



Regional One Health

Annie Lewis
Physician Liaison
Regional One Health
877 Jefferson Ave
Memphis, TN 38103
(901) 545-7825

alewis@regionalonehealth.org

▪ Resident Orientation Welcome Packet

- ✓ Welcome Letter and Campus Map (Annie Lewis)
- ✓ Forms
 1. Request for ID Badge
 2. Outpatient Provider
 - Surescripts Prescriber
 - Provider Demographics Sheet
- ✓ Access to Systems
 1. Documentation (EHR)
 2. Dictation Number
- ✓ ROH **MANDATORY** Training
 1. Application Directory
 2. Web Based Modules
 3. Abuse Module
 4. Restraint Module
 5. Transfusion Module
- ✓ Wireless Access Connection
 1. Computer
 2. Cellular Device
- ✓ IT Security/Compliance Guidelines

▪ Contact Us



RESIDENT ORIENTATION

March 15, 2016

Residents & Fellows,

It is with great joy that I welcome you on behalf of Dr. Reginald Coopwood, CEO, Dr. Eric Benink, CMO, myself, and our 2000 plus employees to Regional One Health. Regional One Health is the premier healthcare facility of the mid-south whose priority is providing excellent quality and patient safety centered care to every patient every time. At Regional One Health, we are the domain for the stellar Elvis Presley Level 1 Trauma Center, Sheldon B. Korones Newborn Center, and the Memphis Firefighter's Burn Center.

Your educational journey with Regional One Health will begin with an orientation:

June 27, 2016
1:00pm- 5:30pm
Registration: 12:30pm
Student Alumni Center (SAC) Auditorium
800 Madison Ave.

Free parking will be provided in the parking SAC garage at the corner of Madison and Manassas, beside the Student Alumni Center.

Please complete the attached modules and forms below. If you need anything before and during your residency or fellowship, please contact Annie Lewis, 901-545-7825 or alewisdst@yahoo.com.

We look forward to seeing you on June 27, 2016.

Much Thanks!!!

Annie

Annie Lewis
Physician Liaison



Regional One Health

Residents/Fellows:

We would like to welcome you to the Regional One Health where patient safety and quality is at the forefront of our mission. We will be the catalyst providing you with a wide range of teaching opportunities to assist you in becoming an outstanding healthcare provider.

SYSTEM ACCESS

MUST have NPI# to get started:

In order to access Regional One Health's health care systems, you will need to complete the following modules. Please click the attached link and follow the instructions.

Module Checklist:

- Application Directory
- Web Based Modules
- Abuse Module
- Restraint Module
- Transfusion Module

Email NextGen forms to: ITAmbulatoryServ@regionalonehealth.org

IT Contact Information: ITeducation@regionalonehealth.org

ROH ID Badge

Please complete the attached **Badge Request Form** and **email it to Carolyn Witt, Security, crwitt@regionalonehealth.org**. You are encouraged to have your ID badge made before ROH orientation. ID badges are made in the Regional One Health Security Office, which is located on the 1st floor of the hospital through the double doors behind the cafeteria, Monday – Friday, 9-11am, 1-3pm, & 6pm-8pm. Replacement badges are available for a \$10 fee. **Security will begin making your ID badges after June 1st**. Please stop by and have yours made.

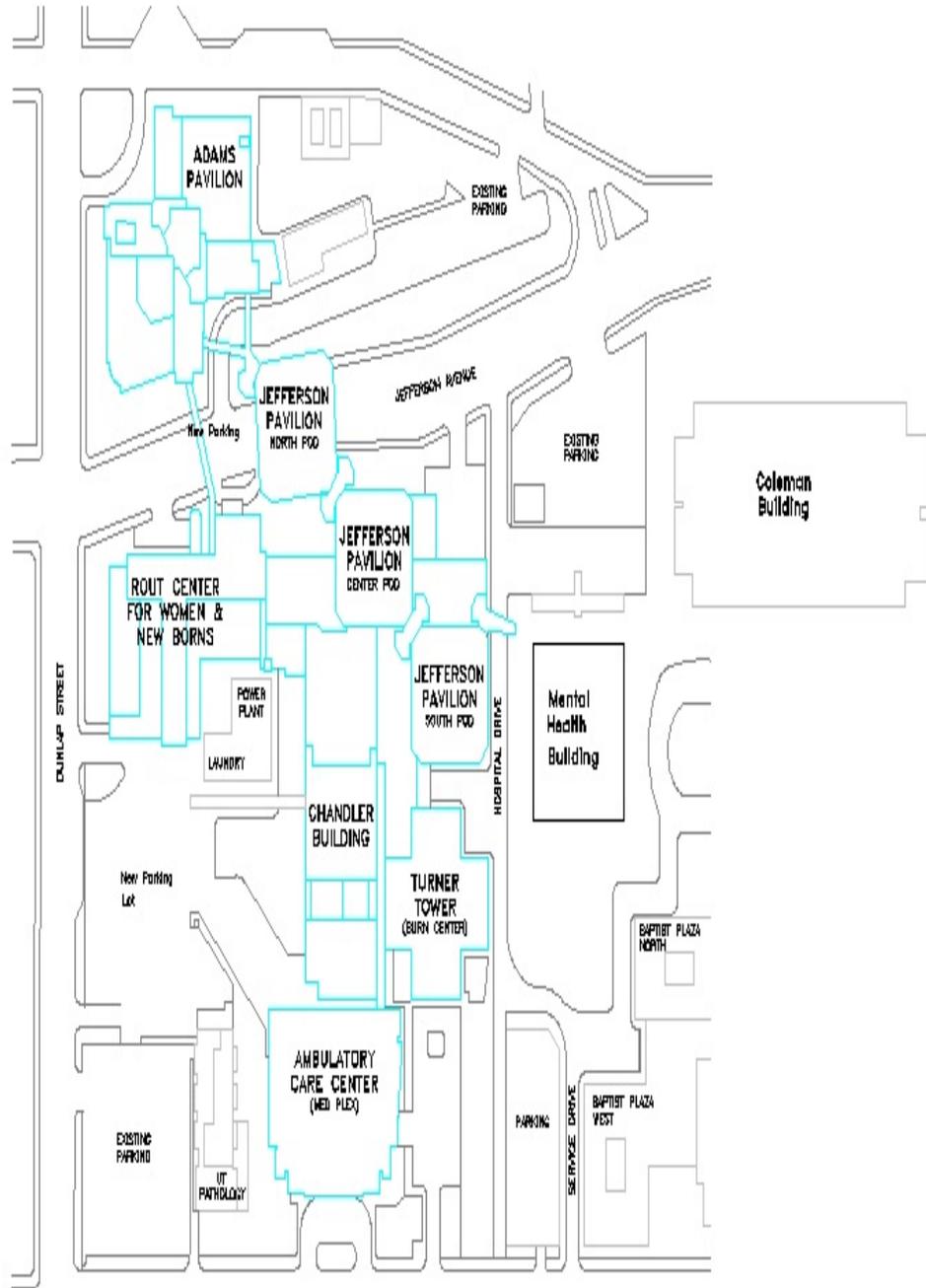
Complete these items ONLY on the Badge ID Form: Check: New Badge, Circle: Resident & UT, Enter: Name, Your Signature

ROH Campus Map

I've attached a map of Regional One Health as a resource to assist you in maneuvering about our campus.



Regional One Health





Regional One Health

REQUEST FOR ID BADGE

Circle one: New Badge or Replacement Badge

►Note: a fee of \$10 will be charged for lost, stolen or damaged badges. If badge is damaged or worn, that badge or portions of the badge must accompany this request.

Date of request: _____

Circle type of badge requested:

Contractor Employee Physician Security Student Resident
UT Vendor Visitor

If request is for subsequent badge, please check reason:

Lost Stolen Damaged Worn Change of Info

Name: (Please Print)

--	--	--

Last

First

M.I.

