Test Report Document For Encryption when exchanging electronic health information

Tested By	**ViCarePlus Team, www.vicareplus.com**
Tested On	**20/09/2010**
Total number of testcases	**5**
Number of testcases passed	**5**
Number of testcases failed	**0**

FINAL RULE:
§170.302(v) Encryption when exchanging electronic health information. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2).

§170.210(a)(2). **(a) Encryption and decryption of electronic health information .(2) Exchange. An encrypted and integrity protected link must be implemented.**

Test Case ID	Test Cases Checked	Output	Status
DTR170.302.v – 1: Encrypt electronic health information			
E_01	Follow the steps in Administration->Other->Certificates ,to create SSL Certificate Authority and Server certificates and Configure Apache to use HTTPS.	SSL server certificates were created successfully. Apache was configured to use https.	**PASS**
E_02	Enter the openemr url with http.	Browser automatically redirects to https. The browser checks that the certificate was issued by a trusted party (usually a trusted root CA), that the certificate is still valid and that the certificate is related to the site contacted.	**PASS**
E_03	Check whether the electronic health information is encrypted into human unreadable form.	While using ssl certificates, 1)The web server sends its public key with its certificate.2)The browser checks that the certificate was issued by a trusted party (usually a trusted root CA), that the certificate is still valid and that the certificate is related to the site contacted. 3)The browser then uses the public key, to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data. These steps ensures that encryption is taking place	**PASS**
DTR170.302.v – 2: Decrypt electronic health information			
E_04	Verify that the decrypted electronic health information is readable	After getting the encrypted data, 1)The web server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and http data. 2)The web server sends back the requested html document and http data encrypted with the symmetric key. The browser decrypts the http data and html document using the symmetric key and displays the information in human readable form. This ensures that data is decrypted.	**PASS**
2)The web server sends back the requested html document and http data encrypted with the symmetric key.			
E_05	Verify that the electronic health information was received by the external receiving system, using the encrypted and integrity protected link and based on the transport technology and configuration necessary to communicate with the EHR system	By using the ssl,the data is transferred ,in a secured way using an encrypted and integrity link,between the client and the server	**PASS**