Are Covered – And If You Are Not 8

III. GENERAL RULE: NO DISCLOSURE..... 8

 A. Article 27-F's General Rule 8

 B. HIPAA'S General Rule 9

IV. EXCEPTIONS TO THE "NO DISCLOSURE" RULES..... 10

 A. Consent 10

B.	Disclosures to Protected Individuals Themselves.....	12
C.	Communications Among Agency Staff.....	12
D.	Health Care Provider Rule.....	13
E.	Physicians' Disclosures about Minors and Incompetent Adults.....	14
F.	HIV/AIDS Case Reporting.....	15
G.	Contact (Partner) Reporting and Notification.....	15
H.	Newborn Testing.....	16
I.	Foster Care and Adoption.....	16
J.	Court Orders.....	18
K.	Insurers.....	18
L.	Program Evaluation.....	19
M.	Convicted and Certain Accused Sex Offenders.....	19
N.	Occupational Exposure.....	20
O.	Disclosures for Medical Education, Research, Therapy or Transplantation.....	20
P.	Employees within Certain Criminal Justice Agencies.....	21
Q.	Public Health Officials.....	22
R.	Child Abuse/Neglect and Elder Abuse/Neglect.....	22
S.	Business Associate Agreements.....	22
V.	HIPAA'S ADMINISTRATIVE REQUIREMENTS.....	22
VI.	PATIENT RIGHTS.....	25
A.	Right to an Accounting of Disclosures.....	25
B.	Right of Access to Health Records.....	26
C.	Right to Request an Amendment to Health Records.....	28
D.	Right to Receive Confidential Communications.....	30
E.	Right to Request Restrictions on Use or Disclosure.....	30
VII.	ENFORCEMENT AND PENALTIES.....	31
A.	Article 27-F.....	31
B.	HIPAA.....	31
C.	Where to find more guidance.....	32



225 Varick Street • New York, NY 10014 • (212) 243-1313

Fax: (212) 675-0286 • E-mail: lacinfo@lac.org

**NEW YORK STATE’S HIV CONFIDENTIALITY LAW
AND
THE FEDERAL HEALTH INSURANCE PORTABILITY
AND ACCOUNTABILITY ACT (HIPAA)**

A Summary For HIV/AIDS Providers

I. INTRODUCTION

A. What is New York State’s HIV Confidentiality and Testing Law?

New York State has a specific law that governs HIV confidentiality and testing: **Article 27-F of the Public Health Law**, sections 2780-2787 ("Article 27-F"). The State’s HIV Reporting and Partner Notification Law also contains confidentiality rules governing HIV case reporting and partner notification activities (Public Health Law Article 21, Title II, sections 2130-2139).¹ This Summary refers to this set of laws as “Article 27-F” or the “State HIV law.”

Article 27-F’s basic rules are:

- **Testing:** generally prohibits anyone from performing HIV tests without informed written consent. A few exceptions allow testing without consent, including of newborns and accused or convicted sex offenders.
- **Confidentiality:** generally prohibits health and social service providers and others (who receive HIV related information about someone with his or her special written consent) from disclosing HIV related information about a “protected individual” – a person who has had an HIV test or has been diagnosed with HIV infection, HIV related illness or AIDS – and his or her sexual or needle-sharing “contacts.” This rule has a number of exceptions, discussed below.

This Summary focuses on Article 27-F’s rules concerning **confidentiality and disclosure of HIV related information**, not HIV testing.

¹ The section references throughout this Summary refer to the Public Health Law, unless otherwise noted.

Why is there a special HIV confidentiality law in New York? The Legislature decided that the confidentiality of HIV related information about individuals must be strictly protected in order to:

- encourage persons to voluntarily learn their HIV status, seek appropriate treatment, and change behavior to avoid acquiring or transmitting HIV, and
- reduce the risk of discrimination and other harms caused by unauthorized, unnecessary disclosures of HIV related information.

Various state agencies have issued regulations implementing Article 27-F. The New York State Department of Health ("DOH") is the "lead agency" on Article 27-F, and its regulations implementing the law are at 10 NYCRR Part 63. The regulations for alcohol and drug treatment programs are at 14 NYCRR Part 309 (alcohol treatment rules) and 14 NYCRR Part 1070, 1072 (drug treatment rules). Other State agencies' Article 27-F regulations apply to providers funded or regulated by those agencies.

B. What is HIPAA?

HIPAA is a federal health privacy law. In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §1320d *et seq.* In October 2002, the U.S. Department of Health and Human Services ("HHS"), the "lead agency" charged with interpreting and enforcing HIPAA, issued final regulations implementing HIPAA's privacy standards, 45 C.F.R. Parts 160 and 164² – known as the HIPAA Privacy Rule. HIPAA's effective date was **April 14, 2003**.

Generally speaking, HIPAA:

- establishes a federal floor of safeguards to protect the privacy of medical records and other personal health information ("PHI"), and
- applies to personal health information which is transmitted in electronic, written, or oral form.

While HIPAA does not supersede Article 27-F, it does impose some additional requirements on most health care providers.

² Other parts of the HIPAA regulations set forth specific security and electronic standards which require those covered by the regulations to have security controls in place to protect confidential information when it is electronically stored and transmitted. See 45 C.F.R. Parts 142 and 162. While a detailed discussion of these regulations is beyond the scope of this summary, providers should consult with their technical and computer support staff to assure the appropriate security measures are in place.

C. HIPAA's Relationship with State Law

The HIPAA regulations have a very specific set of factors that should be considered when determining how HIPAA affects state laws that govern health privacy such as Article 27-F. The general rule is that HIPAA preempts, or overrides, any “contrary” state law provision. 45 C.F.R. § 160.203.

Contrary means that a covered entity would “find it impossible to comply” with both the state and federal requirements; or that the state law “stands as an obstacle” to achieving HIPAA’s purposes and objectives. 45 C.F.R. § 160.202.

However, HIPAA does not preempt a state law when one of the following conditions is met:

1. The state law relates to privacy AND is “more stringent” than the HIPAA provision.

A more stringent state law is one that:

- Prohibits or restricts a use or disclosure of personal health information (PHI) permitted by HIPAA (unless the disclosure is to HHS to determine compliance, or to the individual who is the subject of the protected information, in which case HIPAA does preempt);
- Gives an individual greater rights to access or to amend his/her own health records;
- Provides more information to an individual regarding a use or disclosure of PHI, or rights and remedies;
- Provides a narrower scope or duration, or affords increased privacy protections, for express legal permissions for use or disclosure of PHI, or reduces the coercive effect of such permissions;
- Provides for the retention or reporting of more detailed information in an accounting of disclosures;
- Provides greater privacy protection for the individual who is the subject of protected information.

45 C.F.R. § 160.202

2. The Secretary of Health and Human Services (HHS) has determined that the state law is necessary:

- to prevent fraud or abuse related to providing health care;
- to ensure appropriate regulation of insurance and health plans;
- for state reporting on health care delivery or costs; or
- to serve a compelling need related to public health, safety, or welfare.

45 C.F.R. § 160.203

3. The state law provides for the reporting of, among other things, suspected child abuse, or for the conduct of public health surveillance, investigation, or intervention. 45 C.F.R. §160.203; or
4. The principal purpose of the state law is the regulation of the manufacture, sale, or control of any controlled substance. 45 C.F.R. § 160.203.

Generally, Article 27-F is a "**more stringent**" state law under the first test described above, and therefore is **not** preempted by HIPAA. The relationship between HIPAA and Article 27-F is discussed in more detail below.

D. Are There Other Confidentiality Laws that Providers Have to Know?

Many providers must comply with other federal or New York State laws that protect the confidentiality of information about their patients/clients. Providers who are subject to these other confidentiality laws and are also "covered entities" under HIPAA (see Part II. B. and Part II. C. below) need to learn how those laws and HIPAA relate to each other, and how they can comply with all the confidentiality laws, federal and state, that apply to them.

- Drug and alcohol treatment providers must also comply with the federal law and regulations protecting the confidentiality of drug or alcohol patient records (42 U.S.C. § 290dd-2, 42 C.F.R. Part 2).
- Other New York State laws that protect the privacy of health information and/or impose confidentiality obligations on many health and mental health providers include those protecting the confidentiality of:
 - medical records and information, generally
 - mental health information
 - information concerning treatment for specific health problems, including sexually transmitted diseases.
- Professional licensing rules impose obligations on licensed medical (and other) professionals (including social workers) to maintain client confidences.

II. WHO MUST COMPLY

A. Who Must Comply with Article 27-F: Health and Social Service Providers, and Certain Others

Who is covered. Article 27-F's confidentiality requirements apply to any person (including agencies and their paid or volunteer staff) who receives HIV related information about a protected individual –

- while providing a "health or social service" as defined in Article 27-F (§§ 2780.8, 2782.1), or
- pursuant to a proper written consent form (release) authorizing the disclosure of HIV related information (§§ 2780.9, 2782.1).

Article 27-F also applies to NY State and local governmental agencies, when they –

- provide, supervise or monitor covered "health or social services," or
- obtain HIV related information pursuant to Article 27-F (§§ 2782.6, 2786).

Finally, Article 27-F's confidentiality requirements apply to community-based organizations and service providers funded by the NYS AIDS Institute.

Who is not covered. Article 27-F's confidentiality requirements generally do not apply to –

- federal governmental agencies, including the military and federal prisons (since it is a state law, federal agencies do not have to comply);
- protected individuals themselves and, if they lack "capacity to consent" to their own health care, the persons authorized by law to provide such consent (e.g., parents/legal guardians) (§ 2782.3(a), (b));
- a protected individual's friends, relatives or others who get HIV related information about a protected individual in ways other than through consent or while providing the person with a covered "health or social service" (§ 2782.1);
- foster and prospective adoptive parents, in limited circumstances (§§ 2782.3(c), (d));
- courts (not defined as "persons" subject to 27-F, § 2780.11); and
- insurers (§§ 2782.1(i), (j); 2784); Insurance Law (§ 2611) (see Part IV.K).

