| Requirement | *RequirementSatisfied (Yes/No)* | *Vendor Response/Submission/Comments* |
|---|---|---|
| **§170.302.u: General Encryption** | | |
| Provide EHR documentation that specifies encryption and decryption capabilities and identifies algorithm and encryption key specifications used. | **Yes** | See Below |
| Provide unique test data elements to be used for the testing of this module only. | **Yes** | See Below |

*DTR170.302.u – 1: Encrypt electronic health information*

*1) Examine Vendor-provided EHR documentation to determine if the vendor-identified encryption function utilizes an algorithm specified by the standard.*

*2) The vendor shall verify that the encryption function utilizes an algorithm specified by Annex A of FIPS PUB 140-2*

```
gus@aGustin:~ $ gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2008 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: keyring `/home/gus/.gnupg/secring.gpg' created
gpg: keyring `/home/gus/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 5y
Key expires at Sun 12 Jun 2016 05:49:56 AM MDT
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: LD Landis
Email address: ldlandis@gmail.com
Comment: WV Certification Testing 2011
You selected this USER-ID:
```

```
    "LD Landis (WV Certification Testing 2011) <ldlandis@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
....+++++
.....+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
....+++++
.+++++
gpg: /home/gus/.gnupg/trustdb.gpg: trustdb created
gpg: key 3C8C28FD marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-06-12
pub   2048R/3C8C28FD 2011-06-14 [expires: 2016-06-12]
      Key fingerprint = B819 EF3F 9304 8191 5D8A  F435 6028 5449 3C8C 28FD
uid                  LD Landis (WV Certification Testing 2011) <ldlandis@gmail.com>
sub   2048R/92E084E0 2011-06-14 [expires: 2016-06-12]

gus@aGustin:~ $
```

*3) Using the Vendor-provided test data, the tester shall encrypt the test data using the  encryption function*

```
gus@aGustin:~ $ cat her-name.orig.txt
Her name is Jane Elizabeth.
gus@aGustin:~ $ gpg --encrypt --recipient 'LD Landis' her-name.orig.txt
gus@aGustin:~ $ ls
her-name.orig.txt  her-name.orig.txt.gpg
```

