



myAvatar Electronic Health Record Policy

Effective Date 06/19/2019
Revised Date 12/15/2021

Veronica Kelley, DSW, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to ensure secure maintenance of DBH client medical records in the myAvatar electronic health record (EHR) system. Electronic protected health information (ePHI) stored, accessed and added to this system will be maintained in a manner that assures storage, access, receipt, and transmission is secure, prohibiting unauthorized access.

This policy applies to all software and applications within the myAvatar EHR system and to all DBH workforce members, business associates, contracted employees, consultants, volunteers, other County departments, and all others whom maintain an authorized business agreement and/or business need to access DBH ePHI.

Purpose

To outline requirements related to the DBH myAvatar system and provide reference to DBH data system policies and procedures related to the protection, security, integrity, use and accessibility of ePHI.

Definition(s)

Access Control: The ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. This includes management of user rights and/or access privileges to the myAvatar system based on "user-role" status.

Account Creation: The process of creating an account in myAvatar granting the user/workforce member permission to access or use of a set of files or data.

Confidential Data: Includes, but is not limited to, PHI and information that is sensitive, proprietary, or personal in nature, to which access must be restricted and in which unauthorized disclosure, theft or improper use may be harmful or compromising to an individual, process, and/or organization. Data regarded as sensitive shall be disseminated only to individuals or organizations with authorized access.

Disclosure: The release, transfer, provision of access to, or dividing in any other manner, of PHI outside the covered entity holding the information.

Electronic Protected Health Information (ePHI): Protected health information (PHI) that is produced, saved, transferred or received in an electronic form.

Continued on next page

myAvatar Electronic Health Record Policy, Continued

**Definition(s),
continued**

myAvatar Super Users: Workforce members specifically trained in myAvatar and designated at each DBH facility/site, or County-operated program, to provide support during end-user training of the myAvatar application and act as ongoing liaisons between IT and end-users.

Protected Health Information (PHI): Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. Individually identifiable information is information, including demographic data, that relates to the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and identifies the individual or for which there is reasonable basis to believe it can be used to identify the individual.

Remote Access: The ability to gain access to the DBH network from outside the network's perimeter.

Unauthorized Access: Inappropriate access, review or viewing of client medical information/PHI without authorization or job-related need/justification or other unlawful use not permitted by Confidentiality of Medical Information Act, HIPAA, WIC 5328, 42 CFR Part, or any other statutes or regulations governing the lawful access, use or disclosure of medical information/PHI.

Use: Refers to the utilization of individually identifiable health information, as well as the access, sharing, employment, application, examination, or analysis of such information by a workforce member or covered entity that maintains this information.

User-Role: The set of access permissions determined to be the minimum necessary for the user to perform their assigned job duties.

User-Role Guide: A comprehensive guide which lists designated user-roles based upon the job classifications of users grouped into categories which establish identical access and privileges/permissions. The guide is approved by the DBH Privacy Officer and DBH Security Officer, and is utilized as the standard for determining and establishing user access, capabilities, privileges and permissions in myAvatar.

Workforce Member(s)/Users: Employees, volunteers, trainees, students, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they receive pay from the covered entity.

Continued on next page

myAvatar Electronic Health Record Policy, Continued

myAvatar User Account Eligibility To be eligible for a myAvatar user account (MAUA), an individual must be a current DBH or another County department workforce member, or other entity or individual who has an authorized business need to access DBH client PHI (e.g., DBH contract provider or contract provider staff) whom requires access to myAvatar to perform functions of the established agreement or designated job duties.

Access Control DBH Security Officer will ensure DBH Information Technology (IT) completion of ongoing implementation and maintenance of myAvatar access controls, reviews, features, updates, workforce clearances, integrity, and other required activities in accordance with the Health Insurance Portability and Accountability Act (HIPAA), Security Rule Title 45, Code of Federal Regulations (CFR), Part 160 and Subparts A and C of Part 164; 45 CFR §164.08, §164.310 and §164.312, and Title 42 CFR, §2.13 and §2.16.

Access to myAvatar is granted to eligible users in accordance with the *User-Role Guide*. Deviations from the established/approved *User-Role Guide*, due to a unique user-role or other unique circumstances, require prior review and approval by the DBH Privacy Officer and DBH Security Officer.

System access requires each individual user to enter a unique User I.D. and password not to be shared with any other individual; account access is disabled after five (5) unsuccessful logon attempts; and a manual reset by IT is then required.

MAUA Request Tracking It is required that all DBH workforce members submit requests for actions related to MAUA by emailing the DBH-IT-Helpdesk@dbh.sbcounty.gov, or calling (909) 386-9730. This ensures adequate tracking and response by DBH IT.

MAUA Actions Separate procedures support actions pertaining to MAUA. The table below identifies each procedure and describes its purpose:

Procedure	Purpose
myAvatar User Account Request Procedure (IT5012-1)	Describes the steps necessary to request access to myAvatar. (Supervisors)
myAvatar User Account Creation and Reinstatement Procedure (IT512-2)	Describes the steps necessary to create a new MAUA or reinstate a deactivated MAUA (Supervisor, IT, Privacy Officer, User)
myAvatar User Account Modification Procedure (IT5012-3)	Describes the steps necessary to modify a current MAUA (Supervisor, IT, Privacy Officer)

Continued on next page

myAvatar Electronic Health Record Policy, Continued

MAUA Deactivation

When *immediate* deactivation of a user account is required due to privacy, security, or safety risks, call the **DBH HelpLine at (909) 386-9730**.

