**Evan Rixom**

**SAT5424 Pop Health Info**

**Arch Development Pt 2.**

**2/14/25**

1. Web Page Screenshots:
   1. ASPIRUS:
      1. A screenshot of a computer

         AI-generated content may be incorrect.
   2. BCMH:
      1. A screenshot of a computer

         AI-generated content may be incorrect.
   3. MGH:
      1. A screenshot of a computer

         AI-generated content may be incorrect.
   4. Portage:
      1. A screenshot of a computer

         AI-generated content may be incorrect.
2. Show the steps and commands you used to secure OpenEMR (10 points)
   1. First, I ran sudo mysql\_secure\_installation with he following options:
      1. VALIDATE PASSWORD COMPONENT Y, 2 STRONG SECURITY, REMOVE ANON USER YES, REMOVE TEST DB AND RELOAD PRIV TABLE Y
   2. Then I ran sudo-apt get update and upgrade
   3. Then I enabled automated security updates using sudo apt-get install unattended-upgrades && sudo dpkg-reconfigure --priority=low unattended-upgrades
   4. I then enabled and configured the firewall with: sudo apt-get install ufw && sudo ufw allow http && sudo ufw allow https && sudo ufw allow ssh && sudo ufw enable
   5. I then edited the Apache Security configuration for best practices here: sudo nano /etc/apache2/conf-available/security.conf and then ran sudo systemctl restart apache2 to restart apache.
   6. Keep OpenEMR Up to date.
3. C. What other types of attacks would still be susceptible to the OpenEMR platform? (2 points)
   1. Depending on how SQL and the software is configured, could ne vulnerable to a SQL Injection attack, a cross-site scripting attack, or cross-site request forgery, or Denial of Service.