THE LMR OVER THE INTERNET (LOTI) LOGIN SCREEN WILL BE CHANGING!

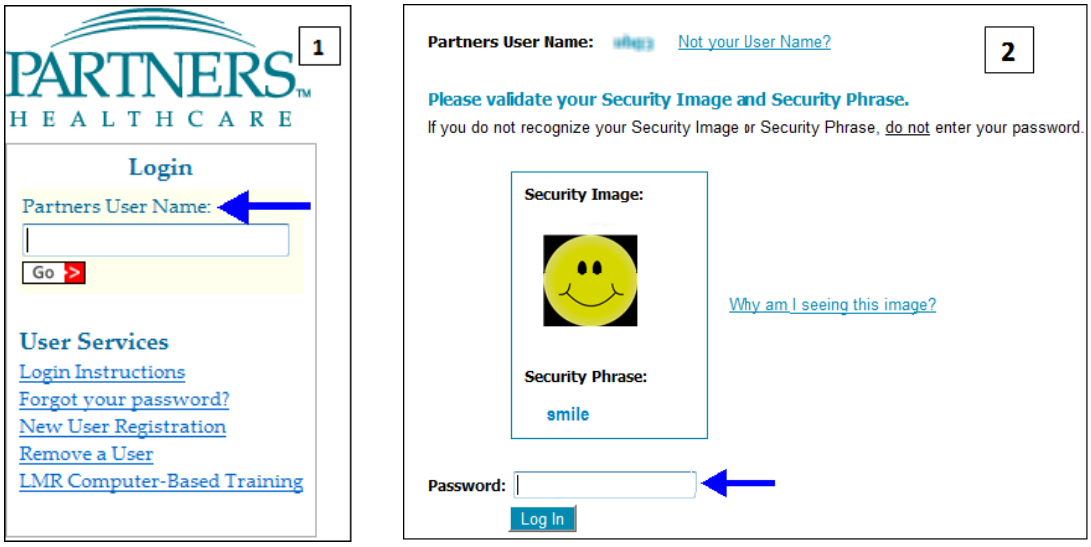
When will this happen?

The Adaptive Authentication security feature will begin in LOTI on **Tuesday**, **May 7, 2013**.

What you will see?

1 The *Partners User Name* field will display on the initial LOTI login screen.

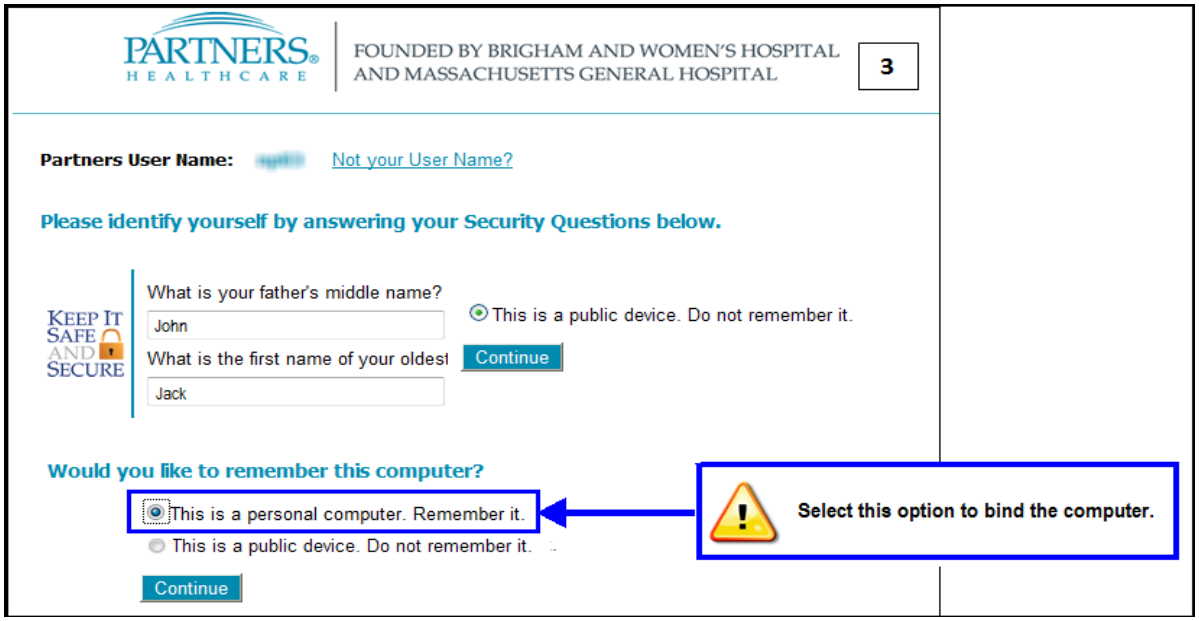
2 Your previously selected security image and security phrase (selected at Password Self Service) will display along with the *Password* field.



3 When accessing LOTI from a computer that is NOT on the Partners network (VPN is considered on network) a prompt will display with previously chosen security questions. For subsequent logins on that same computer, you should *bind that computer* to avoid future security challenges. However, this is NOT recommended for public accessed computers (i.e. Library).

How to Bind a Computer:

1. Login at the LOTI homepage with your Partners User Name. At the next screen, answer your security questions.
2. In the "Would you like to remember this computer?" section select **This is a personal computer. Remember it**. By doing so, you should *not* have to answer the security questions the next time logging into that computer.



What if I have an issue? Who do I contact?

If you do not recognize your security image and phrase, do **NOT** log in. Please call your Help Desk.

For additional assistance or information, please contact your Help Desk. Your LMR Analyst will not be able to assist you with this Partners-level security matter. Help Desk telephone numbers are located at the bottom of each screen of the login process.

Help Desk Phone Numbers			
BWH 617-732-5927	**DFCI** 617-632-3399	**FALK** 617-983-7454	**MCL** 781-416-8940
MGH 617-726-5085	**NWH** 617-243-6001	**NSMC** 978-354-2014	**PCHI** 781-433-3757
PHH 617-726-0790	**PHS** 617-726-5085	**BWH-RICS** 617-525-0848	**SRH** 617-573-2550

What is this Security Enhancement?

As part of the Partners *Keep It Safe & Secure* security awareness campaign which keeps you up to date on best security practices, Partners introduced new security technology called "Adaptive Authentication". This type of security enhancement is currently used by many organizations including the healthcare, financial services, insurance, and manufacturing industries to protect users by balancing security and usability.

In the fall of 2012, the Partners HealthCare Security Information Office implemented Adaptive Authentication with Password Self Service. Starting in February 2013, other web-based applications at Partners such as PeopleSoft, PCHInet, and Insight began using this technology from outside the Partners Network.

Why is the Partners Security Information Office doing this?

Safeguarding your account and making sure that it stays private is a top priority at Partners HealthCare. This security enhancement will introduce a more secure authentication experience for users of the web-based applications than what we currently have. These applications will be secured using the same second-factor authentication technology used by banks and other institutions. It will greatly reduce the risk of remote hackers exploiting and compromising IDs and passwords.

By adding a security image and phrase it helps you recognize when you log in to a valid Partners website. Cyber criminals set up fake websites to steal your ID and password. If you log in to a website and see a security image and phrase that is not yours, you are *not* on a valid Partners website.