B. Who Must Comply with HIPAA: Certain Health Care Providers (Only)

Who is covered. Health care providers, health plans and health care clearinghouses are "covered entities" who must comply with HIPAA *if* they transmit health information *electronically* in connection with certain health care transactions. 45 C.F.R. § 160.102.

Health care provider is any individual or entity that furnishes, bills, or is paid for health care in the normal course of business. 45 C.F.R. § 160.103.

Health care includes preventive, diagnostic, therapeutic, counseling, and assessment services with respect to the physical or mental condition of an individual. 45 C.F.R. § 160.103.

A health care provider covered by Article 27-F is also covered by HIPAA only if it transmits health information *electronically* in connection with a covered electronic transaction described below. 45 C.F.R. § 160.102(a)(3).

Covered electronic transactions include the following financial or administrative activities:

- processing claims
- payment and remittance
- coordination of benefits
- claim status
- enrollment and disenrollment in a health plan
- health plan eligibility
- health plan premium payments
- referral certification and authorization
- first report of injury
- health claims attachments and
- other transactions HHS may prescribe.

45 C.F.R. § 160.103

If a health care provider does not transmit health-related information electronically, then it is NOT a covered entity under HIPAA. However, if the provider begins to transmit health-related information electronically at any point, it will then be subject to HIPAA. 45 C.F.R. § 160.102. Although only those health care providers that transmit information electronically are covered by HIPAA, once a provider makes an electronic transmission, *all transactions*, whether paper, oral, or electronic, are covered by the regulations. 45 C.F.R. § 164.501.

Who is probably not covered. Social service providers and others covered by Article 27-F are probably NOT covered by HIPAA *unless* they provide one of the health care related services included in the above definition, *and* engage in a covered electronic transaction.

Hybrid entities: HIPAA allows an organization whose business activities include both covered and non-covered functions to designate itself as a "hybrid entity." There are many organizations that provide health care in addition to other social and community services. For example, an organization may offer HIV counseling and testing services, or operate a health clinic, and also perform budget or vocational counseling, run a shelter or food pantry, or provide other social services. Under HIPAA, this type of multi-service organization may want to designate itself as a "hybrid entity." 45 C.F.R. § 164.504(u).

A hybrid entity must designate its health care components, including any component that would meet HIPAA's definition of covered entity if it were a separate legal entity. Designated

health care components are subject to HIPAA and the organization must implement all appropriate policies and procedures to ensure that component's compliance with HIPAA. (These are described in Parts V and VI.) The other, non-health care components of the organization would not be required to comply with HIPAA. However, if they receive protected HIV related information they will be subject to Article 27-F.

C. Are You Covered by HIPAA?

Those who are, and are not, covered “health care providers.” Here are examples of the types of organizations who generally will be considered health care providers subject to HIPAA (assuming they conduct covered transactions electronically), and those that generally will not be considered health care providers subject to HIPAA (regardless of whether they conduct covered transactions electronically).

Covered by HIPAA

Hospitals
 Clinics
 Doctors’ offices
 Home health care providers
 Nursing homes
 Drug and alcohol programs
 Medicaid offices
 Mental health professionals
 HIV counseling and testing providers

Not Covered by HIPAA

Laboratories/testing facilities
 Schools
 Foster care agencies
 Public assistance offices
 Housing and shelter services
 Day care programs
 Correctional facilities
 Courts
 Law enforcement, probation & parole
 Budget counseling programs
 Employment/vocational counseling programs
 Case management programs (including COBRA case mgt. programs)³

Remember: even if your organization is listed as not covered by HIPAA, it may be a hybrid entity if it has a health care component.

Covered “health plans.” The State Department of Health (DOH) has determined that the following units and programs within the DOH are health plans that are covered by and must comply with HIPAA:

³ While case management providers coordinate many services, including health care, they are not “health care providers” as defined by HIPAA. HHS has stated that simply billing for certain services does not bring those services under HIPAA. Because there has been some confusion about this within and outside the State Department of Health (DOH), the Legal Action Center asked for (but has not yet received) an opinion from HHS clarifying that case management programs are not “covered entities” under HIPAA. DOH Medicaid staff have decided that all agencies that bill Medicaid must, however, comply with HIPAA’s transaction code set and other security regulations (see 45 C.F.R. Parts 142 and 162) when submitting claims, because Medicaid is a covered health plan and its system must comply with HIPAA.

- (1) the Medicaid program (including Medicaid Managed Care, Family Health Plus, Family Planning Extension, Community Health Worker Programs, and the Medicaid component of Health Care Financing);
- (2) Elderly Pharmaceutical Insurance Coverage ("EPIC") program,
- (3) Cystic Fibrosis program,
- (4) HIV uninsured programs,
- (5) Indian Health Programs, and
- (6) the Child Health Insurance Program ("CHIP").

These programs must also comply with Article 27-F in dealing with or disclosing any confidential HIV related information protected by the state's HIV law.

D. What To Do If You Are Covered – And If You Are Not

If your organization is covered by HIPAA as well as Article 27-F, then it must:

- Put in place the **privacy policies and procedures** and **administrative requirements** explained below in Part V;
- Ensure that patients/clients are afforded the **patient rights** explained below in Part VI; and
- **Continue to comply with Article 27-F** in handling and disclosing any confidential HIV related information – while also understanding how HIPAA relates to Article 27-F and the few ways in which HIPAA affects Article 27-F's basic rules (as explained below in Parts III and IV).

If your organization is covered by Article 27-F but not by HIPAA, then it:

- Must **continue complying with Article 27-F** in handling and disclosing any confidential HIV related information (as explained below in Parts III and IV); and
- Should **be aware** that other providers, including health care providers and health plans, may now have to comply with HIPAA, as well as Article 27-F – and understand how that may affect the way they operate, including when they deal with your organization or your clients.

III. GENERAL RULE: NO DISCLOSURE

A. Article 27-F's General Rule: No Disclosure of HIV Related Information

Article 27-F prohibits covered persons from disclosing any “confidential HIV related information” about a “protected individual” except (1) with special, proper, written consent, or

(2) as otherwise permitted under one of the law's exceptions (§ 2782). This includes disclosures made orally as well as written information (§ 2782.1).

Confidential HIV related information means information that does or reasonably could reveal that someone has been tested for or diagnosed with HIV or a related condition. This includes information that someone (1) had an HIV test (even if the results were negative), (2) has HIV infection, HIV related illness or AIDS, (3) has an HIV related condition (e.g., PCP pneumonia), or (4) takes medications specific to HIV disease (e.g., AZT or protease inhibitors) (§ 2780.7).

Article 27-F shields HIV related information about protected individuals (people who have had an HIV related test or who have been diagnosed with HIV, HIV related illness or AIDS) and their contacts (identified spouse, sex partner or needle-sharing partner) (§§ 2780.6, 2780.10).

B. HIPAA'S Privacy Rule: No Disclosure of Protected Health Information

Under HIPAA's general rule, a covered entity may not use or disclose protected health information except as permitted or required by the regulations. 45 C.F.R. § 164.502(a).

- Use means to share, employ, apply, utilize, examine, or analyze individually identifiable health information *within* an entity. 45 C.F.R. § 164.501.
- Disclose means the release, transfer, provision of access to or divulging in any other manner of information *outside* the entity. 45 C.F.R. § 164.501.
- HIPAA protects personal health information (PHI), which means any health related information which identifies an individual. 45 C.F.R. §164.501.
- Protected health information includes any information, whether oral or recorded, that is:

Created or received by a health care provider, health plan, public health authority, employer, school, life insurer, or health care clearinghouse,

AND

Related to the past, present, or future physical or mental health of an individual, including the provision of or payment for an individual's care.

45 C.F.R. §160.103.

Health information which does not identify an individual is NOT protected. A covered entity may de-identify health information by removing any identifying data, and the information would then not be protected by HIPAA. 45 C.F.R. §§ 164.502(d), 164.514(a), (b).

Protected information does NOT include education records covered by the Family Educational Right and Privacy Act (FERPA) and employment records held by a covered entity in its role as employer. 45 C.F.R. § 164.501.

IV. EXCEPTIONS TO THE "NO DISCLOSURE" RULES

Article 27-F authorizes confidential HIV related information to be disclosed with an individual's proper written consent and, in certain circumstances, without consent. HIPAA too allows the personal health information it protects, including HIV related information, to be disclosed with proper consent and, in specified circumstances, without consent.

The following sections summarize these exceptions allowing disclosure – and explain whether and how HIPAA affects or changes Article 27-F's rules in any way.

A. Consent

Consent Forms and General Requirements. Under **both Article 27-F and HIPAA**, HIV related information can be disclosed if the protected person signs a proper written consent form, which HIPAA calls an "authorization." There are special rules regarding these consent forms:

1. Must be voluntary and revocable at any time.
2. Must be in proper form, with all required elements.

Article 27-F requires the following elements to be included in the consent:

- specific authorization to disclose HIV related information (general authorization for release of medical or other information not sufficient);
- name of individual whose HIV related information will be released;
- name of person/provider authorized to make disclosure;
- name of recipient (person/provider);
- purpose of disclosure;
- date;
- time period during which consent is effective;
- signature (of protected individual, if has capacity for consent; or if does not, then of person authorized to consent to health care for protected individual).

HIPAA Impact. HIPAA requires consent forms to contain two additional elements:

- An explanation of the patient's right to revoke the authorization *in writing* and either a statement of the exceptions to the right to revoke, OR if the exceptions are included in the program's notice of patients' privacy rights (explained below in Part VI), a reference to that notice.

45 C.F.R. § 164.508(c)(2)(i).

- A statement of the provider’s ability to condition treatment, payment, enrollment, or eligibility for benefits on the consent. This must state either that the program may not condition these services on the patient signing the consent OR the consequences for refusing to sign the consent in those circumstances where the program can condition these services on the patient’s signing the authorization.