Planned deactivation of MAUA shall be conducted in accordance with myAvatar User Account Deactivation Procedure (IT5012-4), which specifies in part:

- Changes in user's employment conditions that will result in deactivation of MAUA include, but are not limited to:
 - Termination of employment with DBH;
 - Interdepartmental transfer or relocation of user to a different program, unit, or division.
-

Monitoring of myAvatar

All business conducted, and content contained within myAvatar is the property of DBH, and is subject to monitoring, audit, and/or review by authorized personnel. In accordance with current DBH policies, the DBH Security Officer/designee shall regularly monitor records of information system activity, such as audit logs, access reports, and security incident tracking reports to identify discrepancies between policies and practices, and to identify any unusual behavior/activity

Upon discovery of any unusual activity, the DBH Security Officer/designee shall review the incident and take appropriate action including follow up which may involve reporting possible privacy or security incidents, or possible instances of fraud, waste, or abuse (including false claims) to DBH Office of Compliance.

Privacy and Security Safeguards

Workforce members/users accessing or utilizing myAvatar must comply with Computer and Network Appropriate Use Policy (IT5004), and Workstation and System Security Policy (COM0924), which includes, but is not limited to, the following requirements:

- Users are directly responsible for all actions resulting from the use of their unique MAUA, and **shall not** share their user I.D. or password with any other individual(s).
 - User I.D. and password specifics are further defined in the User I.D. and Password Policy (IT5009).
- Users **shall not** copy, export, download, store, save, print screen, photograph or video-graph, information from myAvatar unless:
 - Actions are an approved aspect of their job function/duties, consistent with their designated user role, or
 - The Privacy Officer and/or Security Officer provides prior written authorization.

All PHI, in electronic or paper media shall be stored, transported, and retained in accordance with DBH policies and procedures.

Continued on next page

myAvatar Electronic Health Record Policy, Continued

Electronic Signature

Workforce members/users providing treatment services electronically sign documents in myAvatar based on their unique user ID and password combination. Workforce members shall follow the guidance provided in the Privacy and Security Safeguards section of this Policy to ensure the integrity and security of their electronic signature.

Remote Access to myAvatar

Remote access to myAvatar is a privilege granted to specific users, based on their respective job function, and upon approval by DBH Executive Management. Participating in remote access to the system shall be consistent with the requirements outlined in the Remote Access Policy (IT5006), and access shall be limited to the minimum necessary required to carry out job responsibilities.

Vendor Access

DBH IT establishes Guest accounts and log in credentials to control Vendor access to myAvatar. DBH IT Security Officer/designee approves Guest accounts on an "as needed" basis. Confidentiality and data security requirements are outlined in the respective vendor contract requirements and/or terms of the business associate agreements.

Oath of Confidentiality

All workforce members are required to sign the Oath of Confidentiality (COM027) as outlined in DBH Information Notice 17-11, at hire, annually thereafter, prior to accessing PHI/ePHI, or in response to a corrective action plan.

The State Agreement between DBH and Department of Health Care Services (DHCS) requires DBH clinics/programs and contractors to obtain a signed Oath of Confidentiality from any personnel or entity, including County/State/Federal representatives, prior to disclosing any client-related records containing PHI for the purpose of reviewing job-related duties, research, monitoring/auditing, or any other business operations.

Consequences of Violations

Violations of this Policy and/or other DBH or County policies by DBH employees may result in disciplinary action(s), including progressive discipline and/or termination; and other actions, including civil and/or criminal actions.

Violations of this Policy and/or other DBH or County policies by non-County employees may result in termination of contractual agreements, and denial of access to County and/or DBH IT systems or resources;

Continued on next page

myAvatar Electronic Health Record Policy, Continued

Referenced Forms, Policies, and Procedures

This information block will guide you to all forms, policies, and procedures referenced in this Procedure.

DBH Standard Practice Manual:

- myAvatar User Account Request Procedure (IT5012-1)
- myAvatar User Account Creation and Reinstatement Procedure (IT5012-2)
- myAvatar User Account Modification Procedure (IT5012-3)
- myAvatar User Account Deactivation Procedure (IT5012-4)
- Computer and Network Appropriate Use Policy (IT5004)
- User- I.D. and Password Policy (IT5009)
- Fraud, Waste and Abuse Prevention Policy (COM0927)

DBH Information Notices:

- DBH Information Notice 17-11

Related Policy or Procedure

San Bernardino County Policy Manual:

- County Policy 09-01: Electronic Mail (E-mail) Policy or Procedure
- County Policy 09-04: Internet/Intranet Use Policy
- County Policy 14-02: Protection of Individually Identifiable Health Information
- County Policy 14-02SP1: Protections of Individually Identifiable Health Information

DBH Standard Practice Manual:

- Confidentiality of Protected Health Information (PHI) (COM0905)
- Retention of Medical Records Policy (COM0906)
- Unauthorized Access of Confidential Medical Records (COM0907)
- Authorization to Release PHI Policy (COM0912)
- Security of Protected Electronic Health Information Policy (COM0923)
- Workstation and System Security Policy (COM0924)
- Data Integrity Policy (COM0925)
- Privacy and Security Incident Sanctions Policy (COM0926)
- Transportation of Protected Health Information (PHI) Policy (COM0948)
- Transportation of Protected Health Information (PHI) Procedure (COM0948-1)
- Employee Separation Procedure (HR4006) Internet Access Policy (IT5003)
- Electronic Mail Policy (IT5005)
- Remote Access Policy (IT5006)
- Device and Media Controls Policy (IT5008)

Reference(s)

- Code of Federal Regulations, Title 42, Part 2, Final Rule
- Code of Federal Regulations, Title 45, Parts 160 and 164, Modifications to the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules
- Welfare and Institutions Code 5328