

# IBHRS PROVIDER USER AGREEMENT

The Iowa Behavioral Health Reporting System (IBHRS) is the statewide integrated substance use disorder and problem gambling treatment data reporting system. In order to activate and maintain an IBHRS user account, the applicant must agree to the following:

1. Only access data in IBHRS to perform legally authorized functions.
2. Read and abide by the IBHRS Security and Confidentiality Policy including procedures to safeguard user name(s) and password(s) against unauthorized use (refer to Appendix A).
3. **Protection of Data:** Ensure use of IBHRS is consistent with the IBHRS Security and Confidentiality Policy (Appendix A) and all applicable local, state, and federal laws and regulations, including but not limited to Iowa Code chapter 715C, HIPAA, 42 CFR Part 2, Iowa Code chapters 22, 125 and 135 and all other current and future laws and regulations relating to spamming, privacy, data protection, and consumer protection.
4. Access records only by using the authorized user id and password.

**Failure to abide by this agreement may result in immediate suspension or termination of access to IBHRS.**

## Section A

First Name: Middle Initial: Last Name:

Licensed Provider (Agency) Name:

Phone: Email:

## Section B

Provider IBHRS Administrator Name:

Title:

Phone: Email:

This form must be signed electronically by both the individual requesting access (Provider IBHRS User) and the organization's Provider IBHRS Administrator.

## Electronic Signature Agreement

By checking the "I Accept" box, you agree your electronic signature is the legal equivalent of a manual signature on this Agreement.

☐ I accept

**By signing below, I agree to the above conditions and will comply with Iowa and Federal law:**

*Signature of Provider IBHRS User*

*Signature of Provider IBHRS Administrator*

## FOR IDPH USE ONLY

User Name Assigned:

Date Activated:

Provider License Number:

User Terminated/Deactivated:

Date:

NOTE: THIS FORM MUST BE KEPT ON FILE WITH THE PROVIDER IBHRS ADMINISTRATOR AND AVAILABLE BY REQUEST FOR AUDIT PURPOSES.

# SECURITY AND CONFIDENTIALITY POLICY

## Background

The Iowa Department of Public Health (referred to as “Department”) licenses substance use disorder treatment providers and supports problem gambling treatment providers throughout the state. Pursuant to Iowa Code chapter 125 and 641 Iowa Administrative Code Chapter 155 and the Department’s policies and procedures, licensed substance use disorder treatment programs are required to collect and report patient data, including identifying information, screening, admission, discharge, and service data. The Department uses these data:

- 1) To assist with data and reporting requirements imposed by the federal block grant;
- 2) To access other federal funding programs;
- 3) To assist the state in planning and service delivery for substance use and gambling disorder treatment;
- 4) To perform evaluation and quality assurance functions;
- 5) To effectively monitor service delivery and utilization and assure that treatment is provided is within the appropriate standards of care; and
- 6) To ensure continuity and coordination of care, recovery support, and program linkages.

### The Iowa Behavioral Health Reporting System (IBHRS)

The Iowa Behavioral Health Reporting System (IBHRS) is the statewide integrated substance use disorder and problem gambling treatment reporting system designed to meet the aforementioned Departmental needs and obligations.

## Purpose

The purpose of this policy is to address the need to provide appropriate security and confidentiality protection to the data contained in IBHRS. The confidentiality of this information must be distinguished from issues of privacy. Privacy is concerned with the control individuals exert over the release of their personal information. Under this policy, confidentiality is concerned with how the information provided to IBHRS by individuals is accessed, collected, stored, used, and provided to other individuals and organizations. In addition, security addresses the physical and other measures taken to guard against attack or breach of this information.

## Definitions

- 1) All terms used in this policy have the same meaning as those terms used in the state law and administrative rules that authorize IBHRS.
- 2) “Provider IBHRS User” means an individual who has completed an enrollment form that specifies the conditions under which the system can be accessed and who has been issued system credentials by the Department.
- 3) “Provider IBHRS Administrator” means the main IBHRS point of contact for an agency/program.
- 4) “Confidentiality” means limiting the collection, access, use, storage, and release of information from Provider IBHRS users to IBHRS and from IBHRS in a manner consistent with Federal and state law.
- 5) “Security” means physical and other measures taken to guard against attack or breach.

## Confidentiality

Based on Iowa Code chapter 715C, HIPAA, 42 CFR Part 2, Iowa Code chapters 22, 125 and 135, rules, and general principles of confidentiality, the security and confidentiality policy for IBHRS is as follows:

- 1) Patient data in IBHRS are confidential under state and federal law. Provider IBHRS Users shall gather, store, log, archive, maintain, transfer, use, and disclose Patient data only in a manner consistent with state and federal laws.
- 2) Provider IBHRS Users:
  - a) Only Provider IBHRS Users may provide information to or receive information from IBHRS.
  - b) All Provider IBHRS Users are required to complete an IBHRS User Agreement and to read and abide by this security and confidentiality policy.
  - c) The Department shall seek appropriate penalties for any misuse of information in IBHRS by any Provider IBHRS User or any other party, including pursuing any sanction authorized under state or federal law.

## Security

- 1) Access to IBHRS is authorized under the conditions required to perform a legally authorized function of the organization.
- 2) A Provider IBHRS User shall:
  - a) Review and abide by the IBHRS Security and Confidentiality Policy;
  - b) Renew the security certification within IBHRS annually;
  - c) Maintain confidentiality;
  - d) Maintain a unique login to access IBHRS. Under no circumstances shall user IDs and passwords be shared;
  - e) Make every effort to protect IBHRS screens from unauthorized view;
  - f) Assure virus protection is in place for each computer on which IBHRS is accessed within the organization; and
  - g) Not copy confidential data onto personal or removable devices (including, but not limited to, flash drives, portable hard drives, memory cards, DVDs, CDs, cell phones, etc.).
- 3) IBHRS information in a paper copy shall not be left where it is visible for unauthorized personnel.
- 4) Any activity that could jeopardize the proper function and security of IBHRS shall not be conducted.
- 5) The Provider IBHRS Administrator at each organization must terminate access for an authorized user who no longer requires access.
- 6) Violators of this policy will be restricted from IBHRS by the Provider IBHRS Administrator at the organization. The Department shall seek appropriate penalties for any misuse of information in IBHRS by any Provider IBHRS User or any other party, including pursuing any sanction authorized under state and federal law.

## Penalties

The Department shall seek appropriate penalties for any misuse of information in IBHRS by any Provider IBHRS User or any other party, including pursuing any sanction authorized.