--	--	--

Job Title

School or Company Name

Department Name

--

Phone Number

Supervisor/ Manager Signature

Applicant Signature

Security Signature

To be completed by Security

Was applicant charged fee for lost, stolen, or damaged badge due to misuse? **Yes** **No**

Fee Collected: **\$10.00 (Adams Cashier or Med Payroll Deduction Form)**

Comments: _____

Proximity Badge #: _____ Date Issued: _____



ROH ID Badge

Please complete the attached Badge Request Form and email it to Carolyn Witt, Security, crwitt@regionalonehealth.org.

You are encouraged to have your ID badge made before ROH orientation.

ID badges are made in the Regional One Health Security Office, which is located on the 1st floor of the hospital through the double doors behind the cafeteria, Monday – Friday, 9-11am, 1-3pm.

Replacement badges are available for a \$10 fee.



Surescript Forms

Please fill out the following 2 forms to include:

1. Prescriber First and Last Name
2. Address of hospital (880 Madison Ave, Memphis, Tn 38103)
3. Phone number
4. NPI number.

The rest of the information will be provided at a later date.

Email the forms to ITAmbulatoryserv@regionalonehealth.org NOT the listed information on the form.



The Nation's E-Prescription Network

Section I: Prescriber Information

*Prescriber First & Last Name:

Practice/Clinic Name:

*Practice Address:

*Phone Number:

() —

*Fax Number:

() —

*NPI Number:

*DEA Number:

*Surescripts Case Number:

Section II: New Vendor Information:

*Vendor Name: (Surescripts is NOT a vendor)

Select e-Prescribing Services:

NEWRX Med History
 REFILL Eligibility

*Effective Date: / /

*Authorized By: (Sign & Print)

By signing the above I hereby certify that I am authorized by the prescribing physician to make changes on their behalf.

Please allow up to 48 hours for your request to be completed.

**Prescriber Vendor Release Form
Fax Completed Form to 703-738-2388**

- Switching Vendors**
 Ex: The prescriber already e-Prescribes but will be using a new software solution.
- Adding a New Refill Capable Location w/ a New Vendor**
 Ex: The prescriber wants to setup a new e-Prescribing capable location with the refill service level at a new physical address and with a new vendor.

If you have any questions concerning this form please contact Surescripts Support.

1-866-RxReady (866-797-3239)
Option 1, Option 1

General Instructions

- Prescriber or prescriber's representative (i.e., office manager) must complete this form in its entirety.
- All fields marked with an asterisk (*) are required. Incomplete forms will not be processed by Surescripts.

Section I: Prescriber Information

- All fields are required (except Practice/ Clinic Name).
- If both DEA and NPI are available, then please supply both. Otherwise only the DEA or NPI is required.
- PO Box number cannot be included in the address.
- Please ensure that the fax number provided is one to which refill requests can be faxed in the event of a network issue.
- Case Number: Your *new* ePrescribing software vendor will create a Surescripts case to track this change request. Contact your *new* ePrescribing software vendor to obtain a Surescripts case number. Forms without Surescripts case numbers will not be processed.

SECTION II: NEW VENDOR INFORMATION

- Please insert the name of your *new* ePrescribing software vendor on the line provided. (Surescripts is NOT a software vendor)
- Effective Date: List the date on which you would like the request to take effect. Forms without effective dates will not be processed.



Regional One Health

Provider Demographics Sheet

*Last Name	
*First Name	
*Credentials	
*Specialty	
*Provider Role	<input type="checkbox"/> Attending <input type="checkbox"/> Resident <input type="checkbox"/> Fellow <input type="checkbox"/> PharmD
Attending Provider <small>(if Resident, Fellow or PharmD)</small>	
Rotation Days	
Start Date	
*End Date	
*NPI	
*DEA	
*Email Address	

*indicates required item

*Sign your name in box below.
Make sure it does not go outside or touch the lines.*

--

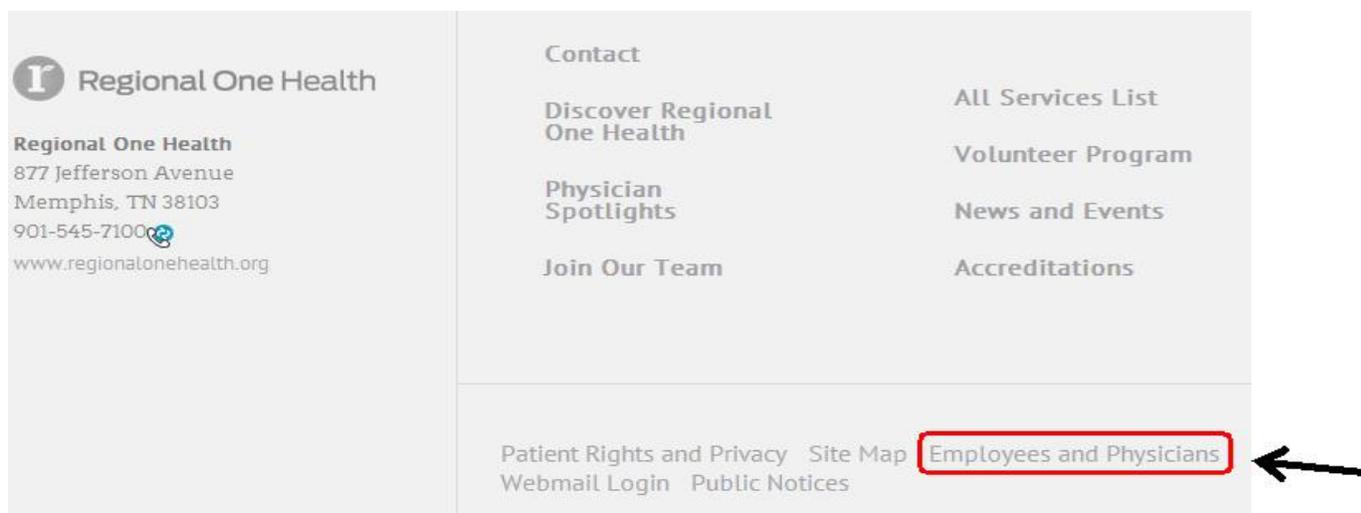
Please email forms to ITAmbulatoryServ@regionalonehealth.org

Obtaining Access to Computer Systems

All New Providers:

Please follow the steps below to obtain access for the computer systems at Regional One Health:

1. Go to Regional One Health's Internet site (<http://www.regionalonehealth.org/>). Scroll to the bottom of the page and click on Employee and Physicians.



2. Select Access Request.

Employees and Physicians

The links below are to resources used by employees and physicians at Regional One Health.

Hospital Links

- [Access Request](#)

– *Signup for access to Soarian Clinicals and other systems*

- [Remote Access \(VPN, Citrix, Wireless, etc.\)](#)

3. Select “I am a new user, employee, or physician”.

Please select an option below:



I have an account. (Webmail, Citrix, etc.)



I'd like to reset my password.



I forgot my username.



I am a new user, employee, or physician.

4. Select “No” or “Yes” if you have a Regional One Health email account.

If you currently have access to any one of the following systems, then you already have an account and you should select “Yes” on item 4 above:

- Webmail, a “regionalonehealth.org or the-med.org” email address
- Windows Computer Login Account (UMC)
- VPN Remote Access
- Citrix Remote Access
- Intranet Log in (ex: Progress Reports)

5. Select your Employer (i.e. UTHSC, Campbell Clinic, etc.) and select “Next”.

6. Select your Job Type and select “Next”.

7. Enter your NPI and Dictation PIN and select “Next”.

If you are unable to verify your NPI/Dictation PIN, please contact HIM by calling Keesha Franklin at 901-545-7662 or Buffy Bell at 901-545-5524.

8. Complete the remaining screens and hit submit.

Once you have submitted your Access Request, it will go into an approval queue. Once approved, it will be sent to IT for implementation. You will receive email confirmations as you are approved and systems are implemented. It may take 24-48 hours to implement all systems.