45 C.F.R. § 164.508(c)(2)(ii).

3. Must be on a form created or approved by the State Department of Health.
4. Every disclosure must be accompanied by a “notice prohibiting redisclosure,” which informs the recipient that it is now bound by Article 27-F and may not redisclose the HIV related information without authorization (§ 2780.9).

A sample consent form developed by the New York State Department of Health and containing all elements required under both Article 27-F and HIPAA is attached to this Summary. See the *HIPPA Compliant Authorization for Release of Medical Information and Confidential HIV Related Information* (DOH-2557 (8/05)).

A sample notice prohibiting redisclosure is also attached. See the *Notice Prohibiting Disclosure of Confidential Information*.

Capacity to Consent. There is no minimum age requirement regarding who may sign a consent form. Any person who has “capacity to consent” has the right to decide whether to authorize disclosures of HIV related information about him/herself. The test for capacity to consent is whether the individual has the ability, without regard to age, to (1) understand and appreciate the nature and consequences of the proposed disclosure, and (2) make an informed decision about whether to not to permit it. (§ 2780.5).

Conditioning Treatment on Consent to Disclosure. HIPAA prohibits covered entities from conditioning the provision of treatment on a patient’s consent to disclosures except in some *limited* circumstances. 45 C.F.R. § 164.508(b)(4).

- HIPAA’s limited exception allows conditioning treatment on consent when treatment is solely for the purpose of providing information to a third party.
- Agencies that do not fall under HIPAA can condition their services on obtaining consent.

The “Minimum Necessary” Rule. HIPAA requires covered entities to make reasonable efforts to limit the information to “the minimum necessary to accomplish the intended purpose” when *using, disclosing, or requesting* protected health information. 45 C.F.R. § 164.502(b)(1). This minimum necessary standard does not apply to disclosures or requests by a health care provider for treatment, uses or disclosures made pursuant to a consent (which HIPAA calls an “authorization”), disclosures made to HHS for compliance and enforcement, disclosures made to

the patient him or herself, uses or disclosures required by law, or uses or disclosures required for compliance with the regulations. 45 C.F.R. § 164.502(b)(2).

Revocation of Consent. Both Article 27-F and HIPAA permit an individual to change his or her mind and revoke consent at any time and for any reason. While HIPAA requires revocation to be done in writing, Article 27-F does not have such a requirement. The Legal Action Center believes that this is another example of Article 27-F being "more stringent" under the test described above in Part I.D (because it "affords increased privacy protections for express legal permissions for use or disclosure"). Therefore, providers covered by Article 27-F should continue to honor oral revocation.

Miscellaneous. Effective April 14, 2003, providers covered by HIPAA must provide patients with copies of all authorizations which the patient signs. 45 C.F.R. § 164.508(c)(4). Providers may continue to disclose information that is created or received prior to April 14, 2003, pursuant to a consent form obtained prior to that date. 45 C.F.R. § 164.532(b).

B. Disclosures to Protected Individuals Themselves

Under Article 27-F, no consent is needed for communications with protected individuals (who have capacity to consent). For example, a provider may give John HIV related information about John without first obtaining John's written consent for the disclosure. If John does not have capacity to consent to his own health care, then the provider may give the information to the person who is legally authorized to consent to John's health care (§ 2782.1(a)).

No change under HIPAA. This is consistent with HIPAA. See Part VII.B below, which discusses HIPAA's requirements for providing a patient with access to his or her own records.

C. Communications Among Agency Staff

Both Article 27-F and HIPAA permit staff members of a health care provider to have access to and share patient related information without consent, as long as certain limitations are met. (The same standard applies to social services and other providers covered by Article 27-F but not by HIPAA.)

HIPAA requires covered entities to limit to the "minimum necessary" those staff members who may have access to patient information. Article 27-F has a similar "need-to-know" requirement. Under both laws, staff members may have access if they:

- are allowed access to patient/client records in the ordinary course of business;
- are specifically authorized in the provider's written "need-to-know" protocol to have access to patient information (specifically, HIV related information, under Article 27-F); and

- have a reasonable need to know or share the information to carry out their authorized duties in providing, supervising, administering or monitoring the services. §§ 2782(1)(c); 2782(6)(b); 2786.2); 45 C.F.R. § 164.514(d)(2).

Both Article 27-F and HIPAA require providers to identify and document in writing which employees belong in the need-to-know circle.

Permissible reasons to include people in the need-to-know circle include: providing direct care/services to the clients; performing administrative, billing or reimbursement functions; and planning, coordinating or supervising services to clients (for example, when staff work in "teams"). Impermissible reasons include: "infection control" (universal precautions should be used instead); and curiosity.

HIPAA Impact. HIPAA also requires providers to document the categories of information to which each staff member needs access and any conditions to their access that exist. 45 C.F.R. § 164.514(d)(2). Article 27-F requires this with HIV related information, specifically.

Remember: the confidential information protected by Article 27-F is limited to HIV related information, while HIPAA protects all health related information. As a result, some health care providers will have two need-to-know protocols: one documenting staff who need access specifically to HIV related information and another documenting staff who need access to any health related information protected under HIPAA.

D. Health Care Provider Rule: Disclosures to Health Care Providers

Both Article 27-F and HIPAA permit persons and providers to disclose HIV related information about a protected individual, without consent, to a health care provider or health facility when they determine that it is necessary for the health care provider or facility to know the HIV related information to provide appropriate care or treatment to the protected individual, his or her child, or a contact of the protected individual (§ 2782(1)(d); 10 NYCRR § 63.4); 45 C.F.R. §§ 164.502(a), 164.506(c)). A "contact" means (1) an identified spouse or sexual partner, (2) a needle-sharing partner, or (3) an occupationally exposed person (§ 2780(10); 10 NYCRR § 63.1(k)).

Article 27-F prohibits – because it is not "necessary" – disclosure of an individual's HIV status to a health care provider solely for "infection control" purposes, i.e., to protect the health care worker(s) from possible exposure to HIV (10 NYCRR § 63.5(j)). This is because the universal infection control precautions that health care providers must use effectively minimize the risk of occupational exposure to HIV; health care workers must protect themselves by using these precautions regardless of whether they know particular patients' HIV status. Because this provision is more stringent than HIPAA's provision allowing communication for the purpose of treatment, providers must follow Article 27-F.

Under Article 27-F, the provider or individual with the confidential HIV related information – and not the outside health care provider – has the discretion to decide whether the outside provider really does need to know the client's HIV status in order to appropriately care for or treat that individual or his or her child. The only employee(s) who may be given HIV related information are those who (1) are authorized (under the health provider's written need-to-know list) to have access to medical records and HIV related information, and (2) provide health care to the individual about whom the information pertains, or maintain the provider's medical records for billing or reimbursement purposes. The notice prohibiting redisclosure (described above in the consent section and attached) must be sent to the recipient.

E. Physicians' Disclosures about Minors and Incompetent Adults

Article 27-F permits physicians (but *not* others) to sometimes disclose HIV related information about a minor (under age 18) to his/her parent or legal guardian (whoever is authorized by law to consent to health care for the minor) even without the minor's consent. (§ 2782(4)(e)). The same rule applies to disclosures about persons who have been judicially declared incompetent (not competent to make health care decisions for themselves).

No change under HIPAA. Similarly, HIPAA permits a health care provider to disclose health related information to the legal guardian or "personal representative" of the minor or incompetent adult. HIPAA's treatment of minors defers to State law. (45 C.F.R. § 164.512(g)). Consequently, such disclosures can only be made within the limits prescribed by Article 27-F.

Article 27-F permits (but does not require) disclosure to the parent/legal guardian if a physician reasonably believes that:

1. the disclosure is medically necessary to provide timely care and treatment to the minor/incompetent adult;
AND
2. the minor or incompetent adult will not inform parent/guardian, even after being counseled about the need for disclosure.

Even when these two conditions are met, the physician may *not* disclose the information if, in the physician's judgment, (1) the disclosure is *not* in the minor's or incompetent adult's best interests, or (2) the minor (or incompetent adult) has legal authority to consent on his/her own to health services. (Married and pregnant minors and minors who are parents, as well as emancipated minors, have the authority to consent to their own health care, including HIV testing and treatment, without parental knowledge or permission; physicians may not disclose HIV related information to parents of these minors without their consent.)⁴

⁴ State law also gives minors the legal authority to consent on their own to treatment for certain sensitive health conditions (e.g., mental health, drug/alcohol, STD, family planning, abortion services); and physicians who provide these health services to minors based on the minor's consent generally may not to disclose this information to third parties, including the minor's parents, without first obtaining the minor's consent to the disclosure.

A physician who makes a decision or takes action under this rule (on disclosure to parents/legal guardians under Article 27-F) must document the reason(s) in the minor or incompetent person's medical record (§ 2782(4)(e)). However, the notice prohibiting redisclosure that must accompany most disclosures of HIV related information need not be given to parents or legal guardians (§ 2782(5)).

F. HIV/AIDS Case Reporting

The State HIV law requires doctors and labs who diagnose HIV to report every case of HIV infection, HIV related illness, and AIDS diagnosed after June 1, 2000 – including the patient's name – to the State Department of Health. They also must report the names of known sexual and needle-sharing "contacts" of people diagnosed with HIV infection or related illness, including AIDS. (See "Contact Notification" discussed in the next section.) Names of people who are tested at anonymous HIV test sites are not reported. (§§ 2130, 2132).

No change under HIPAA. HIPAA permits providers to comply with all state public health reporting requirements. 45 C.F.R. § 164.512(b).

The State Department of Health forwards the names and contact information to the local health departments for use in contact (partner) notification activities. These public health officials also use the information to monitor the progression of the HIV epidemic and plan prevention programs. They must keep the information confidential, except for purposes of contact notification, discussed below.

G. Contact (Partner) Reporting and Notification

Since June 1, 2000, the State HIV law has required public health authorities in New York to make reasonable efforts to notify known "contacts" (spouses and sexual and needle sharing partners) of an HIV-positive person that they may have been exposed to HIV (§ 2133). Priority is given to notification of (1) identified partners of those newly diagnosed with HIV, and (2) spouses. Physicians *may* (but are not required to) notify contacts in certain circumstances, and *must* forward the names of known contacts to the State Department of Health when making mandated HIV/AIDS case reports (see "F" above).

