

## **PRIVACY OF INDIVIDUALS SERVED**

### **I. PURPOSE**

The purpose of this policy is to protect the privacy of individuals served by Jefferson Parish Human Services Authority (JPHSA) in a manner that respects the rights of the individual, facilitates service delivery, ensures safety, and meets relevant legal standards.

### **II. POLICY**

JPHSA respects the rights of all individuals with mental health, addictive disorders and/or developmental disability needs. This respect is reflected by ensuring that the individual's right to privacy of information is recognized as one of the cornerstones of an effective relationship with the Authority. Individuals served provide sensitive information to JPHSA staff as part of working to resolve their problems and achieve their goals; trust in how staff members handle this information is a basic element in a positive working relationship.

### **III. PROCEDURES**

- A. In concurrence with the policies of the JPHSA Board, only information that is essential to provide services and supports is gathered. Extraneous or unnecessarily intrusive information is not obtained.
- B. The uses of information to fulfill administrative and financial responsibilities are limited to those sanctioned by law and regulation.
- C. Every JPHSA employee, student, intern, resident or volunteer as well as all employees of agencies contracted with JPHSA are informed of all relevant procedural requirements, are trained on them, and are expected to comply with them. Employees, students, interns, residents and volunteers shall sign the JPHSA "Privacy Agreement" prior to their engagement with the Authority. (See Attachment A.) All contractors shall sign the JPHSA "HIPAA Business Associate Addendum" prior to implementation of contracts. (See Attachment B.)
- D. Every JPHSA employee shall participate in annual in-service education regarding the privacy of individuals served.
- E. Electronically maintained or transmitted information of individuals served is safeguarded as carefully as verbal transactions or paper records using necessary staff procedures and technological protections.
- F. JPHSA ensures compliance with the Health Insurance Portability and Accountability Act (HIPAA) including providing a copy of the Privacy Notice to all individuals served, informing them of their privacy rights; training all staff on privacy and confidentiality; and, having a complaint procedure for use with perceived violations.
- G. Every piece of paper that is generated by JPHSA, containing identifying information for an individual served, that is no longer needed **and** is not part of the individual's service record or otherwise required to be retained, must be shredded according to the JPHSA Records Retention Schedule. (See Records Management, ADM.08.) This includes "scratch paper" or notes. (Note: Telephone message slips are not included in the client record; however, such messages should be

documented as informational notes in the JPHSA electronic health record.)

- H. Particular attention must be given to safeguarding information when discussing an individual served with other staff, whether in person, by telephone, or other electronic means. Discussion shall only occur among individuals involved in the provision of services to the individual or who have a need to know in order to fulfill their assigned duties. An individual's information shall not be discussed in areas such as waiting rooms, hallways, or other areas where information can be overheard by others.
- I. Confidentiality of information must be maintained when revealing data over JPHSA e-mail. Names of individuals served and other identifying information shall be avoided or minimized. Messages shall be deleted after they have been received and action taken on them. Correspondence by e-mail to individuals outside of JPHSA's e-mail system shall not contain any names or other protected health information.
- J. Information sent to individuals served by mail shall be placed in envelopes that do **not** contain a clinic or specific program identifier in the return address. The general address for JPHSA at each site should be used.
- K. When leaving a telephone message for an individual served or family member, either with another person, by voice mail or on an answering machine, do not identify any specific JPHSA clinic or program.
- L. Do not contact individuals served at their places of employment unless there is an emergency and only with their permission. The emergency contact person listed in the record shall only be contacted in a true emergency.
- M. Computer monitors shall be placed where they cannot be read by individuals served or visitors. Computers shall be "locked" when an employee is away from his/her work area.
- N. Computer access to the JPHSA electronic health record is determined by job function. Division Directors or Supervisors determine the level of other computer access required for each of their employees to perform their jobs. (See Network Security & Integrity, MIS.02.)
- O. Supervisors are responsible for assuring that employees who have access to confidential information, whether it is electronic, hard copy, or orally, are informed of their responsibilities.
- P. Family members, significant others and any other individuals included in the plan of treatment/service shall be allowed to attend an individual's service delivery session. Family members, significant others and any other individual **not** included in the plan of treatment/service shall be allowed to attend an individual's service delivery only upon the written authorization of the individual served or his/her parent or legal guardian and the approval of the service provider.

