Amendment No. 9 to Master System Agreement

This Amendment to Master System Agreement ("Amendment") is entered into by and between OCHIN, Inc. ("OCHIN") and County of Monterey, a political subdivision of the State of California("Member") and is effective as of April 1, 2015 ("Effective Date").

RECITALS

A. OCHIN and Member have entered into that certain Master System Agreement, including the exhibits attached thereto (collectively, "Agreement"). Unless otherwise defined, capitalized terms in this Amendment have the meanings given in the Agreement or exhibits to the Agreement.

B. OCHIN and Member desire to amend the terms of the Agreement to include the additional terms described below.

Agreement

In consideration of the following agreements and covenants, the parties agree as follows:

1. **Business Continuity.** Pursuant to Epic requirements governing Member's access to and use of EMR and the System, Member hereby adopts and implements the Business Continuity Plan ("BCP") indicated by Member on the attached Exhibit AA "Business Continuity Access Requirements," such exhibit to be added to the Agreement as Exhibit AA. In addition, Member hereby adopts and implements all other Business Continuity Access Requirements identified on Exhibit AA. Member's BCP will be subject to the access fees indicated on Exhibit P and payable upon the terms and conditions described in Section 13.1 of Exhibit B. Access fees are subject to change by the OCHIN Board of Directors as provided in Exhibit B.

2. **Lab Demographic Errors.** Member hereby acknowledges and agrees that, to the extent Member uses the services of a third party lab ("Lab"), Member shall be solely responsible for all Lab-generated information and demographics. Member will be solely responsible for ensuring that Lab-generated demographic information matches the Epic demographic information for each applicable patient prior to transmission of any Lab information or data. OCHIN will not be responsible or liable for any Lab information that is improperly filed due to mismatched demographic information. Member will be solely responsible for monitoring transmissions of Lab information, for ensuring that such information is accurately filed, and resolving and correcting any errors in a timely manner.

3. **Effect of Amendment.** This Amendment modifies the Agreement. The Agreement, as amended by this Amendment, is in full force and effect. In the event of any conflict between the provisions of the Agreement and this Amendment, the provisions of this Amendment shall control.

IN WITNESS WHEREOF, the parties have executed this Amendment as of the Effective Date.

OCHIN

OCHIN, Inc.

By: Abby Sears

Title: CEO

Signature:

Dated: 8/28/15

County of Monterey
Health Department

By: Ray Bullick

Title: Director of Health

Signature:

Dated: 3/6/15

Approved as to Legal Form:

By: Stacy L. Saetta

Title: Deputy County Counsel

Signature:

Dated: 7/30/15

Approved as to Fiscal Provisions

By: Gary Giboney

Title: Auditor-Controller

Signature:

Dated: 7/30/15

Amendment No. 9 to Master System Agreement

This Amendment to Master System Agreement ("Amendment") is entered into by and between OCHIN, Inc. ("OCHIN") and County of Monterey, a political subdivision of the State of California("Member") and is effective as of April 1, 2015 ("Effective Date").

RECITALS

A. OCHIN and Member have entered into that certain Master System Agreement, including the exhibits attached thereto (collectively, "Agreement"). Unless otherwise defined, capitalized terms in this Amendment have the meanings given in the Agreement or exhibits to the Agreement.

B. OCHIN and Member desire to amend the terms of the Agreement to include the additional terms described below.

Agreement

In consideration of the following agreements and covenants, the parties agree as follows:

1. **Business Continuity.** Pursuant to Epic requirements governing Member's access to and use of EMR and the System, Member hereby adopts and implements the Business Continuity Plan ("BCP") indicated by Member on the attached Exhibit AA "Business Continuity Access Requirements," such exhibit to be added to the Agreement as Exhibit AA. In addition, Member hereby adopts and implements all other Business Continuity Access Requirements identified on Exhibit AA. Member's BCP will be subject to the access fees indicated on Exhibit P and payable upon the terms and conditions described in Section 13.1 of Exhibit B. Access fees are subject to change by the OCHIN Board of Directors as provided in Exhibit B.

