Configuring User Password Strength

OpenMRS allows user password strength configuration via 'Advanced Settings' or 'Settings (formerly Global Properties from 1.8 downwards)'. This helps in choosing appropriate password strength validation according to your implementation. Though OpenMRS provides the ability to turn off different password validators but it is never a good idea to use weaker passwords for data which has sensitive and confidential patient information.

Read security and authorization standards and protocols here.

Configuration Settings:

Goto Settings (formerly Global Properties from 1.8 downwards) in your OpenMRS server Administration > Advanced Settings and navigate to section having properties prefixed with security.*.
Switch following settings on or off according to your implementation requirements.

- security.passwordCannotMatchUsername
- security.passwordCustomRegex
- security.passwordMinimumLength
- security.passwordRequiresDigit
- security.passwordRequiresNonDigit
- security.passwordRequiresUpperAndLowerCase .

Save settings and your are done!