You can request additional access by logging in and selecting “Request Additional Access.”

Area	Inpatient	Outpatient	ED/Trauma/CCA	L & D	OR
Application	Soarian Clinicals/CPOE	NextGen	MedHost	QS- Centricity Perinatal	SIS- Surgical Information Systems
System Description	SOARIAN Clinicals allows users to perform a range of tasks to manage daily workflow. When a user signs on to the system, a portal screen displays with their patient census and work lists. From the portal screen, the clinician can easily view patient records to find information such as new or existing results and demographic information. The clinician can also place orders or modify existing orders.	EHR software for outpatient areas of Regional One Health that include Provider Documentation, CPOE, and e-prescribe features.	ER Charting System for the Emergency Department areas that include documentation, CPOE order entry and e-prescribe.	QS is a fetal surveillance and documentation system used in L&D, newborn, neonatal ICU, postpartum, and antepartum care areas.	This system provides scheduling, nursing and anesthesia documentation and improved work flows.
Methods of Instruction	WBT's Departmental	WBT's Departmental	Classroom training Departmental	Classroom training Departmental	Departmental





Regional One Health

BLOOD TRANSFUSION MODULE

Link: <http://portal.transfusesolutions.com>

To sign the attestation for completing: <http://www2.regionalonehealth.org/surveys/policyupdates2016/>

Reason for training: Over 30% of blood transfusions done in the US are unnecessary or inappropriate, exposing patients to additional risk and consuming valuable hospital resources. Regional One Health has identified transfusion as an opportunity for improving quality of patient care and will be requiring all residents to complete a short training module. The goal of the training module is to drive appropriate transfuse practice in all service areas of the hospital.

Instructions: Visit <http://portal.transfusesolutions.com> and register with your Name, UT email, role (resident physician), and NPI number. The physician credentialing module will be available in the left-hand menu but we encourage you to explore other areas of the portal such as the Lectures and Journal Watch sections that contain valuable information on appropriate transfusion practice.

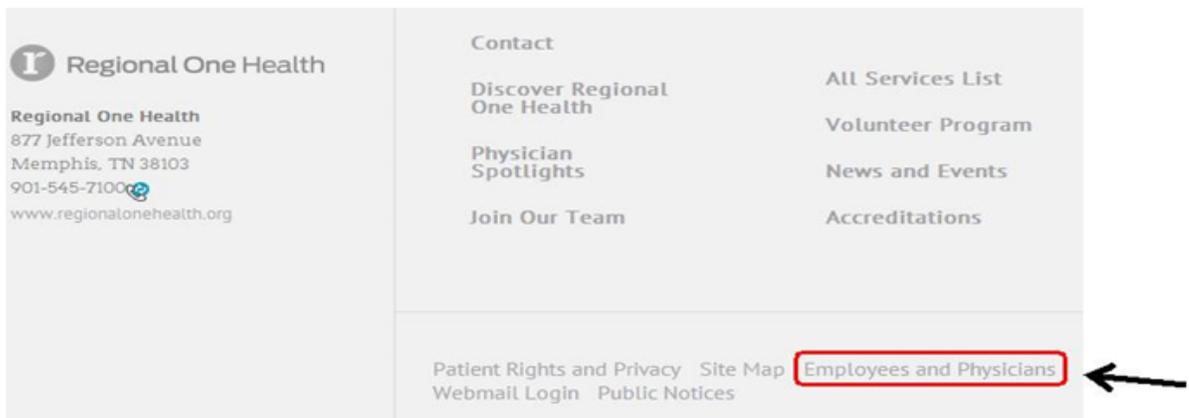
Please contact Annie Lewis at 901-545-7825 if you experience difficulty gaining access to the module.



**** The passcode to access training is GoROH ****

Training for Physicians:

1. Go to Regional One Health's Internet site (<http://www.regionalonehealth.org/>). Scroll to the bottom of the page and click on Employee and Physicians



2. From the Employee and Physicians link on the Regional One internet site (shown above), click on "Training Materials".

Physician Links

- [Physician Portal](#)
- [New Resident Orientation](#)
- [Training Materials](#)





3. When presented with the Training Quick Pass screen, enter [GoROH](#) .



4. Select the appropriate training material heading, and complete the Web Based Modules located within. As an attestation of completion after each WBT, you will be prompted to provide your name and NPI number.



- [Siemens Soarian Clinicals & EDM](#)
- [NextGen Training Materials](#)

****If you feel as if you require additional Soarian Clinicals training AFTER**

reviewing the web based training content, you may contact:

Angela Boswell @ aboswell@regionalonehealth.org or Rhonda Roberson @

rroberson@regionalonehealth.org

Policy Updates – Medical Staff

Restraint or Seclusion: Violent/Behavioral

General Information

- Ordering physicians must have working knowledge of the hospital's policy
- **Each episode** of restraint or seclusion **requires an order**
- Must evaluate and document the patient **face-to-face** within **one hour** of initiation
- Non-physical de-escalation techniques will be used prior to physical holding

Restraint or Seclusion: Violent/Behavioral *Order Requirements*

- Each episode of restraint or seclusion requires an order by a licensed physician or qualified allied health professional
 - Must be primarily responsible for the patient's care
 - If not ordered by the attending physician, they must be consulted as soon as possible (telephone consult is allowed)

Emergency Situations ONLY:

- If primary physician is unavailable, qualified staff may initiate restraint based on assessment and an RN must notify the physician IMMEDIATELY to obtain a telephone or verbal order

Restraint or Seclusion: Violent/Behavioral Order Requirements for *Physical Hold*

Order Details -- Webpage Dialog

SFTest, EPOC 71y ♀ Extended Care Hospital-T402
Allergies: (0) NKA Diagnosis: (0) MR# 4000295 ACCT# 7000056

Nursing Orders

Ordered By: Test Physician (16506) Entered By: Test Physician Order Id: 6502969
To Be Filled By: ECH On: 03/10/2016 15:38 Status: Active
OrderSourceModifier: CPOE Order

VIOLENT RESTRAINT Timing Critical !

Type of Restraint

- Side Rails x 4
- Mitt / Mitten - Right
- Mitt / Mitten - Left
- Mitt / Mitten - Bilateral
- Soft Wrist - Right
- Soft Wrist - Left
- Soft Wrist - Bilateral
- Soft Ankle - Right
- Soft Ankle - Left
- Soft Ankle - Bilateral
- Pelvic Restraint (Rehab Only)
- Enclosure Bed (Rehab Only)
- Seclusion

Other Restraint Type:
Physical Hold

Order & Finish Cancel Help



Restraint or Seclusion: Violent/Behavioral *Face-to-Face*

- Physician must evaluate and document the patient **face-to-face** within **one hour** of the original initiation of restraint or seclusion; even if discontinued prior to one hour
 - Components of a face-to-face include
 - Patient's physical/psychological status
 - Patient's immediate situation
 - Patient's response/reaction to intervention
 - Need to continue or terminate restraint or seclusion

**Qualified allied health professionals may perform this evaluation if they consult with the attending physician immediately (within minutes) and document same.*

Restraint or Seclusion: Violent/Behavioral *Physical Hold*

- A **physical hold** is the use of bodily, physical force to limit an individual's freedom of movement and **is a form of restraint**
 - Requires an order, face-to-face evaluation, and second staff person to observe the patient
- Used only as a last resort and only after non-physical de-escalation techniques have failed

Restraint or Seclusion: Violent/Behavioral Definitions

- Restraint: all manual, physical, mechanical, and material devices used to involuntarily limit freedom of movement, immobilize or reduce the ability of a patient to move his/her arms, legs, body, or head freely.
- Seclusion: The involuntary confinement of a patient alone in a room or area from which the patient is physically prevented from leaving and not allowed visitation.
- Violent/Behavioral Restraints: A manual, physical, medical, material, or chemical device used to involuntarily limit freedom of movement of a patient who exhibits intractable behavior that is severely self-injurious or injurious to others, who have not responded to traditional interventions, and who are unable to contract with staff for safety.
- Qualified Staff: A staff member who is trained and competent in the initiation of, application, monitoring, assessment and discontinuation of restraint or seclusion (Ex: allied health professional, registered nurse).