2. **Lab Demographic Errors.** Member hereby acknowledges and agrees that, to the extent Member uses the services of a third party lab ("Lab"), Member shall be solely responsible for all Lab-generated information and demographics. Member will be solely responsible for ensuring that Lab-generated demographic information matches the Epic demographic information for each applicable patient prior to transmission of any Lab information or data. OCHIN will not be responsible or liable for any Lab information that is improperly filed due to mismatched demographic information. Member will be solely responsible for monitoring transmissions of Lab information, for ensuring that such information is accurately filed, and resolving and correcting any errors in a timely manner.

3. **Effect of Amendment.** This Amendment modifies the Agreement. The Agreement, as amended by this Amendment, is in full force and effect. In the event of any conflict between the provisions of the Agreement and this Amendment, the provisions of this Amendment shall control.

IN WITNESS WHEREOF, the parties have executed this Amendment as of the Effective Date.

OCHIN

OCHIN, Inc.

By: Abby Sears

Title: CEO

Signature:

Dated: 8/28/15

County of Monterey
Health Department

By: Ray Bullick

Title: Director of Health

Signature:

Dated: 8/6/15

Approved as to Legal Form:

By: Stacy L. Saetta

Title: Deputy County Counsel

Signature:

Dated: 7/30/15

Approved as to Fiscal Provisions

By: Gary Giboney

Title: Auditor-Controller

Signature:

Dated: 7/30/15

Exhibit AA
Business Continuity Access Requirements

Unless otherwise defined, capitalized terms in this Exhibit have the meanings given on the Cover Pages or the other exhibits.

1. **Purpose.** The purpose of this exhibit ("Exhibit") is to identity Member's obligations for responding to an emergency or other occurrence that damages or destroys Member's access to patient information maintained using the System ("Access Failure"). It is the intent of OCHIN and Member that this Exhibit will meet Epic requirements regarding the access to patient data in the event of an Access Failure and will also meet Epic's Good Maintenance and Accreditation requirements.

2. **Business Continuity Access Requirements**. In the event of an Access Failure, and for so long as the Access Failure continues, Member is responsible for maintaining and will maintain access to a physical copy of the Member's scheduled appointments and all relevant patient clinical data for each patient on the schedule. The requirements of this Section 2 will not apply if Member ceases clinical operations during the Access Failure.

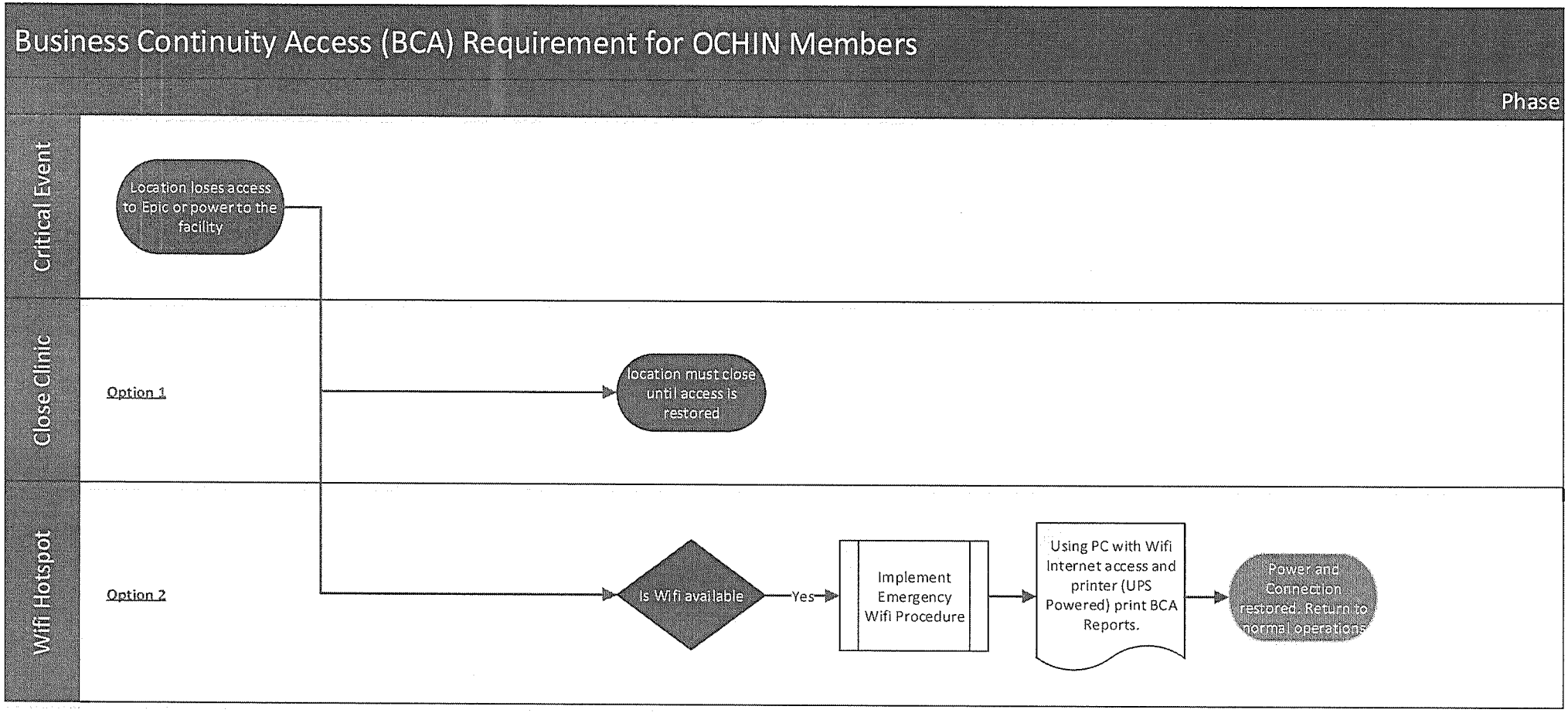
3. **Business Continuity Plan**. In addition to the requirements of Section 2, Member hereby adopts and implements the Business Continuity Plan as indicated by Member below (please circle one of the two options below):

