A screenshot of a computer

Description automatically generated

Above is a screenshot for the successful installation of OpenEMR for Aspirus Hospital.

To secure OpenEMR, I followed the steps shown in the Helpful Steps document. I upgraded the Ubuntu server, enabled automatic security updates, configured the firewall, secured Apache and PHP, and used strong passwords.

Other types of attacks that would be susceptible to the OpenEMR platform include vulnerabilities from untrusted sources causing attackers to have access to files. Phishing emails, phone calls and other means of communication could be used by attackers to trick individuals into revealing sensitive information that could compromise security.