HIPAA Compliance Checklist
For HIV Providers
Covered by HIPAA’s Privacy Rule

Revised February 2008

☐ **Determine if your agency/unit is covered by and must comply with HIPAA**

☐ Determine whether you are a **covered entity** that transmits personal health information **electronically** in connection with specified health care transactions – and must therefore comply with HIPAA’s Privacy Rule

☐ **Personnel Designations**

☐ Designate **staff member(s)** to:

  ☐ Be the Privacy Officer
  ☐ Process patient complaints
  ☐ Process patient requests for accountings of disclosures
  ☐ Process patient requests to access records
  ☐ Review denials of patient requests to access records
  ☐ Process patient requests to amend information contained in records

☐ Document these personnel designations

☐ **Training**

☐ Establish a **training schedule** and curriculum

☐ Train each member of your workforce about HIPAA

☐ **Safeguards**

☐ Conduct a **risk assessment** to determine whether health information is adequately protected

☐ Consult with technical experts and computer support personnel regarding HIPAA’s **technical and electronic** requirements
Design and put in place appropriate technical, administrative and physical safeguards to protect health information from improper use or disclosure.

**Complaints**

- Establish a policy and procedure for patients to file complaints concerning your HIPAA compliance.
- Establish a policy and procedure for sanctions to be imposed against members of the workforce that violate HIPAA’s provisions or your privacy policies.
- Establish procedures for documenting sanctions imposed and mitigating effects of wrongful disclosures.

**Required Forms**

- **Patient Notice of Your Privacy Practices (HIPAA Privacy Notice):** Draft a patient notice – post in prominent location, have copies available to give to patients.
- **Consent (HIPAA Authorization Form):** Use the NYS Department of Health’s approved HIPAA-Compliant Authorization for Release of Confidential HIV Related Information (Form DOH-2557).
- Establish a procedure for giving copies of signed consent forms to patients.
- Establish a procedure for patients to revoke the consent in writing.

**Accounting**

- Establish a system to track and document all relevant uses and disclosures of health information.
- Establish a procedure to provide patients with an accounting of uses and disclosures of health information upon request.

**Limiting Disclosures to Minimum Necessary**

- Identify members of your workforce who need access to health information to carry out their duties, the categories of information to which they need access, and any conditions to their access that exist.
☐ Implement a policy and procedure to limit routine or reoccurring disclosures and requests to the minimum necessary achieve the purpose of the disclosure

☐ Develop criteria for limiting the minimum necessary information in non-routine disclosures or requests and establish procedure for reviewing requests in accordance with the criteria

☐ Develop and circulate to all staff your “need-to-know” list and policy

☐ **Patient Access to Records**

☐ Establish a procedure for reviewing patient requests to access their records

☐ Establish a procedure for providing patients with access to their records – determine a reasonable, cost-based fee if applicable

☐ Establish a policy and procedure to review denials of patient requests to access records

☐ Establish a procedure for processing patient requests to amend information contained in their own records – designate a staff member to process such requests

**REMEMBER:** Document, document, document – all policies, procedures, personnel designations and administrative measures must be documented.