Dear Valued Client,

As you may be aware, a new security bug, called Heartbleed, is impacting many organizations throughout the country. Heartbleed affects servers that use certain versions of a cryptography library called OpenSSL. OpenSSL provides security and privacy for sensitive data such as emails, logins/passwords and Protected Health Information (PHI).

The new flaw gives hackers the ability to read the memory of any server using the affected versions of

OpenSSL for protection.

While analysis is ongoing, none of Allscripts solutions directly use OpenSSL for encryption to the best of our knowledge. However, we have discovered that some of our third-party partners may be at risk.

**ATTENTION:** If you use Google, Yahoo, or Facebook authentication to log in to your patient portal account, it is strongly recommended to change the password of your established login method.

We strongly encourage that your organization conduct its own risk analysis as well to determine if the Heartbleed bug may affect the software or infrastructure you use.

You can read more about the Heartbleed bug here.