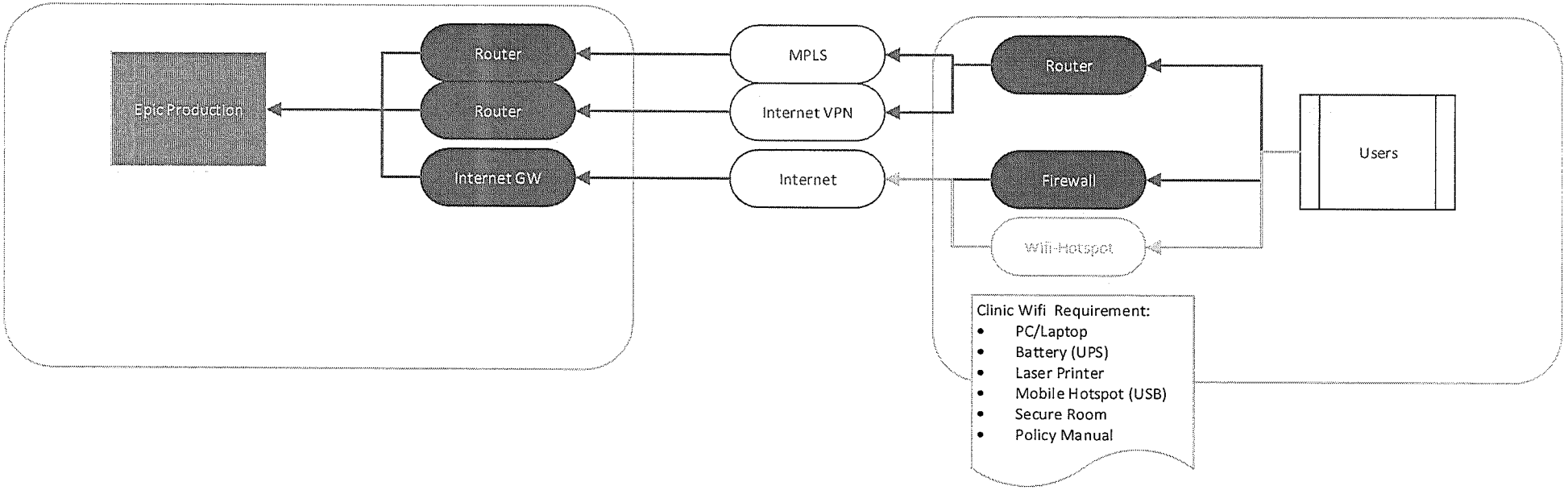
   Option One: In the event of an Access Failure, Member shall cease all clinical operations until access to Epic is restored.

