Security Features of CPDMS.NET

CPDMS has been designed and deployed with patient confidentiality and data security as a top priority. All data for CPDMS is sent over strongly encrypted network channels and stored at rest on strongly encrypted hardware at all times. The system is accessed using the secure HTTPS protocol using a carefully monitored set of secure cipher algorithms that enable a minimum of 256-bit data encryption between hospital clients and the CPDMS Web server at the Kentucky Cancer Registry. Additionally, CPDMS enforces host-based (IP address) access control for each hospital facility along with the required use of Duo multi-factor authentication.
Data for each hospital utilizing CPDMS is stored in an independent database. Access to the hospital database is controlled by designated management staff at each hospital and requires user authentication with the use of strong passwords. Sessions are maintained for each hospital user in CPDMS, which expire after a period of inactivity and require re-authentication to resume work.
Databases for CPDMS reside behind a secure firewall at the Kentucky Cancer Registry. The CPDMS Web application resides in a Demilitarized Zone (DMZ) controlled by the KCR firewall. Access to CPDMS databases is strictly controlled and monitored by KCR technical staff.
Access to any confidential data by KCR technical staff is limited to that required for system support and troubleshooting. No other staff or personnel are allowed access to any hospital databases. KCR strictly adheres to the rules and regulations specified by HIPAA.

Duo-specific guidelines

- With the roll out of Duo for CPDMS, we understand that some of our users do not have a capable device or may not be able to use their personal device as a second authentication factor. Below are listed three hardware-based options that you or your facility could purchase.

  Two of these options require them to be plugged into a USB port on the computer where you will be using CPDMS. You will need to check with your facility IT department to make sure these security keys are compliant with your IT security policies. If USB security keys are not allowed, an offline OTP token is another available option.

  USB Keys:
  - https://www.yubico.com/product/security-key-nfc-by-yubico/
  - https://ftsafe.us/collections/epass-fido/products/k9

  Token option:
  - https://ftsafe.us/collections/otp-authentication-1/products/otp-c100-h41

  Please note that this is not an exhaustive list of options. In general, any USB security key supporting U2F/FIDO and any HOTP token is supported.

Failure to perform the above will lead to a user not being able to log in to CPDMS.NET. Unfortunately, the browser is not specific. It simply says that the page can not be displayed