No change under HIPAA. HIPAA permits health care providers to comply with all state partner notification laws. 45 C.F.R. § 164.512(b)(1)(iv).

While physicians and public health authorities may ask people who have been diagnosed with HIV infection, HIV related illness or AIDS to voluntarily name their "contacts" (spouses, sexual and needle sharing partners) individuals are *not required* to reveal their contacts, and cannot be penalized for refusing to do so.

Under Article 27-F, physicians may notify contacts only if the physician (1) concludes that notification is medically appropriate and that the contact has a significant risk of infection,

(2) counsels (or tries to counsel) the protected person about the need to notify contacts, (3) conducts a domestic violence screening, and (4) informs the protected person (a) of the physician's intent to notify the contacts and his/her responsibility to report them to the Department of Health, (b) that the protected person can choose to have Department of Health (rather than the physician) conduct the partner notification effort, and (c) that the protected person's name will not be revealed (§ 2782.4(a)).

Under Article 27-F, *neither the public health authorities nor physicians may ever reveal the identity of the "source" patient to his or her partners or others* (except to public health officials carrying out partner notification functions). Moreover, neither the state or local health departments nor physicians may conduct notification without first performing a domestic violence screening; and notification must be deferred if there is a risk of domestic violence to either the "source" patient or the partner.

New York State's Partner Notification Assistance Program (P-NAP) conducts contact notification in all parts of the State except New York City and can be reached at 800-541-2437. New York City's Contact Notification Assistance Program (C-NAP) can be reached at (212) 693-1419 or (888) 792-1711.

H. Newborn Testing

The Public Health Law requires all newborns in New York State to be tested for HIV. The test results must be given to the mother, unless she lacks capacity to consent to health care for the newborn. In such cases, the newborn's HIV test results must be given to the individual with authority to consent to such care (who, depending on the circumstances, might be the father or other person authorized by law).

The newborn's HIV test result also must be given to (1) the newborn's physician/primary health care provider, (2) upon request by the newborn's physician, to an HIV specialized care center (a publicly funded facility that provides treatment and services to HIV-positive newborns and their mothers and families), and (3) the Department of Health. (These requirements are set out in Public Health Laws §§ 2500-f, 2781(6)(d), and in the Department of Health regulations, 10 NYCRR Part 69, and related Department of Health materials available on the Department's website, www.nyhealth.gov/diseases/aids/index.htm.)

No change under HIPAA. All of these disclosures are permitted under HIPAA, which allows disclosures to parents and guardians of minors and to health care providers for purposes of treatment, and disclosures required under state public health reporting laws.

I. Foster Care and Adoption

The rules under Article 27-F governing disclosures of HIV related information in the context of foster care and adoption are complex. Briefly put:

- Health and social service providers covered by Article 27-F are permitted to disclose

HIV related information to an authorized agency in connection with the foster care or adoption of a child (§2782)(1)(h)). "Authorized agencies" are foster care and adoption agencies, social service officials responsible for child welfare and the courts. The HIV related information (about the child/biological parent, or other involved persons such as foster/adoptive parents) **must be** directly relevant to a particular foster care or adoption proceeding;

- Providers should obtain the minor's consent where practicable.

Following is a brief summary of the rules concerning disclosures of HIV related information in the context of foster care and adoption. For more detail, consult the Legal Action Center's comprehensive manual, *HIV/AIDS: Testing, Confidentiality and Discrimination: What You Need to Know about New York Law*.

Article 27-F requires or permits authorized agencies to disclose HIV related information about a foster/adoptive child to:

- (1) foster care and adoptive parents –
 - upon placement in foster care or once the adoption process is underway, or
 - after placement, upon request of the foster/adoptive parent;
- (2) law guardians – when necessary to represent the minor;
- (3) other authorized foster care/adoption agencies – upon transfer of the child to their care;
- (4) the foster child when he or she is discharged to his/her own care or is adopted and so requests;
- (5) biological parents –
 - without the minor's consent if the minor lacks capacity to consent, or
 - only with the minor's consent if the minor has capacity to consent;
- (6) other service providers only with the appropriate consent, and only if the disclosure is necessary to obtain essential health or social services for the child; and
- (7) the court in a case involving the foster child, if ordered by the court after a hearing.

No change under HIPAA. These disclosures would also be allowed under HIPAA, which permits a health care provider to disclose a minor's health information, as required by State law, to the minor's "personal representative." A personal representative includes a parent, guardian or other person acting *in loco parentis* (in parents' stead). 45 C.F.R. § 164.502(g)(3).

Article 27-F allows HIV related information about a foster/adoptive child to be redisclosed:

- (1) by foster parents (without consent) only to provide care, treatment or supervision of the child;
- (2) by adoptive parents freely; and
- (3) by law guardians only with the child's consent, if the child has capacity to consent. If the child lacks capacity to consent, then redisclosure is only permitted for the purpose of representing the child.

(§ 2782(3)(c), (d), (e)). These rules are set forth in an administrative bulletin issued by the former Department of Social Services (97 ADM-15, p. 31)).

J. Court Orders

A subpoena – even if issued by a court – does **not** authorize the disclosure of confidential HIV related information. Only a special court order issued in accordance with Article 27-F's requirements can do this. A court may only authorize the disclosure of confidential HIV related information in four circumstances: when the court determines that (1) there is a compelling need for adjudication of a criminal or civil case; (2) there is a clear and imminent danger to an individual's life or health; (3) there is a clear and imminent danger to the public health; or (4) the applicant is lawfully entitled to the disclosure.

Even then, the court must make certain written findings of fact and weigh the need for the disclosure against the privacy interests involved before deciding whether to issue an order authorizing the HIV related information to be disclosed. In addition, special procedures must be followed, such as giving the protected person and the person who has the confidential information an opportunity to oppose the disclosure (§ 2785).

No change under HIPAA. Although HIPAA has less restrictive rules governing subpoenas and court orders, Article 27-F is "more stringent" under the test described above in the state law section of Part I.C. Therefore, providers must follow Article 27-F when dealing with subpoenas and court orders.

K. Insurers and Other Third Party Payers

Disclosure for Reimbursement. Under Article 27-F, providers may disclose HIV related information to insurers without an HIV-specific consent form for the purpose of getting reimbursed for health care services. In this case, the health care provider only needs a general medical release meeting the requirements of New York State law. (§ 2782(1)(i)).

No change under HIPAA. Although HIPAA permits disclosures for purposes of payment and health care operations without consent, Article 27-F is "more stringent" under the test described above in the state law section of Part I.C. Therefore, providers must continue to obtain patient consent when disclosing HIV related information to insurers for the purpose of obtaining reimbursement for their health services. A general medical release satisfies this requirement. The special HIV-specific release form usually required by Article 27-F is not needed to authorize disclosures for purposes of obtaining reimbursement for health care services.

Disclosure for Other Purposes. If, however, the disclosure to an insurer is for any other purpose (for example, in connection with an individual's application for health or life insurance), then an HIV-specific release is necessary (§ 2782(1)(j)). Special rules apply in the case of a Health Maintenance Organization (HMO) that acts both as an insurer and a health care provider. A disclosure made to the HMO-as-health-care-provider for the purpose of obtaining medical care

(rather than for reimbursement or other insurance purposes) can be made without any written consent, in accordance with the health care provider rule discussed in “D” above.

Insurers and other third party payers, although probably subject to HIPAA as "health plans," generally are not subject to Article 27-F's confidentiality requirements. The only times where insurers would be subject to Article 27-F is when they obtain HIV related information pursuant to an individual's HIV-specific written consent, or if they are providing health care, as in the case of an HMO.

L. Program Evaluation, Monitoring

Under **both Article 27-F and HIPAA**, certain private and government oversight authorities may obtain HIV related and other health related information from the agencies they oversee, without the consent of the individuals whose HIV related information is being disclosed. These include health care facilities and committees performing such oversight functions, oversight review organizations, and government agencies that are authorized to have access to medical records and to HIV related information in those records when needed to supervise, monitor or administer a health or social service. Under Article 27-F, the disclosure is only permissible to carry out program monitoring, evaluation or review functions (§ 2782(1)(f)). Article 27-F also places strict limitations on the use and disclosure of confidential HIV related information obtained by such organizations (§ 2782(6)).

No change under HIPAA. This is another example of where Article 27-F is more stringent than HIPAA. As a result, providers must continue to abide with Article 27-F's restrictions.

M. Convicted and Certain Accused Sex Offenders

A court may order convicted sex offenders and defendants accused of certain sex offenses to take an HIV test upon the request of the victim. Article 27-F permits the public health officials who perform the test to communicate the results (and provide post-test counseling) to the victim and the tested person, unless the tested person does not want to learn the results. Under Article 27-F, the victim may redisclose the test results to his or her immediate family, guardian, physicians, attorneys, medical or mental health providers, and past and future contacts to whom there was or is as reasonable risk of HIV transmission. The court shall not learn the test results (§ 2785-a; N.Y. Crim. Proc. L. § 210.16; N.Y. Pub. Health L. § 2805-i).

HIPAA Impact. HIPAA may not permit the disclosure of the test results to the victim absent a court order issued in accordance with HIPAA's provisions. 45 C.F.R. 164.512(e)(1)(i). Consequently, a court that orders a convicted or accused sex offender to take an HIV test should include in its order a provision that the test results be disclosed to the victim.

N. Occupational Exposure

Under Article 27-F, workers in specified occupations who may have been exposed to HIV on the job may be told the HIV status of the "source" of the exposure in limited circumstances if medical experts determine that the exposure incident involved a significant risk of infection. The source's consent to the disclosure is not needed. This exception applies only to the *disclosure* of information about someone who has already been tested for HIV or consents to be tested. Article 27-F does not permit mandatory testing of the source.⁵

This exception only applies in certain occupational settings, such as medical and dental offices, emergency response settings (e.g., emergency medical technicians; firefighters or law enforcement officers when performing emergency response duties), and facilities licensed by specific state agencies (e.g., drug and alcohol treatment programs, mental health facilities, foster care agencies, prisons) (10 NYCRR § 63.8).

