



CASA Database: Implementation Overview and Checklist

Greetings from your CASA database design team!

Overview:

The CASA database is ready for the next stage of implementation. Access to the system is obtained by:

- ❑ Attending and Completing Basic CASA database training (refresher courses are also available). This training is scheduled by OCCF and offered by the CASA database design team.
- ❑ Activation of a login by OCCF Web-support.

CASA Database Training:

CASA database training involves an interactive, hands-on 2 hour web-based training session. The sessions are limited to a maximum of 4 participants per session. The training gives basic level instruction on how to use and access the system. If you haven't done so already, you can sign up by emailing occfwebsupport@fc.state.or.us.

Login Activation:

- ❑ All users **MUST** sign and fax back a ***2h systems user agreement form and HIPAA Confidentiality Agreement***. OCCF web support will activate the CASA user once all forms are signed and received by OCCF. A fax cover sheet is included in this packet.



2h Systems User Agreement

User Agreements and Acknowledgements

User (referred to as “login”) will adhere to the following. Any deviation from the stated items indicates a willful misuse of the system and can constitute login termination, and in some extreme cases, court action.

- User agrees that sharing logins constitutes immediate login termination.
- User understands that when any database transaction occurs within any of the existing “tools” or modules, his or her login ID is “stamped” upon that transaction thereby creating a data audit trail.
- User agrees that when the tool that s/he has access to contains HIPAA-sensitive data (confidential health information), s/he will sign (Agency’s Name) ’s HIPAA agreement prior to logging in to the (Agency’s Name) Web Framework.
- User understands that training is an essential component of the system and will schedule training through Web Support or with your Agency trainer as soon as possible.
- User agrees that exporting confidential or sensitive data from the system and then storing and/or communicating aforementioned data in an unsecured manner constitutes a violation of (Agency’s Name) ’s HIPAA or confidentiality agreements.
- User understands that both the speed of the workstation (PC) and the Internet connection (dialup, DSL, cable, fiber-optic) all affect “speed” of the web applications within the (Agency’s Name) Web Framework
- “Willful Misuse” includes – **but is not limited to** - Denial of Service activities, intentionally entering or modifying data in a manner inconsistent with the Agency’s desires, sharing logins, violating HIPAA policies, violating Agency’s confidentiality policies, and intentionally sharing information that compromises the security of the Web Framework.
- User understands that sharing of login information as well as distributing links to the Production site to unauthorized users constitutes willful misuse of the system and can result in the items described as “willful misuse”.

Signature of User

Date

*The signature of this form indicates that the Authorizer **acknowledges** and **accepts** the preceding Agreements and Acknowledgements*



Basic HIPAA and Confidentiality form for CASA staff:

To be used prior to initial login:

Beginning on June 30, 2009 Client and Family Specific data (names, addresses, DOB, etc) will now be collected and stored electronically on OCCF's Web based applications system through an electronic module known as the CASA web-database. Because CASA collects private health information and may be run by medical health care organizations, the OCCF CASA program may now subject to HIPAA (Health Insurance Portability and Accountability Act) provisions and is classified as a Covered Entity for HIPAA purposes. As a Covered Entity, the CASA program is entitled to purpose specific use of Protected Healthy Information (PHI) but must take steps to ensure that this information is used only for the purpose for which it is collected. In addition, safeguards must be in place to protect the privacy of the information collected for this program. This document outlines the security measures users of the online system must be aware of and employ prior to first logging into the online system for the first time. These provisions do not represent a comprehensive list of security measures employed. They are meant only as a minimum list of measures that all users must observe before any use of the system.

I: Secure Logins:

- All users will be provided with a system specific login name and password. This may not be shared with other users and should be used only by the individual assigned the specific login.
- Logins and passwords must be deleted upon termination of CASA program staff.

II: Minimum Necessary Standard:

- All users must abide by the Minimum Necessary Standard **[45 CFR 164.502(b), 164.514(d)]**: That is, protected health information (PHI) will be used only for the purpose for which it is collected. It can only be used to satisfy the basic data collection elements necessary to implement the CASA program, document compliance with its mission, and monitor follow up with activities with program clients and their representatives. The Privacy Rule **[45 CFR Parts 160 and 164]** generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose.

III: Privacy Practice notice: [45 CFR 164.520]

- Covered Entities must provide a notice of its privacy practices: This notice must state their duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the notice. It must describe the individual's rights, right to complain to HHS and to the covered entity if they feel their privacy rights have been violated. It must include a point of contact for further information and for making complaints to the covered entity. **No client data may be collected without the client's, or the client's representative's, written notice.** No data should be entered in the CASA program without this prior authorization. No data should be disclosed to any agency, individual or third party without first reviewing and documenting the entities entitlement to receive the protected health information

IV: Securing of hard copy information: Each local agency must have a written plan to secure and protect access to computer screens and access to hard copy data produced from the CASA web-database system.

Name: _____

Please print

Signature: _____

Date: _____



**OCCF On-line Applications System
Profile Set-up Request
Fax to occfwebsupport: (503) 378-8395**

User Information (All fields must be completed)	
Program Name (Section Name)	
Last Name	
First Name	
Classification	
Phone Number	
Email Address	
Hire Date	
FTE	
Supervisor Approval	
Supervisor Name (please print)	
Supervisor Signature	

Fax completed form to (503) 378-8395 Attn: OCCF Websupport or email the completed signed form to occfwebsupport@fc.state.or.us.



FAX COVER SHEET

ATTN: OCCF WEB SUPPORT

FAX NUMBER: 503-378-8395

FROM:

REGARDING: USER SET-UP

PHONE:

ATTN: OCCF WEB SUPPORT

PAGES:

COMMENTS