Checklist

- [ ] Two methods for data at rest: encrypt or destroy PHI
- [ ] All mobile devices must be encrypted
- [ ] Dispose of any PHI properly (shred)
- [ ] Dispose of digital media containing PHI (shred/destroy/erase)
- [ ] Any PHI on paper needs to be locked up when unattended
- [ ] Every computer (laptops) must have a password-protected login
- [ ] Your login should time out after inactivity, lock your PC if you leave
- [ ] No PHI in email including internal emails
- [ ] Educate employees and Business Associates
- [ ] Breach Team
- [ ] Include the new requirements into your Policy and Procedures with specific guidelines and action steps
- [ ] 60 days notice to report a breach for covered entities and business associates
- [ ] >500 report needs to be made to HHS
- [ ] Covered Entities must maintain log of data security breaches - annual submission to HHS
- [ ] Business Associates report breach to the covered entity, the covered entity notifies individuals