No change under HIPAA. This disclosure would also be permitted under HIPAA, which allows disclosures of health related information to a health care provider for the purpose of treatment. HIPAA also permits disclosure of health related information to an individual when it is necessary to prevent or lessen a serious and imminent threat to the health of the individual. 45 C.F.R. § 164.512(j). In the occupational exposure context, information about whether the incident involved exposure to HIV may be needed to help an exposed worker decide whether to start or stop prophylaxis.

O. Disclosures for Medical Education, Research, Therapy or Transplantation

Under Article 27-F, no consent is required for disclosures of HIV related information to health care providers or facilities in connection with the procurement, processing, distribution or use of human bodies or body parts (including organs, tissues or fluids) for use in medical education, research, therapy or transplants (§ 2782(1)(e)).

HIPAA Impact. These types of disclosures are permitted under HIPAA without consent for medical education, therapy and transplants. However, HIPAA has new requirements for disclosures for research purposes. These are mandatory provisions that must be adopted by covered entities.

HIPAA's Research Rules. For a covered entity to use or disclose patient identifying health related information for research purposes, it must first obtain the patient's written authorization (consent), or a waiver from either an Institutional Review Board (IRB) or a "privacy board." 45 C.F.R. § 164.512(i)(1)(i).

⁵ The State Department of Health has developed a consent form that may be used for this purpose. A person who is the source of an occupational exposure may voluntarily agree to be tested for HIV and to allow the test results to be given to the exposed health care worker. This form – *Informed Consent to Perform HIV Testing and Authorization for Release of HIV-related Information for Purposes of Providing Post-exposure Care to a Health Care Worker Exposed to a Patient's Blood or Body Fluids* (DOH- 4054 (Rev. 8/05)) – can be downloaded from the DOH website at www.nyhealth.gov/diseases/aids/index.html.

Authorization. If the patient’s written authorization is sought, the authorization must have all the elements required by HIPAA and Article 27-F described in Part IV.A above. Although HIPAA allows the authorization to use an expiration date such as “end of research study,” “none,” or similar language when the authorization is used for research purposes, 45 C.F.R. § 164.508(c)(i)(v), Article 27-F requires that a consent form specify the date, event, or condition upon which the consent expires, so providers may NOT use “none” as an expiration date.

Waiver. A waiver authorizing research may be approved if the IRB or privacy board determines – and documents – that the waiver satisfies the following criteria:

1. The use or disclosure of protected information involves no more than a minimal risk to the individuals who are research subjects.
2. The research could not practicably be conducted without the waiver.
3. The research could not practicably be conducted without access to and use of the protected information.
4. There is an adequate plan to protect patient-identifying information from improper use and disclosure.
5. There is an adequate plan to destroy the identifiers at the earliest opportunity unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law.
6. There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for oversight of the project, or for other research for which the disclosure of protected information would be permitted by HIPAA.

45 C.F.R. § 512(i)(2)(ii).

P. Employees within Certain Criminal Justice Agencies

Under Article 27-F, certain employees or agents of the State Division of Parole, Department of Correctional Services, Division of Probation and Correctional Alternatives and Commission of Corrections and local criminal justice agencies are permitted, in limited circumstances, to have access to HIV related information about individuals under their jurisdiction without those individuals’ consent. (§§ 2782(1)(m), 2782(1)(l), 2782(1)(o)). Each agency has its own rules describing who may have access to confidential HIV information and for what purposes.

No change under HIPAA. While HIPAA permits disclosure of health related information to and within correctional institutions and other criminal justice system agencies in certain limited circumstances, this is another example where Article 27-F is more stringent and should be followed.

Q. Public Health Officials

Article 27-F authorizes state, county or local public health departments and officers to disclose HIV related information in four circumstances: (1) when the disclosure is "specifically authorized or required by federal or state law"; (2) in the course of contact notification (see "G," above); (3) when the person to whom the HIV related information pertains (or other person authorized by law) has signed a proper HIV consent form authorizing the disclosure; or (4) when the disclosure is authorized by a special court order issued under Article 27-F (§ 2782(2)).

No change under HIPAA. HIPAA permits each of these disclosures as well.

R. Child Abuse/Neglect and Elder Abuse/Neglect

Neither Article 27-F nor HIPAA prevents people and agencies from carrying out their duties and authority to report, investigate, or redisclose child protective or adult protective information as required or permitted the New York State's laws addressing child abuse and neglect and elder abuse and neglect (§ 2782(7)) (45 C.F.R. § 164.512(c)). Under Article 27-F, it is permissible to disclose HIV related information about an individual only if it is relevant to the abuse or neglect matter.

S. Business Associate Agreements

While HIPAA permits covered entities to enter into a written agreement with certain outside service providers, called business associates, allowing them to exchange confidential health information without individual patients' consent, Article 27-F does not permit such agreements. Any disclosure of confidential HIV related information must be done through one of the exceptions discussed in Parts A through R above.

However, providers that must comply with Article 27-F may encounter other providers that use business associate (BA) agreements, or may even be asked to enter one. For your information, **a sample Business Associate agreement is attached.**

V. HIPAA'S ADMINISTRATIVE REQUIREMENTS

If your organization is a covered entity or a hybrid entity under HIPAA (See Part II.B), HIPAA requires you to put in place several administrative measures to ensure that the privacy of patients' personal health administration is protected. These measures are mandatory and all covered health care providers must have implemented them by April 14, 2003.

Privacy Official. Providers must appoint a privacy official who is responsible for the development and implementation of the program's privacy policies and procedures. 45 C.F.R. § 164.530(a). The provider may designate a current staff member or hire a new individual. Responsibilities could include providing guidance in the identification, implementation, and

maintenance of the program's privacy policies and procedures; performing initial and periodic assessments and compliance monitoring of such policies and procedures; and ensuring that the program maintains appropriate patient notices and release forms.

Training of Workforce. Training on HIPAA's privacy rules is required for each member of the provider's workforce; providers must document that the required training has been provided. 45 C.F.R. § 164.530(b).

Safeguards. Providers must put in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information from any intentional or unintentional use or disclosure which would violate HIPAA, including any incidental use or disclosure made in the course of an otherwise permitted or required use or disclosure. 45 C.F.R. § 164.530(c).

HIPAA also sets forth specific security and electronic standards which require covered entities to have security controls and measures in place to protect confidential patient information when it is electronically stored, maintained, or transmitted. (See 45 C.F.R. Parts 142 & 162.)

Complaints and Sanctions. Providers must provide a process for individuals to make complaints concerning the provider's HIPAA policies and procedures and its compliance with the requirements of HIPAA's Privacy Rule. 45 C.F.R. § 164.530(d), (e). Providers must:

- Designate a staff member to be responsible for receiving complaints (this can be the privacy official discussed above).
- Document all complaints received and their disposition.
- Establish sanctions to be imposed if a member of the provider's workforce fails to comply with any of HIPAA's requirements or the provider's privacy policies and procedures.

Notice of Privacy Rights. HIPAA requires providers to notify patients of the existence of its Privacy Rule's requirements and to give them a written summary of the law. 45 C.F.R. § 164.520.

A sample notice of privacy rights is attached. See the *Sample Notice of Privacy Practices*.

HIPAA requires this notice to be in plain language. It may be in written or electronic form (with some additional requirements), and it must contain the following elements:

1. Header with the following statement: "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."

2. Description, including at least one example, of the types of uses and disclosures of protected health information that the provider is permitted to make for treatment, payment, and health care operations; should include only those also permitted under Article 27-F.
3. Description of each of the other purposes for which the provider is permitted or required to disclose protected health information without the individual's consent or authorization; should include only those permitted under Article 27-F.
4. Statement that other uses and disclosures will be made only with the individual's written authorization (consent) and that the individual may revoke this authorization.
5. Statement of the individual's rights under HIPAA and a description of how the individual may exercise those rights.
6. Statement that the provider is required by law to maintain the privacy of protected health information and to provide individuals with notice of the provider's legal duties and privacy practices.
7. Statement that the provider is required to abide by the terms of the notice.
8. Statement that the provider reserves the right to change the terms of the notice, and a description of how the provider will provide individuals with a revised notice.
9. Statement that individuals may complain to the provider and to HHS if they believe their privacy rights have been violated, together with a description of how the complaint may be filed.
10. Name, title, and telephone number of a contact for further information.
11. Date on which the notice became effective.

45 C.F.R. § 164.520(b).

Providers must provide this notice to each patient no later than the first service provided to the individual after April 14, 2003 (even if the service is provided by telephone or electronically). 45 C.F.R. § 164.520(c)(2)(i). In an emergency treatment situation, providers must provide the notice as soon as reasonably practicable.

The notice must be posted in a clear and prominent location and readily available for individuals to take with them upon request. Providers must also make a "good faith effort" to obtain a written acknowledgment from the patient that he or she received the notice except in emergency treatment situations. If the provider is unable to get a written acknowledgment because the patient refuses to provide it or for any other reason, then the provider must document good faith efforts and the reason the acknowledgment was not obtained. 45 C.F.R. § 4.520(c)(2).

Providers must document compliance by retaining copies of the notices and any written acknowledgments or documentation of good faith efforts. 45 C.F.R. § 64.520(e). Providers must also designate a staff member to be responsible for providing further information about matters covered by the notice (this person could be the privacy official and/or the contact for complaints discussed above). 45 C.F.R. § 164.530 (a)(1)(ii).

Documentation. All privacy policies, procedures, and personnel designations must be documented in written or electronic form. 45 C.F.R. § 164.530(j).