Restraint or Seclusion: Violent/Behavioral *Training Requirements*

- Training will occur:
 - With initial credentialing
 - At re-appointment
 - With any significant content changes to the policy

Critical Tests and Critical Results (Values)

General Information

- Regional One Health defines the length of time between **availability of the results and the receipt** by the responsible licensed independent caregiver as **one (1) hour**
- MSEC approves the list of critical tests and results (values)

Critical Tests and Critical Results (Values) *Notification Process*

- **Laboratory Results**
 - Once result is available, lab personnel notify nurse within 30 minutes
 - Nurse **MUST** notify provider within 30 minutes of receipt with “read back” process
- **Radiology Results**
 - Provider to provider notification within one (1) hour
- **EKG and Echocardiogram Results**
 - EKG: Nurse/EKG tech notify ordering provider within one (1) hour
 - Echo: Cardiologist notifies ordering provider within one (1) hour
- **Outpatient Results**
 - During practice hours: Nurse must notify provider within one (1) hour of receiving a critical result with “read back” process
 - After practice hours: Any critical result is called to the After Hours Call Center

If the ordering provider cannot be contacted, the provider chain of command will be initiated.

Blood Collection Process

Blood Collection Process

Physicians

- **MUST** use two patient identifiers when drawing blood
 - Name or Trauma Number (if patient name unknown)
 - Account Number
- MD holds blood until patient label is placed on specimen

PREVENTION AND REPORTING OF PATIENT ABUSE

Medical Staff and House Staff



Orig: 12/10/13

Regional One Health

Patient Abuse and Neglect Policy Statement

Regional One Health strives to ensure that patients are protected and free from neglect and abuse. Regional One Health must protect vulnerable patients including newborns and children. Additionally, Regional One Health must provide protection for the patient's emotional health and safety as well as physical safety. Any employee, house staff (resident), students, volunteers, contract staff, medical and allied health staff, vendors, contractors, and agents who suspects a violation of this policy or Regional One Health's standard of conduct is responsible for reporting such concern as set forth below. Medical staff, house staff (resident), students, volunteers, contract staff, allied health staff, vendors, contractors, agents, patients, family members or general public are encouraged to report any suspected abuse or neglect.

Please read Regional One Health's policy: Patient Abuse and Neglect located on the intranet

Definition of Abuse and Neglect

Abuse is defined as “the **willful** infliction of injury, unreasonable confinement, intimidation or punishment with resulting physical, emotional or psychological harm, pain or mental anguish.”

(ROH Abuse and Neglect Policy)

Neglect: The failure to provide goods and services necessary to avoid physical harm, mental anguish or neglect.

Prevention of Abuse & Neglect

To protect patients from abuse and neglect, Regional One Health will adhere to the following 7 requirements:

1. Prevention

- Ensure that adequate staffing levels working within clinical areas are maintained at all times.
- Adequate staffing will serve as a critical component of preventing the abuse and neglect of a Regional One Health patient.

2. Pre-Employment Screening

- Pre-employment screening process will include review of state adult and/or child registries to ensure that individuals reported to such registries are not hired as employees of Regional One Health.
- Require the same for vendors and contractors providing services on the premises of Regional One Health's campus and/or off-site outpatient clinics.

3. Identification

Maintain an internal incident reporting system that will allow personnel to report events and occurrences

Prevention of Abuse & Neglect

4. Training

The general orientation curriculum for newly hired personnel and ongoing training for existing personnel will include training on patient abuse and neglect, and will include a minimum:

- Definition of abuse and neglect
- Reporting requirements for abuse and neglect
- Prevention of abuse and neglect
- Intervention/Detection of abuse and neglect

Prevention of Abuse & Neglect

5. Protect

Should an allegation of abuse and/or neglect be made, the patient identified in the allegation will be protected in accordance with the process set forth in Process section Patient Abuse and Neglect policy.

6. Investigation

Should an allegation of abuse and/or neglect be made, the investigation of abuse and/or neglect will be:

- Objective
- Completed in a timely and thoughtful manner

Prevention of Abuse & Neglect

7. Report and Respond

Should an investigation of an allegation of abuse and/or neglect result in a finding of abuse and/or neglect:

- Report such abuse and/or neglect to the appropriate authorities as required by applicable law and
- Implement the appropriate corrective/remedial action

Role of Risk Management or Quality in Patient Alleged Abuse

1. Risk Management and/or Quality will empanel an investigative team. The investigation will be done within 72 hours.
2. The completed investigative summary will be reviewed by the Program Director, Site Director and Attending Physician, appropriate executive team members to determine a consensus for actions to be taken.
3. The Program Director will review the findings of the investigation with the **Resident.**

Reporting Suspected Violations

- Reports of suspected violations or acts of patient abuse/neglect are handled confidentially to the extent the law allows.
- Anonymity is provided to any reporting person desires it.
- Regional One Health has a policy of not tolerating retaliation for any report which is made in good faith. However, a person who makes a report of suspected violation or act of patient abuse/neglect without good faith belief that the actions are wrong may be subject to disciplinary action.

Policy Acknowledgement

In order for you to acknowledge that you have read and understand the policies outlined in this document, please follow the below link.

[Policy Acknowledgement Form](#)

<http://www2.regionalonehealth.org/surveys/policyupdates2016/>



The following link will direct you to an abuse module that must be completed within 30 days.

The Resident will use their NPI number to log in, and this will be the information used to keep track of the training for reporting purposes.

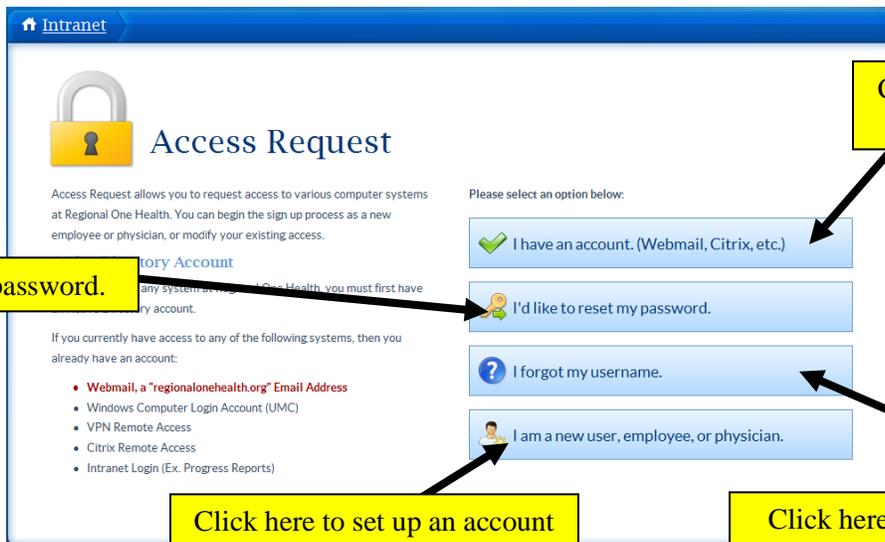
<http://www.the-med.org/media/training/compliance/abuse/>

Wireless Access Connection

ROH Wireless Connection Tip Sheet

2016

Follow these steps to connect employee owned wireless devices to the secured Regional One Health wireless network. You must request wireless access through **Access Request** before you can join the network. You may use the **Access Request** system to retrieve your user name and/or password. During this process, you will be required to enter your user name and password. To navigate to **Access Request**, go to <http://intranet2.the-med.org/> and select **Access Request** on the right side of the webpage, as shown below. You can also access it directly at <https://accessrequest.the-med.org/>.



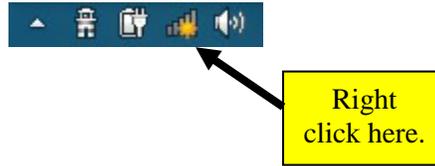
Click here to reset your password.