   -Or-

   (Option Two:) Member shall obtain and maintain a workstation and printer connected to an uninterruptable power supply (UPS) or a cellular service and Internet mobile access device, in accordance with and as more thoroughly described in the attached workflow and Wi-Fi hotspot diagram ("Attachment 1"). In the event of an Access Failure, Member will use the workstation and printer or cellular service and Internet mobile access device to meet the requirements of Section 2.

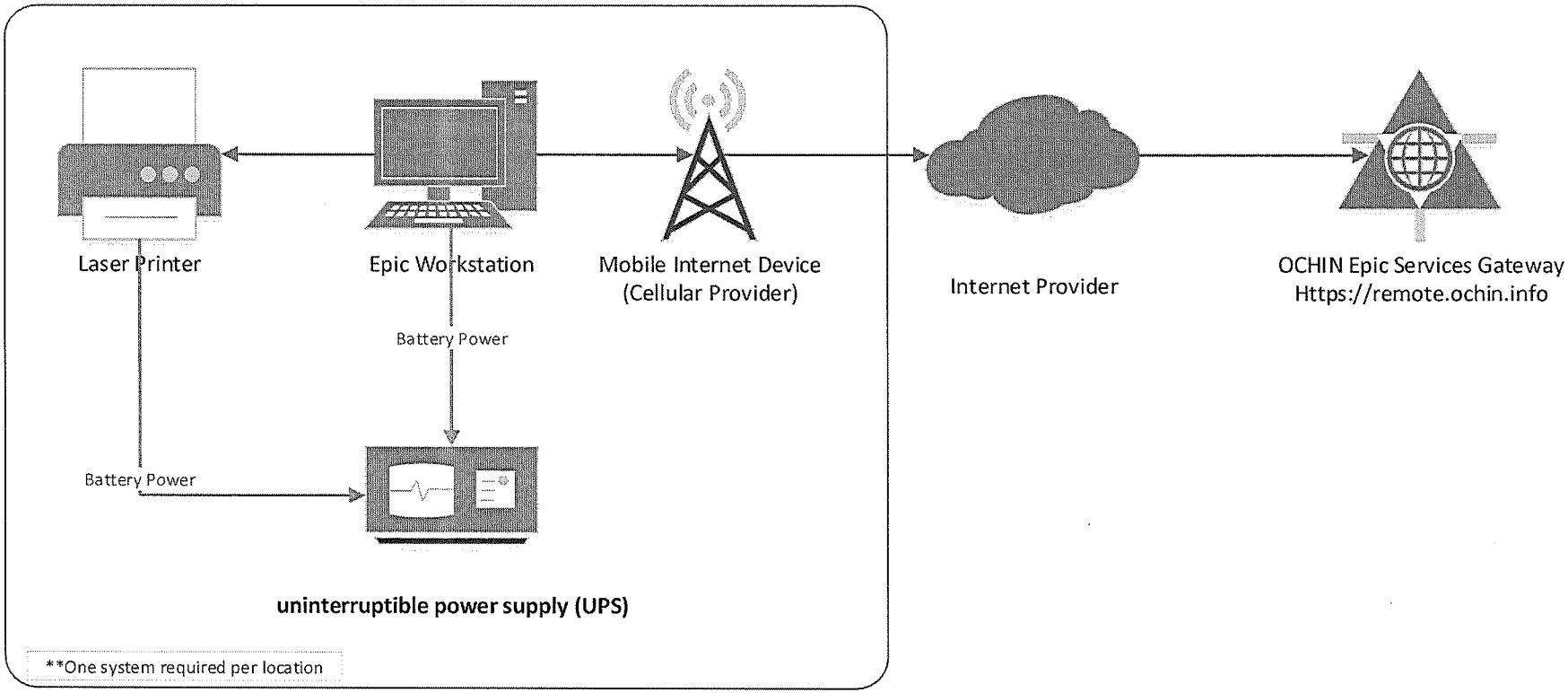
Attachment 1 to Exhibit AA
Workflow and Wi-Fi Hot Spot Diagram




Epic Production
Router
Router
Internet GW
MPLS
Internet VPN
Internet
Router
Firewall
Wifi-Hotspot
Users
Clinic Wifi Requirement:
• PC/Laptop
• Battery (UPS)
• Laser Printer
• Mobile Hotspot (USB)
• Secure Room
• Policy Manual