#### **IV. CONTINUANCE OF CONFIDENTIALITY**

Information contained in the record of an individual served shall continue to remain confidential after the record is closed, scanned, or destroyed as some identifying information is kept even when a record is destroyed.

#### **V. SANCTIONS FOR UNAUTHORIZED RELEASE OF INFORMATION**

**Adopted: 12/06/10**  
**Implemented: 12/06/10**  
**Reviewed:**  
**Revised:**

- A. Any occasion of unauthorized release of information about an individual served by a JPHSA employee or contractor is managed as a critical incident per JPHSA policy (Incident Reporting and Review, ADM.03) and those policies and procedures established under the Federal HIPAA rules.
- B. Any employee who violates JPHSA policies or procedures regarding the safeguarding of information of an individual served is subject to disciplinary action up to and including termination from employment.
- C. An employee who knowingly and willfully violates State or Federal law for improper use or disclosure of an individual's information is subject to criminal investigation and prosecution and/or civil monetary penalties.

**References**

Health Insurance Portability & Accountability Act of 1996, 45 CFR, Parts 160 & 164, HIPAA Privacy Rule  
Code of Federal Regulations, Title 42 – Public Health, Rev. 2002  
Louisiana Administrative Code: Title 48, Section 531, Patient Rights  
Office of Citizens with Developmental Disabilities Licensing Requirements, Section 30.13  
Council On Accreditation: PA-RPM, 6.01- 6.02; PA-CR 2.02; and, PRM 8.01

**Adopted: 12/06/10**  
**Implemented: 12/06/10**  
**Reviewed:**  
**Revised:**

**Jefferson Parish Human Services Authority (JPHSA)**

**Privacy Agreement**

I understand that I may have access to written and/or electronic information or records which may contain private and personal information about staff or individuals served. Access to these records will be based on a "need to know" in order to complete my assigned duties.

I further understand and agree that I am not to disclose any private or personal information without proper consent of the individual involved in the disclosure.

I understand that all user IDs, passwords or devices to access data are issued on an individual basis. I further understand that I am solely responsible for all information obtained through system access, using my unique identification. At no time will I allow another person to use my password or other device to access private information or records.

I understand that accessing or disclosing private information or records or causing private information to be accessed or released, outside the scope of my assigned duties, will constitute a violation of this agreement and may result in disciplinary action up to and including dismissal from JPHSA and including any penalties or sanctions provided by Federal or State laws.

I acknowledge that there are laws, regulations and policies concerning access, use, maintenance and disclosure of private information or records; and, I agree that it is my responsibility to assure the privacy of all information to which I may have access, even after my assigned duties with JPHSA have ended. I further acknowledge that I have reviewed, understand, and agree to abide by the JPHSA "Privacy of Individuals Served" Policy ADM 1.10.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**Adopted: 12/06/10**  
**Implemented: 12/06/10**  
**Reviewed:**  
**Revised:**

### HIPAA Business Associate Addendum

This Business Associate Addendum is hereby made a part of this contract in its entirety as an Attachment to the contract.