Click here to request wireless access.

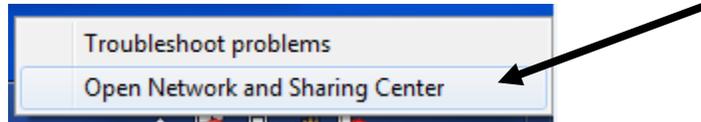
Click here to set up an account if you are a new user.

Click here to retrieve your user name.

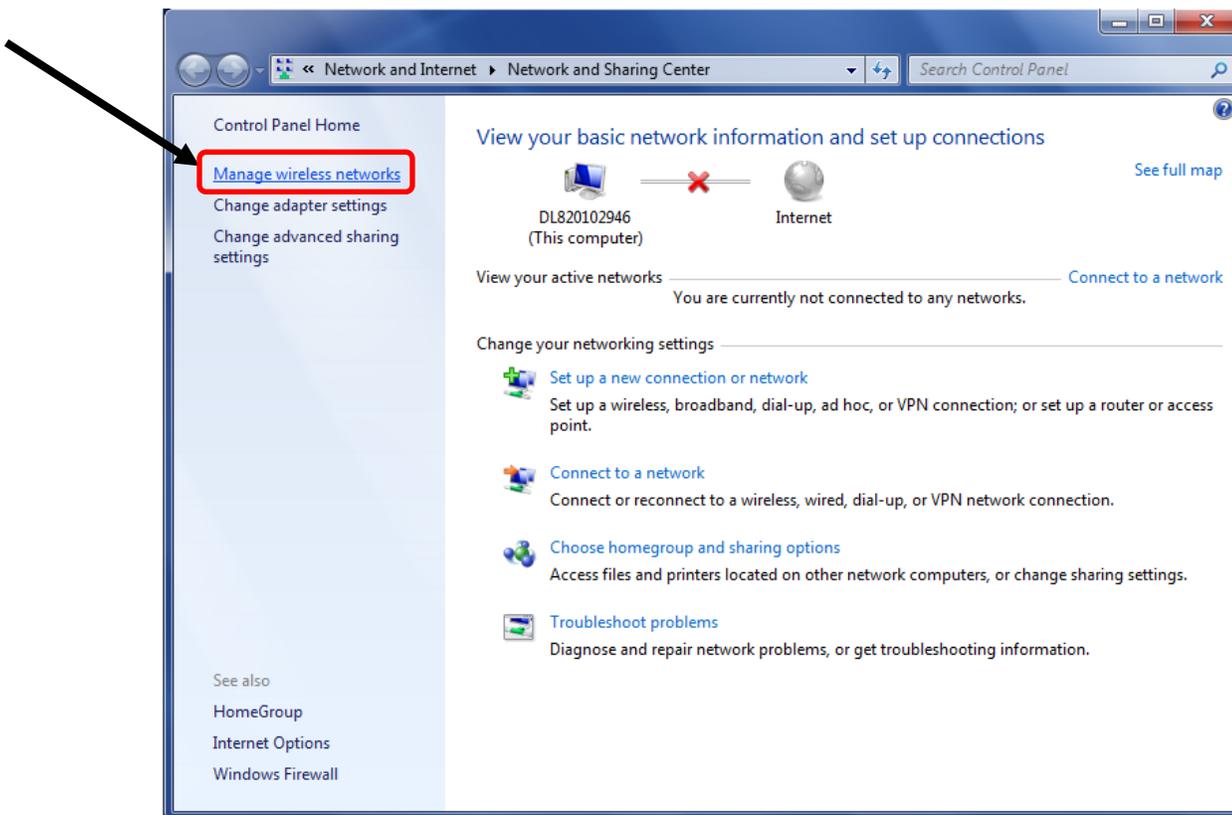
1. Find the wireless network icon on the bottom right side of the screen. Right click the network icon.



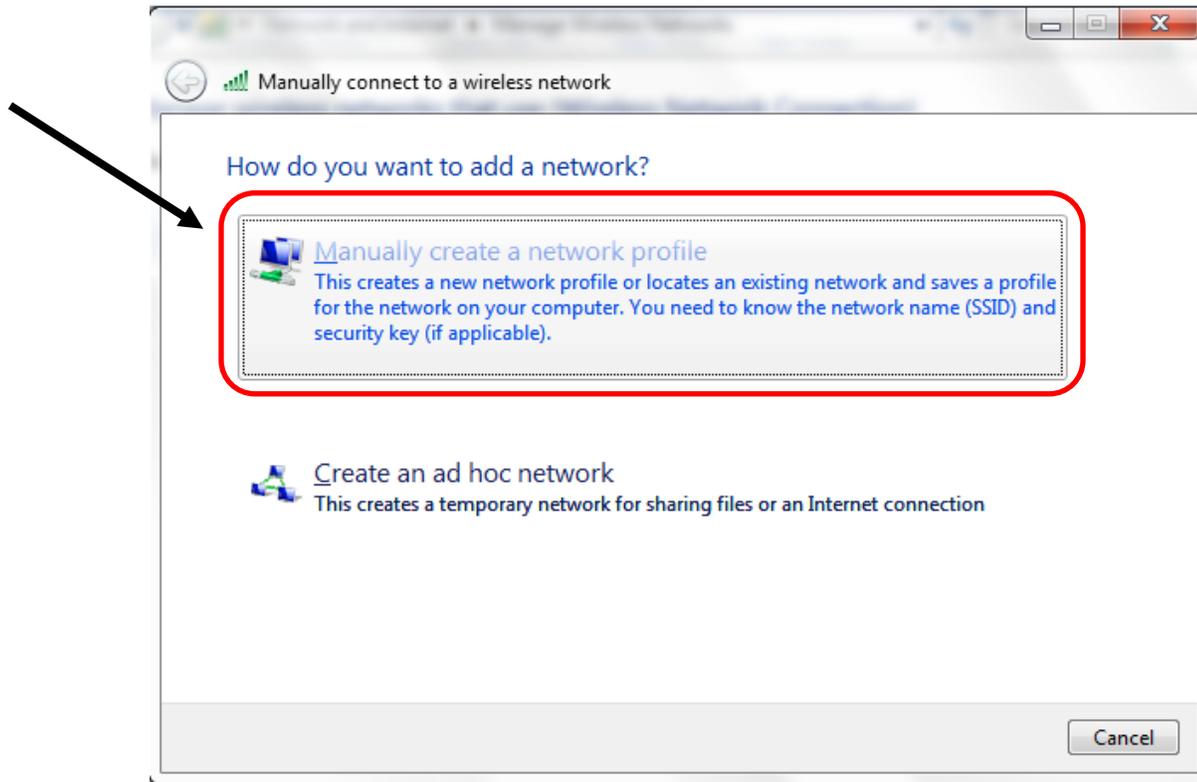
2. Select "Open Network and Sharing Center".