TITLE

OCHIN Wifi-Hotspot (BCA Requirement)



MEMORANDUM OF AGREEMENT (MOA)
ACCESS CONTROLS FOR PHI and WORKFORCE IDENTITY/ABILITY IN THE USA

I. INTRODUCTION

It is the policy of OCHIN to a) protect the confidentiality, integrity and availability of patient information belonging to our Member's patients, b) protect confidential business information and OCHIN property, and c) ensure that OCHIN's member organizations have confirmed that their workforce members have had their identity and ability to work in the USA verified prior to granting them access to systems owned, operated and/or hosted by OCHIN. To this end, OCHIN has specific policies in place, including an updated policy regarding access controls for Protected Health Information (PHI) and a new policy regarding verification of identity and ability to work in the USA of our Epic members' workforce.

II. PURPOSE OF AGREEMENT

The purpose of this agreement is to formalize a commitment from our Members to adhere to OCHIN's policies #OCHIN-003 and #OCHIN-038 (attached as Exhibit A) in order to guard the PHI of our Members' clients and to be in compliance with applicable laws around PHI and employment practices prior to having access to the OCHIN Epic system.

III. STATEMENT

By signing this MOA, the Member agrees that they have thoroughly reviewed and will adhere to OCHIN's policies #OCHIN-003 and #OCHIN-038 in their entirety.

IV. DURATION

This agreement shall be in effect as of the last date listed in the signatures below and remain in effect until altered by both parties and superseded by a new agreement.

The parties, intending to be legally bound, have executed this agreement by their signatures below:

BY: **County of Monterey**

Ray Bullick, Director of Health
Print Name, Title

Signature

Monterey County Health Department
Organization

Date

Approved as to Fiscal Provisions

Gary Giboney, Auditor-Controller
Print Name, Title

Signature 8-24-15

Auditor-Controller
Organization

Date

Approved as to Legal Provisions

Stacy L. Saetta, Deputy County Counsel
Print Name, Title

Signature

County Counsel / Deputy
Organization

8/24/15
Date

County:
Michael R DERR
8/26/15
CONTRACTS/PURCHASING OFFICER
COUNTY OF MONTEREY

BY: **OCHIN**

Abby Sears, CEO
Print Name, Title

Signature

OCHIN
Organization

9-1-15
Date

Exhibit A

Subject: OCHIN Member User Credential Verification	Policy Number: OCHIN-038
Effective Date: 3.1.15	Original Implementation Date: 3.1.15
Revision Date: NEW	Approved by: Abby Sears, CEO

Purpose

The purpose of this policy is to verify that users issued credentials to access systems owned, operated and/or hosted by OCHIN have the ability to work in the United States of America in compliance with applicable law and their identity has been verified.

Scope

The scope of this policy is systems owned, operated and/or hosted by OCHIN.

Policy

It is the policy of OCHIN to ensure that OCHIN customers have confirmed that their workforce members have had their identify verified, and their ability to work in the USA verified before they are given access to the systems.

Methods to Verify Identity

OCHIN customers may use either of the following methods to verify their workforce member's identity and ability to work in the USA. OCHIN will require customers to confirm that this verification has taken place as a prerequisite to the OCHIN assignment of credentials..

Form I-9

The federal Form I-9, Employment Eligibility Verification, is used by employers as a record of their basis for determining eligibility of an employee to work in the United States. The form is kept by the employer and made available for inspection by officials of the Department of Homeland Security, the Department of Labor, and the Office of Special Counsel for Immigration Related Unfair Employment Practices.

Employers must sign and date the certification. Employees must present original documents to verify their identity. Employers may, but are not required to, photocopy the document(s) presented. These photocopies may only be used for the verification process and must be retained with the I-9. However, employers are still responsible for completing the I-9.

E-Verify

E-Verify is an Internet-based system that compares information from an employee's Form I-9, Employment Eligibility Verification, to data from U.S. Department of Homeland Security and Social Security Administration records to confirm employment eligibility and allows businesses to determine the eligibility of their employees to work in the United States.