1. The U. S. Department of Health and Human Services has issued final regulations, pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), governing the privacy of individually identifiable health information. See 45 CFR Parts 160 and 164 (“HIPAA Privacy Rule”) and 42 CFR Part 2 (confidentiality of alcohol and drug abuse patient records). The Jefferson Parish Human Services Authority (“JPHSA”), as a “Covered Entity” as defined by HIPAA, is a provider of health care, a health plan, or otherwise has possession, custody or control of health care information or records.
2. “**Protected health information**” (“PHI”) means individually identifiable health information including all information, data, documentation and records, including but not limited to demographic, medical and financial information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual or payment for health care provided to an individual; and that identifies the individual or which JPHSA believes could be used to identify the individual. “**Electronic protected health information**” means PHI that is transmitted by electronic media or maintained in electronic media. “**Security incident**” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
3. Contractor is considered a Business Associate of JPHSA, as contractor either: **(A)** performs certain functions on behalf of or for JPHSA involving the use or disclosure of protected individually identifiable health information by JPHSA to contractor, or the creation or receipt of PHI by contractor on behalf of JPHSA; or **(B)** provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, financial or social services for JPHSA involving the disclosure of PHI.
4. Contractor agrees that all PHI obtained as a result of this contractual agreement shall be kept confidential by contractor, its agents, employees, successors and assigns as required by HIPAA law and regulations and by this contract and addendum.
5. Contractor agrees to use or disclose PHI solely **(A)** for meeting its obligations under this contract, or **(B)** as required by law, rule or regulation or as otherwise permitted under this contract or the HIPAA Privacy Rule.
6. Contractor agrees that at termination of the contract, or upon request of JPHSA, whichever occurs first, contractor will return or destroy (at the option of JPHSA) all PHI received or created by contractor that contractor still maintains in any form and retains no copies of such information; or if such return or destruction is not feasible, contractor will extend the confidentiality protections of the contract to the information and limit further uses and disclosure to those purposes that make the return or destruction of the information infeasible.
7. Contractor will ensure that its agents, employees, subcontractors or others to whom it provides PHI received by or created by contractor on behalf of JPHSA agree to the same restrictions and conditions that apply to contractor with respect to such information. Contractor also agrees to take all reasonable steps to ensure that its employees’, agents’ or subcontractors’ actions or omissions do not cause contractor to breach the terms of this Addendum. Contractor will use all appropriate safeguards to prevent the use or disclosure of PHI other than pursuant to the terms and conditions of this contract and Addendum.
8. Contractor shall, within 3 days of becoming aware of any use or disclosure of PHI, other than as permitted by this contract and Addendum, report such disclosure in writing to the person(s) named in section 14 (Terms of Payment), page 1 of the CF-1.
9. Contractor shall make available such information in its possession which is required for JPHSA to provide an

**Adopted: 12/06/10**  
**Implemented: 12/06/10**  
**Reviewed:**  
**Revised:**

accounting of disclosures in accordance with 45 CFR 164.528. In the event that a request for accounting is made directly to contractor, contractor shall forward such request to JPHSA within two (2) days of such receipt. Contractor shall implement an appropriate record keeping process to enable it to comply with the requirements of this provision. Contractor shall maintain data on all disclosures of PHI for which accounting is required by 45 CFR 164.528 for at least six (6) years after the date of the last such disclosure.

- 10. Contractor shall make PHI available to JPHSA upon request in accordance with 45 CFR 164.524.
- 11. Contractor shall make PHI available to JPHSA upon request for amendment and shall incorporate any amendments to PHI in accordance with 45 CFR 164.526.
- 12. Contractor shall make its internal practices, books, and records relating to the use and disclosure of PHI received from or created or received by contractor on behalf of JPHSA available to the Secretary of the U. S. DHHS for purposes of determining JPHSA’s compliance with the HIPAA Privacy Rule.
- 13. Compliance with Security Regulations - In addition to the other provisions of this Addendum, if Contractor creates, receives, maintains, or transmits electronic PHI on JPHSA’s behalf, Contractor shall: **(A)** Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of JPHSA; **(B)** Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; **(C)** Report to JPHSA any security incident of which it becomes aware; **(D)** Contractor shall sign for the receipt of any paper records or digital media received from JPHSA that contains PHI. The original receipt shall be filed with the contract at JPHSA and the contractor shall receive a copy of the receipt. The receipt form is on page 2 of this addendum.
- 14. Contractor agrees to indemnify and hold JPHSA harmless from and against all liability and costs, including attorneys’ fees, created by a breach of this Addendum by contractor, its agents, employees or subcontractors, without regard to any limitation or exclusion of damages provision otherwise set forth in the contract.
- 15. Notwithstanding any other provision of the contract, JPHSA shall have the right to terminate the contract immediately if JPHSA determines that contractor has violated any material term of this Addendum.

**Verification of Receipt of PHI**

I have received the following PHI from JPHSA:

---



---



---

I agree to abide by the Security Regulations described in item # 13 of the JPHSA HIPAA Business Associate Addendum.

\_\_\_\_\_  
Contractor signature

\_\_\_\_\_  
Date

**Adopted: 12/06/10**  
**Implemented: 12/06/10**  
**Reviewed:**  
**Revised:**