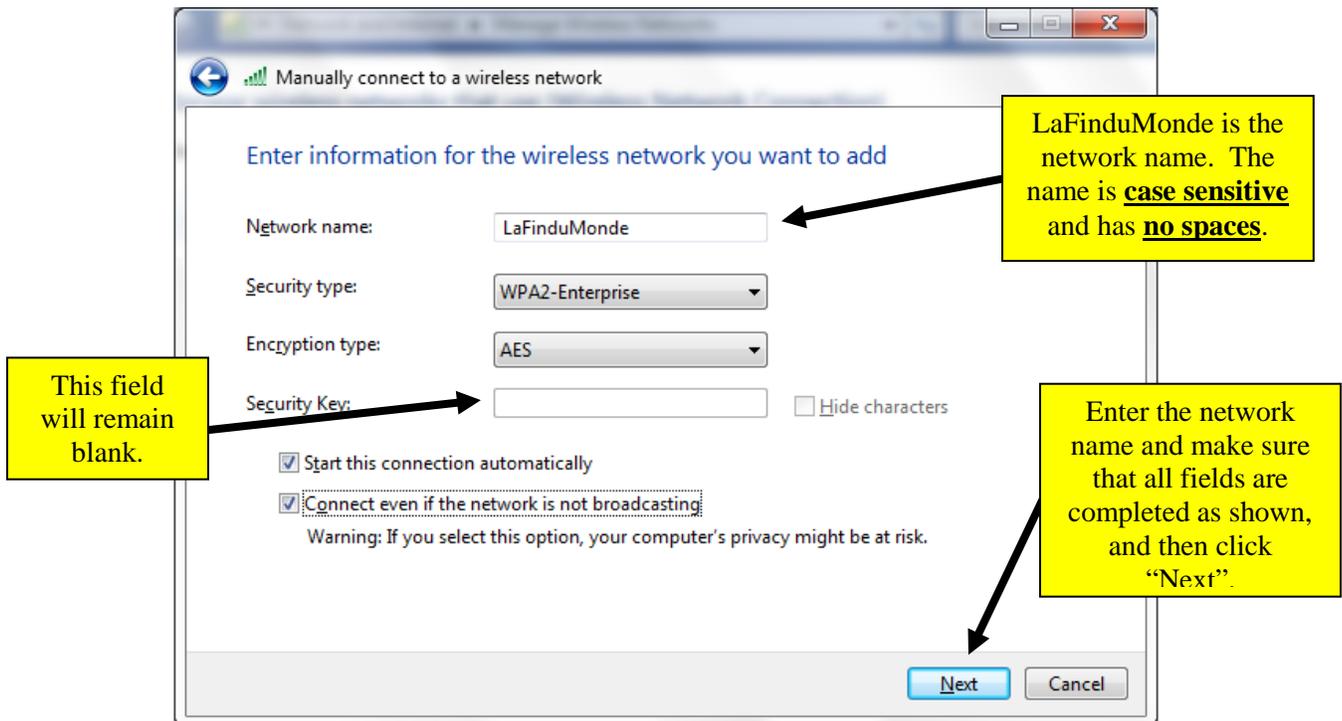
3. Select "Manage Wireless Networks".



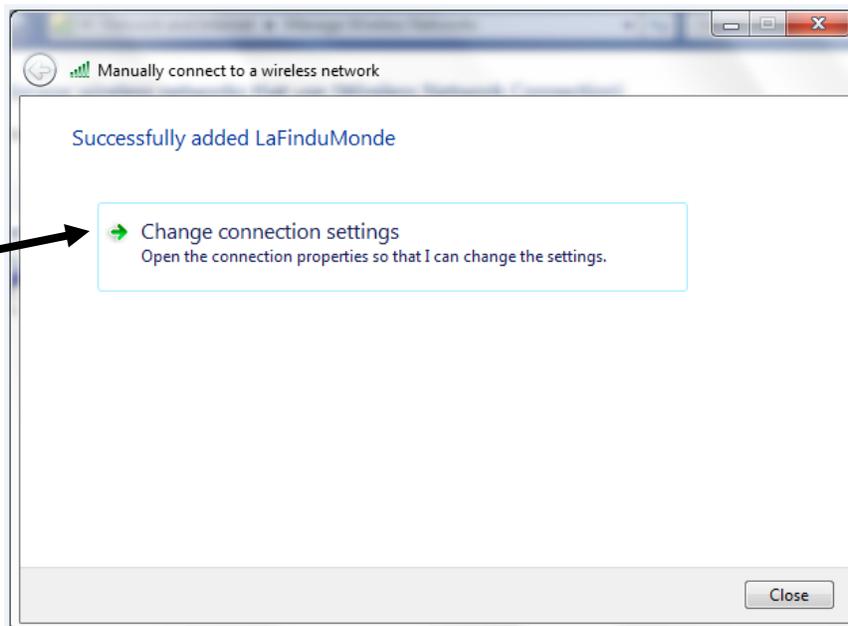
4. Choose "Manually create a network profile".



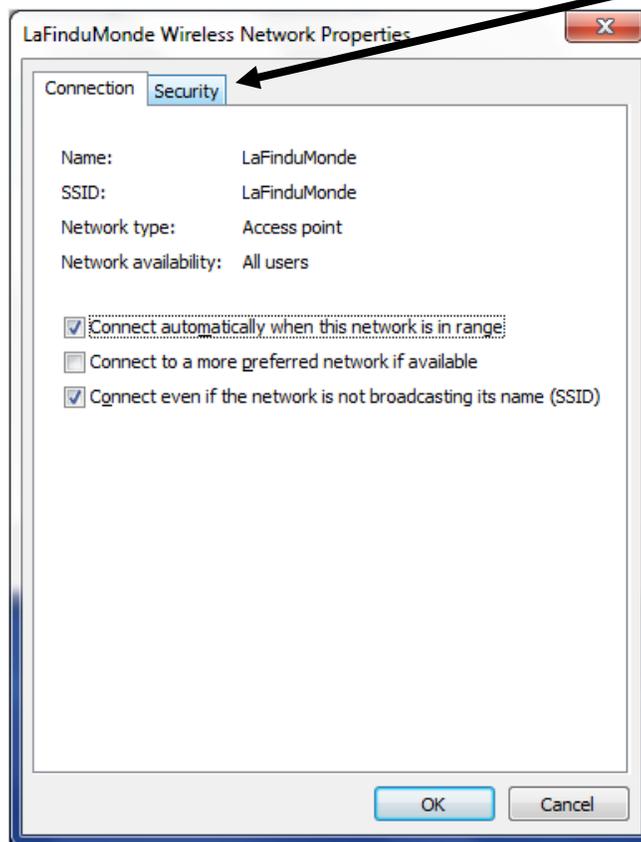
5. Enter the network name. This screen should look exactly as below.



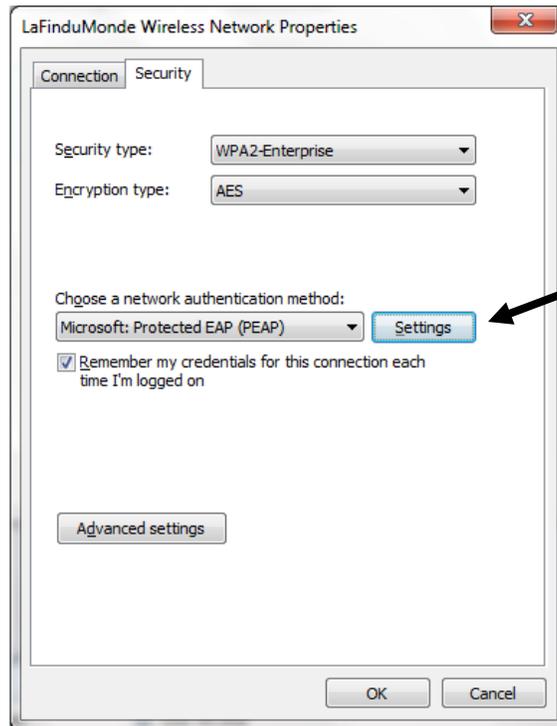
6. Select "Change connection settings".