VI. PATIENT RIGHTS

In addition to new administrative requirements, HIPAA's Privacy Rule also provides individuals with patient rights. Some of these patient rights are also provided by existing New York State laws – including Article 27-F; Public Health Law §18; which deals with patients' rights to access their medical records generally; and Mental Hygiene Law § 33.16, which deals with mental health records.

Covered health care providers must establish procedures to assure that patients can exercise these rights in compliance with HIPAA, Article 27-F, Public Health Law §§ 17 and 18 and, for mental health providers, Mental Hygiene Law § 33.16.

The Legal Action Center has performed the analysis required under the “more stringent” test described in Section I.C above. The following sections are the result of this analysis – they synthesize HIPAA and New York's Public Health and Mental Hygiene Laws to provide a simple and concise explanation of how New York providers can allow patients to exercise these rights in compliance with both federal and state laws.

A. Right to an Accounting of Disclosures

Article 27-F requires a provider, upon request, to tell individuals about disclosures of confidential HIV related information about the individual. § 2782(5)(a). HIPAA also requires covered health care providers to provide individuals, upon request, with an accounting of certain disclosures made regarding a patient's health care. 45 C.F.R. § 164.528(c). HIPAA also provides specific procedures that must be followed when providing this accounting. To meet this requirement, providers should establish a system for tracking and documenting certain disclosures of confidential information.

Exceptions. The following disclosures do not have to be included in the accounting: (1) to the individual patient; (2) under the internal communications exception discussed in Section IV.C; (3) to insurance companies beyond the initial disclosure (the initial disclosure must be noted in the record); or (4) to persons engaged in quality assurance, program monitoring or evaluation or governmental payment agents. 45 C.F.R. § 164.528(c)(1), N.Y. Pub. Health L. §§ 18(f)(6), 2782(5)(b).

Procedure. The accounting must be provided within **10 days** of the patient's request.

Under HIPAA, if more time is needed, the provider can extend the deadline for up to 30 days, as long as the patient is given an explanation for the delay. HIPAA requires providers to include in the accounting the date of the disclosure, the name and address of the person who received the information, a description of the disclosed information, and a statement of the purpose of the disclosure. 45 C.F.R. §164.528(b)(2). Providers must also designate and identify by title the members of their workforce who are responsible for receiving and processing patient accounting requests. 45 C.F.R. § 164.528(d)(3).

B. Right of Access to Health Records

Right and Exceptions. Both HIPAA and New York law require providers to give patients access to their own health records upon request. 45 C.F.R. § 164.524, N.Y. Pub. Health L. § 18 (medical records), N.Y. Ment. Hyg. L. § 33.16 (mental health records).

1. Psychotherapy notes. Although HIPAA states that patients do not have the right to access “psychotherapy notes,” under New York law there are some circumstances when a patient may have access to psychotherapy notes. In order to be in accordance with both HIPAA and New York’s Mental Hygiene Law, practitioners can deny access to information in psychotherapy notes if it is likely to cause substantial harm to patient or others. However, if the health related information is not in psychotherapy notes, a practitioner may deny access to it only if it is likely to cause substantial harm to others, or to endanger the life or cause physical harm to the patient. 45 C.F.R. § 164.524(a)(1), N.Y. Ment. Hyg. L. § 33.16, N.Y. Pub. Health L. § 18(3)(d).

Psychotherapy notes, as defined by HIPAA, are notes recorded in any medium “by a health care provider who is a mental health professional documenting or analyzing the contents of conversations during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual’s medical record.” 45 C.F.R. § 164.501.

2. Confidentiality agreement. HIPAA allows a provider to deny access to information if it was obtained from someone other than a health care provider under a *promise of confidentiality* and the access would likely reveal the source of the information. 45 C.F.R. § 164.524(a)(2). Although there is a similar provision under New York’s Public Health and Mental Hygiene laws, providers should follow HIPAA because it is more stringent.

Who May Exercise the Right. The subject of the information, the parent or guardian of a minor who lacks capacity to consent (see section IV.E on minors) – with some exceptions under New York law that give a minor the right to consent to certain health services on his/her own, and also require the minor’s consent for health care providers’ disclosures of that information to third parties, including the minor’s parents – or the court-appointed guardian of a mentally incompetent individual can exercise the right to access HIV related information in an individual’s medical or mental health records. N.Y. Pub. Health L. §18(1)(g) , § 17; N.Y. Ment. Hyg. L. § 33.16(b).

Procedure. When processing a patient’s request to access his or her own records, a provider covered by HIPAA and New York law must comply with the following requirements:

1. Providers must act on a written request for access no later than **10 days** after receipt of the request. N.Y. Pub. Health L. § 18(2), N.Y. Ment. Hyg. L. § 33.16(b).
 - Providers have *60 days* if the requested information is not maintained or accessible at the provider's site. 45 C.F.R. § 164.524(b)(2)(ii).
2. If the provider *grants* the request in whole or in part, it must inform the patient and provide the requested access within 10 days of the request. 45 C.F.R. § 164.524(c), N.Y. Pub. Health L. § 18(2), N.Y. Ment. Hyg. L. § 33.16(b).
 - The provider must provide the access, including inspection or obtaining copies or both.
 - The provider may provide a *summary* of the requested information in lieu of providing access, or may provide an explanation of the information, if: (1) the request to review can reasonably be expected to cause substantial and identifiable harm to the patient or others which would outweigh the right of access; or, in the case of medical records only, (2) the requested material consists of the practitioner's personal notes and observations. N.Y. Pub. Health L. § 18(3)(d), N.Y. Ment. Hyg. L. § 33.16(c)(3).
 - The practitioner must either arrange a convenient time and place to inspect or copy the information, or mail the information at the individual's request. Practitioners may place reasonable limits on the time, place and frequency of inspections. 45 C.F.R. § 164.524(c), N.Y. Pub. Health L. § 18(2)(f), N.Y. Ment. Hyg. L. § 33.16(b)(7).
 - If the individual requests copies of the information, the provider may impose a reasonable cost-based fee not to exceed 75¢ per page. 45 C.F.R. § 4.524(c)(4), N.Y. Pub. Health L. § 18(2)(e), N.Y. Ment. Hyg. L. § 33.16(b)(6).

Denial of Access. Although HIPAA provides “unreviewable” and “reviewable” grounds for denying a patient access to his/her own records, 45 C.F.R. § 164.524(a)(2), (3), under the more stringent New York law all denials of patient access to medical or mental health records are subject to review.

If the provider denies a patient access under any of the exceptions described above, the provider must:

1. To the extent possible, exclude only that information to which the provider believes it has grounds to deny access, and provide access to any other requested information. 45 C.F.R. § 164.524(d)(1), N.Y. Pub. Health L. § 18(3)(d), N.Y. Ment. Hyg. L. § 33.16(c)(4).

2. Inform the patient of the denial, and the basis for the denial, as well as the patient's right to obtain, without cost, a review of the denial by the appropriate medical record access review committee. N.Y. Pub. Health L. § 18(3)(e), N.Y. Ment. Hyg. L. § 33.16(c)(4).
3. If the patient requests review, the provider must, **within 10 days** of receiving the request, transmit the information in question to the chair of the review committee with a statement setting forth the specific reasons for denying access. 45 C.F.R. § 164.524(d)(2), N.Y. Pub. Health L. § 18(3)(e), N.Y. Ment. Hyg. L. § 33.16(c)(4).
4. If the provider does not maintain the requested information, but knows where the information is maintained, it must inform the patient where to direct his request for access. 45 C.F.R. § 164.524(d)(3).

Review Committee. Upon the patient's request, all denials of access to patient records must be reviewed by an external medical record access review committee. The committee must conduct an *in camera* review and provide all parties with a reasonable opportunity to be heard. The committee's decision must be in writing and issued promptly. N.Y. Pub. Health L. §§ 18(3)(e), (f), & (4), N.Y. Ment. Hyg. L. § 33.16(c)(4).

C. Right to Request an Amendment to Health Records

HIPAA provides individuals with the right to request that a provider amend health information kept in his/her own records, and requires specific procedures to be followed when processing such a request. 45 C.F.R. § 164.526. Although New York law also gives individuals the right to challenge the accuracy of factual information in their health records, HIPAA's provisions provide patients with greater rights in this area. Consequently, New York providers should follow the HIPAA requirements when patients request changes to their health records.

Procedure. When processing a patient's request to amend his or her own records, a provider covered by HIPAA and New York law must comply with the following requirements:

1. The provider must document the titles of the persons responsible for receiving and processing amendment requests.
2. A provider can *deny* a request to amend if it determines that the information or record:
 - Was not created by the covered entity, unless the individual provides information that the originator of the information is no longer available to act on the requested amendment;
 - Is not part of a designated record set;
 - Would not be available for inspection under 45 C.F.R. § 164.524 (the access to information section described above); or

- Is accurate and complete.

45 C.F.R. § 164.526(a)(2).

3. A provider may require individuals to make requests in writing and to provide a reason to support the amendment, as long it informs them in advance of the requirements. 45 C.F.R. § 164.526(b)(1).
4. A provider must act on the amendment request no later than 60 days after receiving it.

If unable to act within 60 days, the program may have a one-time, 30-day extension if it provides a written statement explaining the delay and the date it will complete the request.

45 C.F.R. § 164.526(b)(2).

5. If the provider *accepts* the amendment, in whole or in part, it must at a minimum make the amendment by identifying the affected records and appending or otherwise providing a link to the location of the amendment.

- The provider must inform the patient in a timely manner that the amendment is accepted and obtain the patient's consent for the provider to notify the relevant persons with whom the amendment needs to be shared.
- Within a reasonable time, the provider must make "reasonable efforts" to inform and provide the amendment to persons identified by the patient and persons, including business associates, that the program knows have the affected information and that have relied on or could foreseeably rely on the information to the patient's detriment.