Reference

1. Department of Homeland Security

LES 3.1.15

Subject: Access Controls for Protected Health Information	**Policy Number:** OCHIN-003	**Effective Date:** 4.21.10
Original Implementation Date: 4.21.10	**Approved by:** Abby Sears, CEO	**Revision Date:** 6.7.13 3.27.15

Purpose

The purpose of this policy is to define how access to OCHIN confidential or internal use information, Protected Health Information (PHI), OCHIN information systems, facilities, devices and networks will be limited to those individuals who need access in order to perform their job duties. Any such access shall be subject to reasonable security safeguards.

Scope

This policy applies to all OCHIN workforce members (Employees, interns, students, consultants, contractors, subcontractors), and others including OCHIN Member users, who may have access to OCHIN confidential or internal use information and PHI, including information that is used for compliance activities, product development, Help Desk, data aggregation, claims processing, OCHIN Member support, the delivery of patient care, and quality improvement.

Policy

It is the policy of OCHIN to protect the confidentiality, integrity and availability of patient information belonging to our Member's patients. It is also OCHIN's policy to protect confidential business information and OCHIN property. OCHIN workforce members, OCHIN Member users and any other individuals that have an appropriate need to access OCHIN information, information systems, facilities, devices or networks in connection with their job duties and functions will be granted appropriate access.

It is the policy of OCHIN to utilize Active Directory and/or Application specific Security Groups to manage access to systems containing PHI, utilizing the principle of least privilege in assigning rights and permissions to systems. Administrators will add access as authorized by the manager/supervisor on the employee Network Connect (Jira) Access request defined through the HR policy.

Upon notice to OCHIN that any user has inappropriately or illegally accessed PHI, or upon OCHIN's discovery that any user has inappropriately or illegally accessed PHI, OCHIN will terminate the user's access to OCHIN information systems, immediately.

Review of employee access and assignment of Role will be conducted semi-annually.

Human Resources Notification to Systems Team

Workforce member's manager may initiate the systems and network access process. The Human Resources Team (HR) will send a Jira request for information systems and telephone access request to the Systems Team for completion. Access and equipment will be granted based on the role the individual will be performing at OCHIN, and their need to know the information, and that access is based on the manager's request. For example, a person working at the Help Desk would have different access to information systems than an administrative assistant.

Access Controls

Access to information, information systems, processes, facilities, devices or networks is subject to OCHIN policies relating to confidentiality, integrity, and availability of OCHIN information. Any such access to OCHIN information will be consistent with State and Federal laws, rules, regulations, accreditation standards and other OCHIN policies. Workforce members and any other individuals that are permitted this access shall take reasonable precautions to prevent the disclosure of such information, unauthorized use of systems, processes, facilities, devices, and networks.

All users will be responsible to access only those systems and devices that have been authorized for their use. Any use of OCHIN information and or systems, facilities, networks or devices not specifically authorized by OCHIN is prohibited.

Member organizations grant security for access to their organization's electronic patient information contained on OCHIN information systems. User's security is based on the user's role within the organization.

Termination of Employment

Upon termination of employment, internship or contract, the manager of the workforce member will notify Human Resources and Systems Team of the termination. This notification should be in writing. The Systems Team will remove telephone and information system access for the individual and they will deactivate their proximity card (key card). OCHIN laptops, proximity cards, keys, company owned cell/smart phones, iPads, telephones, etc. must be returned to the individual's manager on the last day of employment.

When a user leaves a Member organization, the Member's Site Specialist is required to remove the user's access to PHI in a timely manner.

Data Center Access

Access to the OCHIN data center and servers will be granted by the Chief Technology Officer (CTO). Access to the data center is allowed by the use of a proximity card, and entrance being granted by a security guard who requires visitor sign-in.

Reporting Improper use of Information, Information Systems

Workforce members and any other individual with access to OCHIN information or information systems, facilities, devices, and networks are required to immediately notify the Integrity Officer and the HR Director in the event that they become aware that OCHIN information, information systems, facilities or devices or networks are being used improperly, in an unauthorized manner, or if that use has resulted in an unauthorized or improper disclose of confidential information.

Member organizations are required by the OCHIN Member contract to report improper or illegal use of information systems containing PHI that results in a breach of PHI, within 24 hours of discovery.

Please see the Notification of Breach of Unsecured Protected Health Information policy for additional information pertaining to unauthorized or improper disclosures of PHI.

Reference

45 CFR 164

LES 4.21.10
Rev 6.7.13
Rev 3.27.15