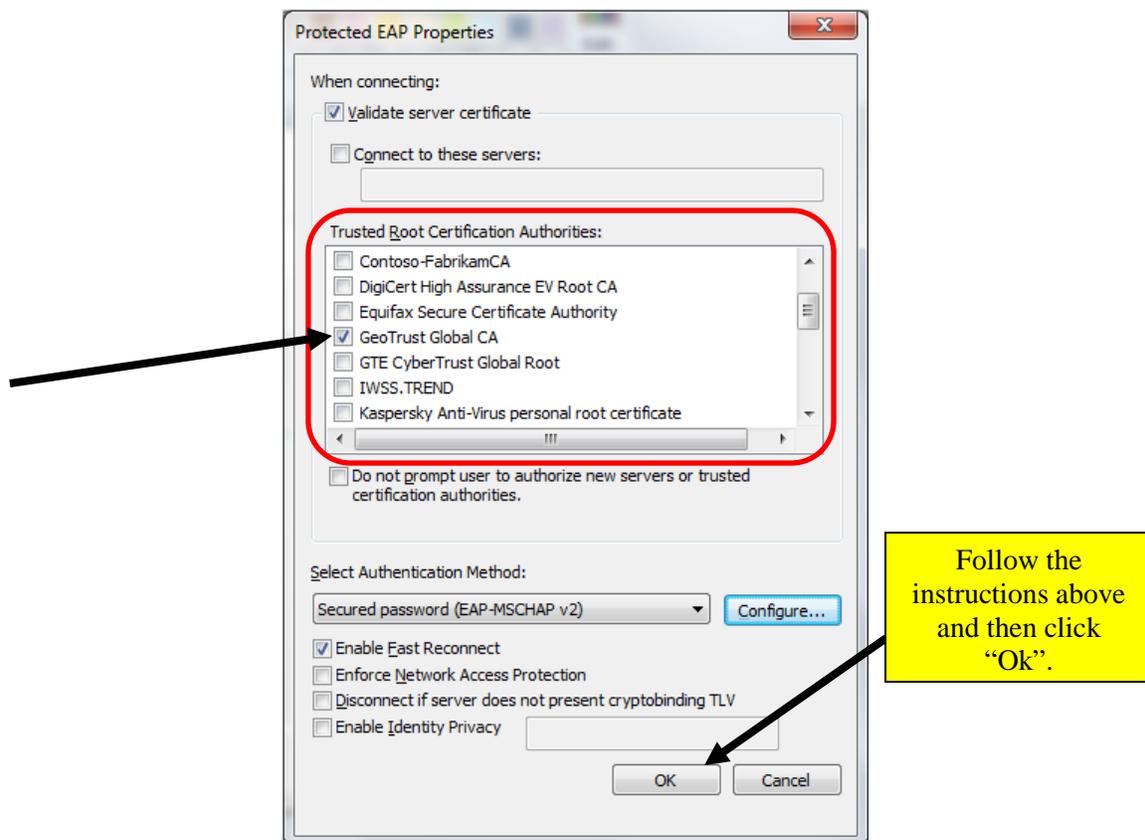
7. Click the "Security" tab.



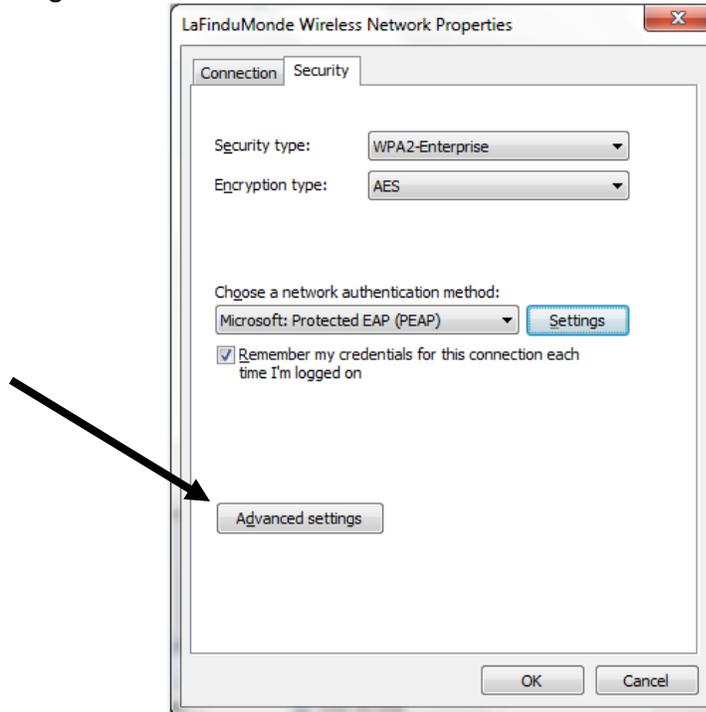
8. Click "Settings".



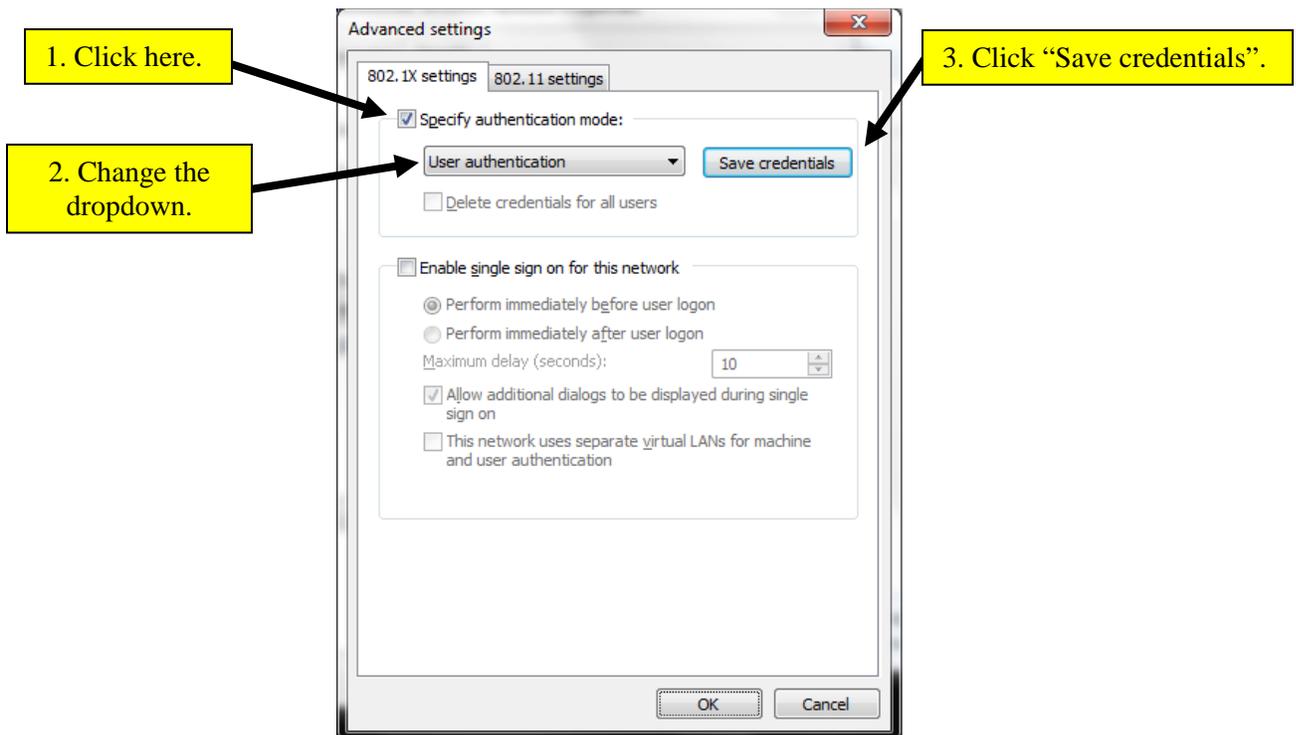
9. The "Protected EAP Properties" screen should look exactly as below. Scroll through the "Trusted Root Certification Authorities" and ensure that "GeoTrust Global CA" is the only option that is selected.