45 C.F.R. § 164.526(c).

6. If the provider *denies* the request to amend:

(a) It must provide a timely written denial, written in plain language and containing:

- The basis for the denial;
- A description of the patient's right to submit a written statement disagreeing with the denial and the instructions for filing such a statement;
- A statement that, if the patient does not submit a statement of disagreement, he or she may request the provider to provide the amendment request and the provider's denial with any future disclosures of the subject information; and
- A description of how the patient may complain to the provider pursuant to its complaint procedures; must include name or title and telephone number of the contact person for complaints.

- (b) the provider must permit the individual to submit a statement disagreeing with the denial of all or part of the requested amendment, and the provider may prepare a written rebuttal to the statement of disagreement.
- (c) The provider must also, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the provider's denial of the request, the individual's statement of disagreement, and the provider's rebuttal, if any, to the designated record set.

45 C.F.R. § 164.526(d).

D. Right to Receive Confidential Communications

HIPAA requires covered providers to accommodate reasonable requests by patients to receive communications of protected health information by alternative means or at alternative locations. 45 C.F.R. § 164.522(b)(1). For example, patients may request that communication be emailed, or sent to a different location than their homes. Although the provider may not require an explanation from the patient regarding the basis of the request, it may require the request to be made in writing. A provider may also condition its accommodation of the request on information as to how any additional costs will be paid and specification of an alternative address or other method of contact. 45 C.F.R. § 164.522(b)(2). Since New York law does not give patients this right, covered entities should follow HIPAA.

E. Right to Request Restrictions on Use or Disclosure

A health care provider covered by HIPAA must give patients the opportunity to request that the provider restrict certain uses or disclosures of the patient's protected health information to carry out treatment, payment or health care operations. 45 C.F.R. § 164.522(a). Although the provider is not required to agree to the patient's request, if it does agree it must then abide by the restriction and not use or disclose the restricted information (unless it is necessary to treat the patient in an emergency situation). Any agreed upon restriction must be appropriately documented. Since New York law does not give patients this right, covered entities should follow HIPAA.

HIPAA excludes a number of specific uses and disclosures from those on which a patient may request a restriction. For example, even if a covered entity agrees to a restriction, the restriction is simply "not effective" to prevent uses or disclosures required by HHS to determine the provider's compliance with HIPAA or any of the uses and disclosures permitted under 45 C.F.R. § 164.512.

Once a provider has agreed to a restriction, the restriction can only be lifted if the patient agrees to or requests the termination in writing, or orally agrees and the agreement is documented.

A provider may inform the patient that it is terminating the agreement, but the termination is only effective with respect to protected health information that is created or received after the provider has informed the patient. 45 C.F.R. § 164.522(a)(2).

VII. ENFORCEMENT AND PENALTIES

A. Article 27-F

Remedies for violation of Article 27-F's HIV confidentiality requirements. Persons who violate Article 27-F's confidentiality requirements are subject to civil and criminal penalties for the unlawful disclosure of confidential HIV related information protected by the HIV law. Individuals whose rights have been violated by illegal disclosure of confidential HIV related information may also file their own lawsuits for money damages and other remedies.

Complaints about Article 27-F violations – within the agency. While not specifically required by Article 27-F or the state agencies' regulations implementing the law, it is good practice for health care providers and facilities covered by Article 27-F to establish grievance/complaint policies and procedures for handling their patients' (and staff member's) complaints alleging violations of Article 27-F's confidentiality requirements.

Complaints about Article 27-F violations – with New York State Department of Health AIDS Institute. The AIDS Institute has a special unit that takes Article 27-F complaints, called the Special Investigation Unit (SIU). Its HIV Confidentiality Hotline is 800-962-5065. If the Department of Health/AIDS Institute finds an agency violated Article 27-F's HIV Confidentiality or HIV testing requirements, the DOH may require the agency to take corrective action and/or may impose a fine of up to \$5,000 per violation. Criminal penalties may be imposed if the violation was "willful" (§ 2783(2)).

Individuals wishing to make Article 27-F complaints can call or write the AIDS Institute's Special Investigation Unit, and may write their own complaint or use the AIDS Institute's form (Complaint Report for Alleged Violation of Article 27-F) to do so. This can be obtained by calling the HIV Confidentiality Hotline (at 800-962-5065), and can also be downloaded from the DOH website. DOH website at www.ny.health.gov/diseases/aids/docs/complaint/pdf.

Lawsuits. An individual may also file a lawsuit against the agency/persons charged with violating the HIV law and may seek monetary damages as well as other remedies to remedy harms caused by illegal HIV testing or confidentiality violations.

B. HIPAA

No federal lawsuit for HIPAA privacy violations. HIPAA does not give individuals a federal right to sue for violations of its privacy or other provisions, but violations may be grounds for state tort actions.

Complaints about HIPAA privacy violations – with the covered entity. Individuals may file a complaint with the covered entity they allege has disclosed or used their protected health information in violation of HIPAA's Privacy Rule or the entity's HIPAA Privacy policies and procedures. As noted above, HIPAA requires covered entities must have procedures and policies in place for accepting, investigating and handling the disposition of HIPAA privacy violations.

Each covered entity is responsible for establishing its own procedure for processing patient complaints.

Complaints about HIPAA privacy violations – with the U.S. Department of Health and Human Services (HHS) Office of Civil Rights. Individuals may also file a complaint charging health care providers covered by HIPAA with violating HIPAA's Privacy Rule with the U.S. Department of Health and Human Services (HHS). 45 C.F.R. § 160.306(a). HHS is the federal agency responsible for enforcing HIPAA. HHS may investigate complaints of HIPAA privacy violations by reviewing the covered entity's policies, procedures, and practices, and the circumstances regarding the alleged act or omission. HHS can impose fines or other sanctions on the covered entity for each violation. 42 U.S.C. § 1320d-5 *et seq.*

You can get a complaint form (called a Health Information Privacy Complaint) to submit to HHS's Office of Civil Rights (OCR) by calling OCR toll-free at 1-800-368-1019 (any language) or 1-800-537-7697 (TDD); or can download it from www.hhs.gov/ocr/privacy/howtofile.html.

Complaints to HHS must be filed in writing, either on paper or electronically, within 180 days of discovery of the act or omission. 45 C.F.R. § 160.306(b). To submit a complaint by mail in New York, people should write to the Office of Civil Rights, U.S. Department of Health and Human Services, Jacob Javits Federal Building, 26 Federal Plaza – Suite 3312, New York, New York, 10278. Voice Phone (212) 264-3313. FAX (212) 264-3039. TDD (212) 264-2355.

HHS may also conduct compliance reviews to determine whether covered entities are complying with the regulations. 45 C.F.R. § 160.308. Covered entities must maintain and provide records and compliance reports, cooperate with investigations and compliance reviews, and permit access to necessary information. 45 C.F.R. § 160.310.

C. Where to Find More Guidance

The State Department of Health plays a leading role in interpreting and enforcing Article 27-F. The U.S. Department of Health and Human Services is charged with interpreting and enforcing HIPAA. In general, therefore, HHS, rather than the State DOH, has the final say in explaining what HIPAA means and what it requires of providers that are covered entities who must comply with HIPAA's requirements.

So, providers that are covered by and must comply with both Article 27-F and HIPAA –

- can continue looking to the DOH for guidance on the State's HIV Confidentiality Law, as well as to any other State agency that funds or regulates the provider's services.
- will need to look to HHS to get definitive answers on questions relating to HIPAA and how it applies to them.

- can also consult with lawyers and advisers who have expertise in the State's HIV Confidentiality Law and HIPAA and can help providers that are covered both by Article 27-F and by HIPAA comply with both laws.
- can always call on the Legal Action Center for help. Funding from the AIDS Institute makes it possible for the Center to provide technical assistance through the Center's HIV Confidentiality Hotline about both Article 27-F and HIPAA for health and human service providers throughout New York State.

**For more information about HIPAA and
New York's HIV Testing and Confidentiality Law:**

Consult the Legal Action Center's manual,
*HIV/AIDS: Testing, Confidentiality and Discrimination:
What You Need to Know about New York's Law,*

or

Call the Legal Action Center at (212) 243-1313 or (800) 223-4044

HIPAA Compliant Authorization for Release of Medical Information and Confidential HIV* Related Information

New York State Department of Health

This form authorizes release of medical information including HIV-related information. You may choose to release just your non-HIV medical information, just your HIV-related information, or both. Your information may be protected from disclosure by federal privacy law and state law. Confidential HIV-related information is any information indicating that a person has had an HIV-related test, or has HIV infection, HIV-related illness or AIDS, or any information that could indicate a person has been potentially exposed to HIV.

Under New York State Law HIV-related information can only be given to people you allow to have it by signing a written release. This information may also be released to the following: health providers caring for you or your exposed child; health officials when required by law; insurers to permit payment; persons involved in foster care or adoption; official correctional, probation and parole staff; emergency or health care staff who are accidentally exposed to your blood, or by special court order. Under State law, anyone who illegally discloses HIV-related information may be punished by a fine of up to \$5,000 and a jail term of up to one year. However, some re-disclosures of medical and/or HIV-related information are not protected under federal law. For more information about HIV confidentiality, call the New York State Department of Health HIV Confidentiality Hotline at 1-800-962-5065; for information regarding federal privacy protection, call the Office for Civil Rights at 1-800-368-1019.

By checking the boxes below and signing this form, medical information and/or HIV-related information can be given to the people listed on page two (or additional sheets if necessary) of the form, for the reason(s) listed. Upon your request, the facility or person disclosing your medical information must provide you with a copy of this form.

- I consent to disclosure of (please check all that apply):
- My HIV-related information
 - Both (non-HIV medical and HIV-related information)
 - My non-HIV medical information **

Information in the box below must be completed.

Name and address of facility/person disclosing HIV-related and/or medical information: _____ _____
Name of person whose information will be released: _____
Name and address of person signing this form (if other than above): _____ _____
Relationship to person whose information will be released: _____ _____
Describe information to be released: _____
Reason for release of information: _____
Time Period During Which Release of Information is Authorized From: _____ To: _____
Disclosures cannot be revoked, once made. Additional exceptions to the right to revoke consent, if any: _____ _____
Description of the consequences, if any, of failing to consent to disclosure upon treatment, payment, enrollment or eligibility for benefits (Note: Federal privacy regulations may restrict some consequences): _____ _____

All facilities/persons listed on pages 1,2 (and 3 if used) of this form may share information among and between themselves for the purpose of providing medical care and services. Please sign below to authorize.

