SECURITY REQUIREMENTS
FOR LOCAL STORE OF HRS DATA

Security requirements for applications requesting to maintain a local persistent store of HRS data:

1. Local persistent store must be required for application to function properly, i.e., critical features of the application will fail without a local data store.
2. Application server must use HTTPS for all web access. For non-web applications, user access must be achieved through similarly encrypted channels.
3. Application and data storage servers must have appropriate physical access controls.
4. Application and data storage servers must have regularly scheduled OS patching.
5. Application and data storage servers must have regularly scheduled software patching, to include anti-virus and other threat mitigation software updates as appropriate.
6. Application and data storage servers must be protected by appropriate firewalls that deny all traffic from untrusted networks, prohibit all direct public access to the data store, and restrict traffic between the application server and other publicly accessible hosts and the data store to channels required for application function, i.e., block all ports not required for the application server's data access.
7. Communication between application server and data storage must be secured by encryption software like IPSec, SCP, SSL, TLS, etc. Such software must use an encryption algorithm that has no known major security flaws, e.g. AES, 3DES, or Blowfish. Such communication, even when encrypted, should not be routed over the open internet.
8. Sensitive or personal data should be stored in an encrypted form, or at least obfuscated when viewed from outside the application by unprivileged application users. Plain text storage of sensitive or personal data is strongly discouraged.
9. In addition to transactional logging, the data store must maintain an audit log of data updates. Every read access to restricted data should also be logged in the audit log.
10. Shell or command access to application server must be limited to systems administrators and application developers. Ideally, such access should also be IP restricted. Shell or command access to data storage server must be limited to systems administrators and database administrators, and such access must be IP restricted.
11. Shell or command access to all servers should be appropriately encrypted, and ideally traffic to and from the servers should not be routed over the open internet. Access logs must be maintained in accordance with local IT policy, and should be audited for inappropriate access on a scheduled basis. Intrusion detection software or audit policies are strongly encouraged.
12. Server login accounts must be unique for each developer and administrator, and servers should apply a password strength policy requiring that passwords meet generally accepted security standards, e.g., passwords must not contain dictionary words or any variation of personal names, passwords must contain mixed case letters, numbers, and preferably punctuation characters, etc. Level of access should be appropriately restricted to the lowest level of privilege required for access, and any need for elevated privileges should be met by privilege changing software like "sudo" or similar tools. Servers must maintain an audit log of all changes in privilege level exercised through this method.