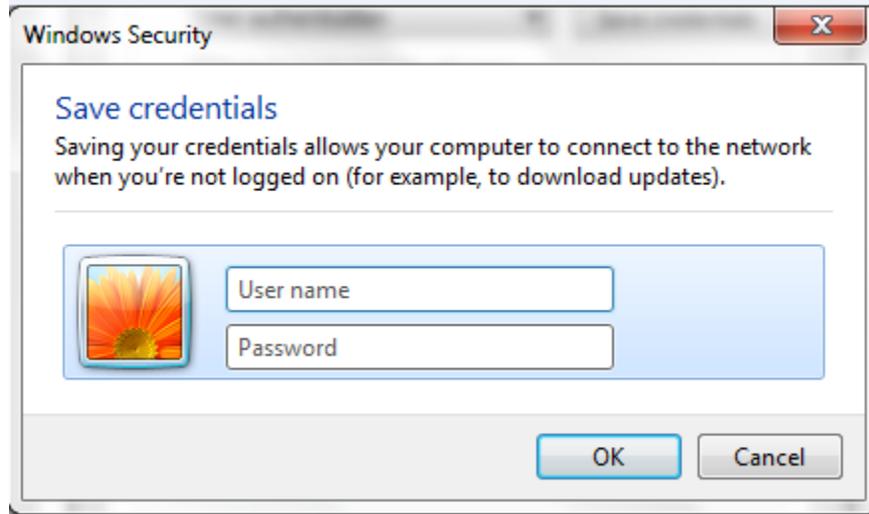
10. The user will be taken back to the “LaFinduMonde Wireless Network Properties” box. Click “Advanced Settings”.



11. Click the box beside “Specify authentication mode:” and change the dropdown to “User authentication”. Then click “Save credentials”.

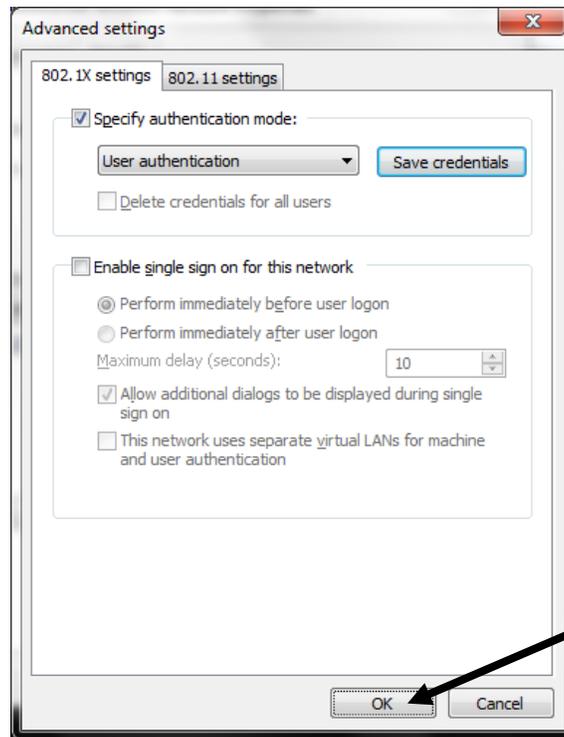


12. The user will now be prompted to enter a user name and password, and then click “OK”.



This user name is the same as your computer and/or Soarian logon. If you are unsure of your user name and/or password, you may use **Access Request** to obtain your username and/or reset your password, as shown on the first page.

13. Once you are back at the “Advanced Settings” window, you can click “OK” to finalize your settings.



14. Click the wireless network icon on the bottom of your screen. **LaFinduMonde** will show as an option. Select **LaFinduMonde** and then click **Connect**.

****If the steps presented do not provide wireless access for your device, please call the Help Desk at 5-7480 for further assistance. ****



Regional One Apple/iOS Device Wireless Setup

- 1.) On your Apple/iOS device, go to **“Settings”** then select **“Wifi”**.
- 2.) Underneath the section titled **“CHOOSE A NETWORK”**, select **“Other”**.
- 3.) In the field **“Name”**, type **LaFinduMonde**. (Note: This is case sensitive, so please type it exactly as it is shown).
- 4.) Select **“Security”**, and choose **“WPA2 Enterprise”**. Once selected, press **“Other Network”** at the top left of the screen.
- 5.) In the field labeled **“Username”**, type your Regional One username. This is the same login information as what you would use with Access Request. (If this has not been provided to you, it is typically your first initial and your last name. Sometimes it will be your first initial, your middle initial and your last name. For example, John E. Smith would have a username of **jsmith** or **jesmith**).
- 6.) In the field labeled **“Password”**, type the password provided to you. This is the same login information as what you would use with Access Request.
- 7.) Once all the information has been entered, select **“Join”** at the top-right of the screen.
- 8.) If you are prompted to install a certificate or trust the certificate, please select **“Trust”**, **“Install”**, or **“Accept”** at the top-right of the screen.
- 9.) You should now have full connectivity to the Regional One network. If you experience any issues, please contact the IT Help Desk at 901-545-7480.



Regional One Android Device Wireless Setup

- 1.) On your Android device, go to **“Settings”**.
- 2.) Go to your **“Wifi”** section, then select **“More”** or locate the selection to **“Add a Network”**.
- 3.) For the **“Network Name”**, please type **LaFinduMonde**. (Note: This is case sensitive, so please type it exactly as it is shown).
- 4.) For the **“Security”**, please select **“802.1x EAP”**
- 5.) For the **“EAP Method”**, select **“PEAP”**
- 6.) For **“Phase 2 Authentication”**, select **“MSCHAPv2”**
- 7.) In the field labeled **“Identity”**, type in your Regional One username. This is the same login information as what you would use with Access Request. (If this has not been provided to you, it is typically your first initial and your last name. Sometimes it will be your first initial, your middle initial, and your last name. For example, John E. Smith would have a username of **jsmith** or **jessmith**).
- 8.) In the field labeled **“Password”**, type the password provided to you. This is the same login information as what you would use with Access Request
- 9.) Leave all remaining fields as they are in the default state.
- 10.) Once finished, select **“Connect”**.
- 11.) You should now have full connectivity to the Regional One network. If you experience any issues, please contact the IT Help Desk at 901-545-7480.



Regional One Health

Compliance Summary

To protect the confidential information of Regional One Health and of our patients, a compliance program has been implemented. Outlined below are some key points of protection.

HIPAA Privacy and Security

- ✓ Only access information that is needed to perform job responsibilities.
- ✓ Ensure that you have the patient's consent *before* discussing any protected health information (PHI) such as diagnosis and treatment information in front of anyone not providing direct patient care (i.e., family members, friends, guards, etc.).
- ✓ Speak quietly when discussing a patient's condition with family members in a waiting room or other public areas.
- ✓ Avoid using patients' names in public hallways and elevators.
- ✓ Emails containing PHI (including attachments) should *ALWAYS* be encrypted.
- ✓ Do not email PHI to a private email address.
- ✓ Do not use your personal email address to send company and patient data.
- ✓ Do not try to bypass any company security controls.
- ✓ Do not share usernames and passwords.
- ✓ Always maintain the security of documents containing PHI (*rounding sheets, etc.*).
- ✓ Never leave information containing PHI unattended.
- ✓ Use a coversheet when sending a fax.
- ✓ Dispose of confidential materials in shredder bins.
- ✓ *Always* log off your computer before leaving your work area.
- ✓ Do not download PHI to a mobile device or jump drive.
- ✓ Photographs should not be taken unless required for patient treatment.
- ✓ Report any suspicious activity to the Privacy Officer and/or your direct supervisor immediately.
- ✓ Report any lost or stolen equipment to IT and/or your direct supervisor immediately.

Social Networking

- ✓ Do not reference *any* PHI, including name, demographic information, diagnosis, or image.
- ✓ Accessing social networking sites is *not* permitted, unless in the performance of duties.

Cell Phone Usage

- ✓ The use of personal cell phones, unless required in the treatment of our patients or for official ROH business, should be limited and not interfere with duties.

*Please note that the items listed are not inclusive of Regional One Health's policies and procedures.

Contact the IT Team

Angela Delashmit, BSN

901-545-7448

aboswell@regionalonehealth.org

Rhonda Roberson, MSN

901-545-7039

rroberson@regionalonehealth.org

Karen Hamilton, RN

901-545-6416

khamilton@regionalonehealth.org

Cherilyn Jones, MSN

901-545-7536

crjones@regionalonehealth.org