1. Application and database sharing the same resources.

smartData : Application and database server separated.

2. Database password is hard coded in the application. Allcode Suggestion: use Aptible or ClearData.

smartData : We have separated all credentials from application folder. In database layer we are following **Authentication, Authorization, and Encryption** for sensitive date like PHI We will implement **Auditing** too.

3. Patient data encryption is not using discernible key management policy. (priority)

Allcode Suggestion: passing a third party application penetration test and implementing a password management for users have not been done.

smartData : We are using AES 256 CTR encryption for patient data and for penetration testing we are using Owasp Zed Attack Proxy (ZAP). Will update you once the testing is done.

4. Login forms should be post using ng-submit not by button onclick functionality. (priority)

smartData: Done

5. When users touch PHI in your web application, this must be recorded and saved to your logging mechanism for two years

smartData : PHI log added.

6. Users password must be unique, at least 8 characters, must include one numeric, upper and lower case letters, and special characters and changed at least every ninety (90) days.  
  
smartData: Restrictions implemented.

7. For root access password must expire within 365 days and length 12 characters and 16 characters

smarTData : Yes, Will do that.

8. Integrity protection for resources from an external server or CDN.  
smartData : All external resources are replaced with local files.

9. Remove autocomplete from password fields  
smartData: Autocomplete removed.

10. Add capcha in contact us form on home page

smartData: Capcha added in contact us form.

11. info@nowaitdoc.com mail id should be in human readable format like info AT nowaitdoc DOT com from dashboard and assets files.

smartData: Done

12. Each person must have an individual account that authenticates the individual’s access to PHI Data. Supplier will not allow sharing of accounts.

smartData: we are already having access control on patient data for different user types.

13. Supplier will utilize two-factor authentication for network access/VPN

smartData: we are already having Jenkins for automated deployment and it is protected by firewall.

14. Architecture, Engineering, Application/Data Landscape Documentation - Supplier must maintain current, accurate, and complete documentation on overall system, network, and application architecture, data flows, process flows, and security functionality for all applications that process or store PHI data. Supplier must employ documented secure programming guidelines, standards, and protocols in the development of applications or systems.

Allcode suggestion: Our recommendation is to use a third party, e.g. Aptible or ClearData.

smartData: Need to check as, we are using AWS and that is fully HIPAA compliant.

15. All application and system development shall follow industry best practices and processes for secure programming. Supplier shall be responsible for verifying that all software developers working on application and system development under this Agreement have been trained on and are knowledgeable and proficient on secure programming techniques and able to deal with all current application vulnerabilities, including, but not limited to OWASP Top 10, WASC TCv2, and the CWE-25.

smartData: we are already following

16. Data Transmission and Storage – Supplier shall not transmit or store data outside the United States, or allow its employees or agents to download, extract, store, or transmit data through personally owned computers, laptops, personal digital assistants, tablet computers, cell phones, or similar personal electronic devices.

Appcode Suggestion: If Device Management is required, this can be done through JAMF or Google Apps Device Policy.

smartData: Need to discuss.

17. Supplier will employ an effective documented change management program with respect to the Services. This includes logically or physically separate environments from production for all development and testing. No data will be transmitted, stored or processed in a non-production environment.

Allcode suggestion: Change Management can be tracked in Aptible or ClearData.

smartData: Jenkins have all the log of change management.

18. Supplier will deploy appropriate firewall, intrusion detection/prevention, and network security technology in the operation of the Supplier’s systems and facilities. Traffic between PHI and Supplier will be protected and authenticated and encrypted. Specifically, firewall(s) must be able to effectively perform stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing. Supplier will review firewall rule sets annually at a minimum to ensure that legacy rules are removed and active rules are configured correctly. Supplier will deploy intrusion detection or preferably prevention systems (NIDS/NIPS) in order to monitor the network for inappropriate activity. Supplier shall deploy a log management solution and retain logs produced by firewalls and intrusion detection systems for a minimum period of one 1 year unless specified otherwise in this Agreement.

Allcode suggestion: This will require a Network Intrusion Detection System (NIDS). ThreatStack has a NIDS that can leveraged.

smartData: we are using HTTPS, encryption etc.

19. All workstations and servers must run anti-virus software. Virus definitions must be updated within 24 hours. Supplier will have current anti-virus software configured to run real-time scanning of machines on a regularly scheduled interval not to exceed seven (7) calendar days.

Allcode response: If you go with one of the third party HIPAA providers, this is much easier as 3rd parties like Aptible are not publicly exposed to the Internet.  
smartData : yes, will make sure.

20. Supplier will minimally utilize the following encryption algorithms and key strengths to encrypt PHI Data when in transit, at rest in any application or system, or transported/stored via any physical media (e.g. tapes, disks, etc.):

smartData: we are using AES 256 CTR mode