



## **How to Use The Patient Portal**

A secure web portal is a kind of webpage that uses encryption to keep unauthorized persons from reading communications or information. Secure messages and information can only be read by someone who knows the right password to log in to the portal site.

**All communication via Patient Portal will be included in your permanent patient record.**

### **Protecting Your Private Health Information and Risks**

This method of communication and viewing prevents unauthorized parties from being able to access or read messages while they are in transmission. However, keeping messages secure depends on two additional factors: the secure message must reach the correct email address, and only the correct individual must be able to get access to it.

Only you can make sure these two factors are present. We need you to make sure we have your correct email address and are informed if it ever changes. Only use your personal email address. You also need to keep track of who has access to your email account, so that only you, or someone you authorize, can see the messages you receive from us.

If you pick up secure messages from a Web site, you need to keep unauthorized individuals from learning your password. If you suspect someone has gained unauthorized access, you should promptly go to the Web site and change it.

### **How to participate in Boston Mountain Rural Health Centers Online Portal**

1. Request access from the front office receptionist
2. After this is complete, you can expect to see a welcome email. On this email you will click on the URL link (web page) and use the assigned login and password.  
<https://myew20.eclinicalweb.com/portal1402/jsp/login.jsp> or you may access the portal by going to [www.bmrhc.net](http://www.bmrhc.net)
3. Once logged into the portal, you should read the consent forms and verify agreement to the terms and conditions of the portal.
4. You should then go to "My Account" on the Left of the page. Here you need to change your password to something only you will know. This is essential to make sure your information remains secure and private!

Implemented May 24, 2012



## **Guidelines for creating secure passwords**

The first step in protecting your online privacy is creating a **strong password**. To help you choose a secure password, we have added password strength meter that lets you know visually how safe your password is as soon as you create it.

### **Tips for creating a secure password:**

- Do not use words that can be found in the dictionary.
- Mix capital and lowercase letters.
- Include symbols like @ , \_ , # , \* and/or numbers.
- Don't use a password that contains personal information (name, birth date, etc.)
- Don't use keyboard patterns (qwerty) or sequential numbers (1234).
- Don't make your password all numbers, uppercase letters or lowercase letters.
- Don't use repeating characters (aaaazzzz).

### **Tips for keeping your password secure:**

- Never tell your password to anyone.
- Never write your password down.
- Never send your password by email.