Signature _____ Date _____

*Human Immunodeficiency Virus that causes AIDS

** If releasing only non-HIV medical information, you may use this form or another HIPAA-compliant general medical release form.

HIPAA Compliant Authorization for Release of Medical Information and Confidential HIV* Related Information

**Complete information for each facility/person to be given general medical information and/or HIV-related information.
Attach additional sheets as necessary. It is recommended that blank lines be crossed out prior to signing.**

Name and address of facility/person to be given general medical and/or HIV-related information:

Reason for release, if other than stated on page 1:

If information to be disclosed to this facility/person is limited, please specify:

Name and address of facility/person to be given general medical and/or HIV-related information:

Reason for release, if other than stated on page 1:

If information to be disclosed to this facility/person is limited, please specify:

The law protects you from HIV related discrimination in housing, employment, health care and other services. For more information call the New York State Division of Human Rights Office of AIDS Discrimination Issues at **1-800-523-2437** or (212) 480-2522 or the New York City Commission on Human Rights at **(212) 306-7500**. These agencies are responsible for protecting your rights.

My questions about this form have been answered. I know that I do not have to allow release of my medical and/or HIV-related information, and that I can change my mind at any time and revoke my authorization by writing the facility/person obtaining this release. I authorize the facility/person noted on page one to release medical and/or HIV-related information of the person named on page one to the organizations/persons listed.

Signature _____ Date _____
(Subject of information or legally authorized representative)

If legal representative, indicate relationship to subject: _____

Print Name _____

Client/Patient Number _____

HIPAA Compliant Authorization for Release of Medical Information and Confidential HIV* Related Information

Complete information for each facility/person to be given general medical information and/or HIV-related information.
Attach additional sheets as necessary. Blank lines may be crossed out prior to signing.

Name and address of facility/person to be given general medical and/or HIV-related information:

Reason for release, if other than stated on page 1:

If information to be disclosed to this facility/person is limited, please specify:

Name and address of facility/person to be given general medical and/or HIV-related information:

Reason for release, if other than stated on page 1:

If information to be disclosed to this facility/person is limited, please specify:

Name and address of facility/person to be given general medical and/or HIV-related information:

Reason for release, if other than stated on page 1:

If information to be disclosed to this facility/person is limited, please specify:

If any/all of this page is completed, please sign below:

Signature _____ Date _____

Client/Patient Number _____

Notice Prohibiting Redisclosure of Confidential Information

This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for further disclosure. Disclosure of confidential HIV information that occurs as the result of a general authorization for the release of medical or other information will be in violation of state law and may result in a fine or jail sentence or both.

(Source: Public Health Law § 2782(5); 10 N.Y.C.R.R. § 63.5)

SAMPLE 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.

General Information

Information regarding your health care, including payment for health care, is protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Any HIV-related information is also protected by a New York law, Article 27-F of the Public Health Law ("Article 27-F"). Under these laws, [insert name of health care provider] may not disclose any health related information about you except as permitted by both laws.

Your Rights

Under HIPAA you have certain rights regarding your health information. You have the right to:

- ✓ Receive a copy of this notice;
- ✓ Request restrictions on certain uses and disclosures of your health information;
- ✓ Request that we communicate with you by alternative means or at an alternative location;
- ✓ Inspect and copy your own health information which we maintain, except to the extent that the information contains psychotherapy notes or information compiled for use in a civil, criminal or administrative proceeding or in other limited circumstances;
- ✓ Request that we amend health care information maintained in our records;
- ✓ Receive an accounting of certain disclosures of your health related information which we made during the six years prior to your request.

How and When We May Disclose Your Health Information

We understand that the privacy of your health information is important. We will take reasonable measures to safeguard your confidential health related information. Generally, we must obtain your written consent before we can disclose any HIV related information about you. For example, we must obtain your written consent before we can disclose information to your health insurer in order to be paid for services. Under New York law, we generally need your permission to disclose health information about you to others for the purpose of providing you treatment or medical services. However, we may disclose HIV related information about you without your consent to a health care provider or health facility when we decide the provider or facility needs to know it in order to provide appropriate care or treatment to you, your child or your contacts.¹ We may also disclose your health information, including HIV related information, to certain private and government oversight authorities responsible for monitoring and evaluating our services.

There are a few circumstances when we can disclose HIV related information about you *without* your written consent. These are:

- Among our own staff, in accordance with a written protocol;
- To the State Department of Health for public health monitoring and partner notification;
- To an authorized agency in connection with the foster care or adoption of a child;
- For medical education or in connection with organ, tissue or fluid transplants;
- To appropriate authorities when relevant to a report of suspected child or elder abuse or neglect;
- As allowed by a court order;
- In limited circumstances when someone may have been exposed to HIV while on the job;
- In limited circumstances a physician may disclose HIV related information about a minor to the minor's parent or guardian;
- For organ or tissue donation.

¹ A "contact" means (1) an identified spouse or sexual partner, (2) a needle-sharing partner, or (3) an occupationally exposed person.

We can disclose general health information (other than HIV related information) about you *without* your written permission in the following circumstances:

- To avert a serious threat to public health or safety;
- For certain law enforcement purposes;
- Through a written agreement to outside contractors (called "business associates") that provide us services;
- For national security purposes;
- To correctional facilities regarding inmates;
- To funeral directors, coroners and medical examiners;
- To the Food and Drug Administration for product monitoring and recall;
- For Workers' Compensation;
- In facility directories, if you do not object;
- For research if certain requirements are met.

Before we can use or disclose any information about your health in a manner which is not described above, we must first obtain your specific written consent allowing us to make the disclosure. Any such written consent may be revoked by you in writing.

Our Responsibilities

We are required by law to maintain the privacy of your health information and to provide you with notice of our legal duties and privacy practices with respect to your health information. We are required by law to abide by the terms of this notice. We reserve the right to change the terms of this notice and to make new notice provisions effective for all protected health information we maintain. *[Insert description of how the covered entity will provide individuals with a revised notice.]*

Complaints and Reporting Violations

You may complain to *[name of provider]* and the Secretary of the United States Department of Health and Human Services if you believe that your privacy rights have been violated under HIPAA. *[Insert description of how a complaint is filed with the covered entity.]* You will not be retaliated against for filing such a complaint.

If you believe your rights have been violated under Article 27-F (which protects the confidentiality of HIV related information about you), you may file a complaint with the New York State Department of Health and/or file a lawsuit. The Health Department's AIDS Institute has a special unit that takes Article 27-F complaints. Its HIV Confidentiality Hotline is 800-962-5065. The Department of Health may impose a fine of up to \$5,000 per violation. Criminal penalties may be imposed if the violation was "willful."

Contact

For further information, contact *[insert name or title and telephone number of contact.]*

Effective Date

[Insert date on which notice became effective.]

Acknowledgment

I hereby acknowledge receiving a copy of this notice.

Patient signature

Date

**SAMPLE
BUSINESS ASSOCIATE AGREEMENT**

XYZ Service Center ("the Center") and the _____
(Name of health care provider)

("the Provider") hereby enter into an agreement whereby the Center agrees to provide

(Nature of services to be provided)

Furthermore, the Center:

(1) acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received from the Provider identifying or otherwise relating to the Provider's patients, it is fully bound by the provisions of the Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. Parts 142, 160 and 164, and may not use or disclose the information except as permitted or required by this Agreement or by law;

(2) agrees to use appropriate safeguards (*can define with more specificity*) to prevent the unauthorized use or disclosure of the protected information;

(3) agrees to report to the Provider any use or disclosure of the protected information not provided for by this Agreement of which it becomes aware (*insert negotiated time & manner terms*);

(4) agrees to ensure that any agent, including a subcontractor, to whom the Center provides the protected information received from the Provider, or created or received by the Center on behalf of the Provider, agrees to the same restrictions and conditions that apply through this agreement to the Center with respect to such information;

(5) agrees to provide access to the protected information at the request of the Provider, or to an individual as directed by the Provider, in order to meet the requirements of 45 C.F.R. § 164.524 which provides patients with the right to access and copy their own protected information (*insert negotiated time & manner terms*);

(6) agrees to make any amendments to the protected information as directed or agreed to by the Provider pursuant to 45 C.F.R. § 164.526 (*insert negotiated time & manner terms*);

(7) agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the Provider, or created or received by the Center on behalf of the Provider, to the Provider or to the Secretary of the Department of Health and Human Services for purposes of the Secretary determining the Provider's compliance with HIPAA (*insert negotiated time & manner terms*);

(8) agrees to document disclosures of protected information, and information related to such disclosures, as would be required for the Provider to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. § 164.528 (*insert negotiated time & manner terms*); and

(9) agrees to provide the Provider or an individual information in accordance with paragraph (8) of this agreement to permit the Provider to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. § 164.528 (*insert negotiated time & manner terms*).

Termination

(1) The Provider may terminate this agreement if it determines that the Center had violated any material term;

(2) Upon termination of this agreement for any reason, the Center shall return or destroy all protected information received from the Provider, or created or received by the Center on behalf of the Provider. This provision shall apply to protected information that is in the possession of subcontractors or agents of the Center. The Center shall retain no copies of the protected information.

(3) In the event that the Center determines that returning or destroying the protected information is infeasible, the Center shall notify the Provider of the conditions that make return or destruction infeasible (*insert negotiated time & manner terms*). Upon notification that the return or destruction of the protected information is infeasible, the Center shall extend the protections of this Agreement to such protected information and limit further uses and disclosures of the information to those purposes that make the return or destruction infeasible, for so long as the Center maintains the information.

Executed this ____ day of _____, 200__.

President
XYZ Service Center
[address]

Provider Director
[Name of the Provider]
[address]