*4) The tester shall verify that the encrypted test data is unreadable*

```
gus@aGustin:~ $ cat her-name.orig.txt
Her name is Jane Elizabeth.
gus@aGustin:~ $ od -x her-name.orig.txt
0000000 6548 2072 616e 656d 6920 2073 614a 656e
0000020 4520 696c 617a 6562 6874 0a2e
0000034
gus@aGustin:~ $ od -x her-name.orig.txt.gpg
0000000 0185 030c 6c4b 7460 e092 e084 0701 47ff
0000020 2738 0d82 6e91 91aa 7548 e282 57ed c2c0
0000040 8ebe ffaf dc85 e369 518e 7908 7963 f26f
0000060 a1ab 415c ceef f82f 3a46 7024 23c1 4cc6
0000100 ec72 afb3 ef87 bc74 b7a2 c748 1d37 204c
0000120 cc85 ab3b 7650 f21d 3801 155c 1275 94ba
0000140 c930 fd10 674d 8460 7627 4388 bcf5 4460
0000160 5bdb f337 9e56 96f1 03d5 a5b8 c64f f08f
0000200 531d 81e3 4a73 74e5 540a 17dd 0f1d 25bd
0000220 a9f2 f8c5 3a0b b63a 1265 85bd 5d4f 6888
0000240 3545 8444 dff1 57cb 12c3 cbe2 899b a35c
0000260 7d74 5d45 2e23 be7c 98dd c4c7 f72e 1845
0000300 594c e795 8728 59fe 27aa bdda fc38 9296
0000320 86ca a6d0 650b 2ad8 3d15 8b3f 8107 94eb
0000340 cfee 20c0 d737 a731 565f 2021 311f f650
0000360 ca04 4f06 6a60 e081 4e6a ec9b 90ca 4ab0
0000400 f80f 9dd0 cf71 7dc0 f934 8cc6 f349 d222
0000420 0166 f9ac 83e9 27a4 605f 9bb8 a196 6cfd
0000440 7e00 e506 d815 dda7 6a86 3bbc 0e06 4c67
0000460 d99d 11e1 a161 4662 acd9 ae72 b4eb 9a7f
0000500 be5f bcd2 54c6 5410 5b50 ac31 0e66 a1c8
0000520 4b6f 09d1 fb09 5e6e aeb1 f502 696e 1473
0000540 a6ca c1e3 dece 05b5 de76 91be 8608 f4ab
0000560 b6a7 2083 7cd0 0011
0000567
gus@aGustin:~ $ od -a her-name.orig.txt.gpg
0000000 enq soh  ff etx   K   l   `   t dc2   ` eot   ` soh bel del   G
0000020   8   ' stx  cr dc1   n   * dc1   H   u stx   b   m   W   @   B
0000040   >  so   / del enq   \   i   c  so   Q  bs   y   c   y   o   r
0000060   +   !   \   A   o   N   /   x   F   :   $   p   A   #   F   L
0000100   r   l   3   / bel   o   t   <   "   7   H   G   7  gs   L  sp
0000120 enq   L   ;   +   P   v  gs   r soh   8   \ nak   u dc2   : dc4
0000140   0   I dle   }   M   g   ` eot   '   v  bs   C   u   <   `   D
0000160   [   [   7   s   V  rs   q syn   U etx   8   %   O   F  si   p
0000200  gs   S   c soh   s   J   e   t  nl   T   ] etb  gs  si   =   %
0000220   r   )   E   x  vt   :   :   6   e dc2   = enq   O   ]  bs   h
0000240   E   5   D eot   q   _   K   W   C dc2   b   K esc  ht   \   #
```

```
0000260   t   }   E   ]   #   .   |   >   ] can   G   D   .   w   E can
0000300   L   Y nak   g   ( bel   ~   Y   *   '   Z   =   8   | syn dc2
0000320   J ack   P   &  vt   e   X   * nak   =   ?  vt bel soh   k dc4
0000340   n   O   @  sp   7   W   1   '   _   V   !  sp  us   1   P   v
0000360 eot   J ack   O   `   j soh   `   j   N esc   l   J dle   0   J
0000400  si   x   P  gs   q   O   @   }   4   y   F  ff   I   s   "   R
0000420   f soh   ,   y   i etx   $   '   _   `   8 esc syn   !   }   l
0000440 nul   ~ ack   e nak   X   '   ] ack   j   <   ; ack  so   g   L
0000460  gs   Y   a dc1   a   !   b   F   Y   ,   r   .   k   4 del sub
0000500   _   >   R   <   F   T dle   T   P   [   1   ,   f  so   H   !
0000520   o   K   Q  ht  ht   {   n   ^   1   . stx   u   n   i   s dc4
0000540   J   &   c   A   N   ^   5 enq   v   ^   > dc1  bs ack   +   t
0000560   '   6 etx  sp   P   | dc1
0000567
```

```
gus@aGustin:~ $ gpg -o her-name.decrypted --decrypt her-name.orig.txt.gpg
You need a passphrase to unlock the secret key for
user: "LD Landis (WV Certification Testing 2011) <ldlandis@gmail.com>"
2048-bit RSA key, ID 92E084E0, created 2011-06-14 (main key ID 3C8C28FD)
gpg: encrypted with 2048-bit RSA key, ID 92E084E0, created 2011-06-14
"LD Landis (WV Certification Testing 2011) <ldlandis@gmail.com>"
gus@aGustin:~ $ ls -l
total 12
-rw-r--r-- 1 gus gus  28 2011-06-14 06:10 her-name.decrypted
-rw-r--r-- 1 gus gus  28 2011-06-14 04:52 her-name.orig.txt
-rw-r--r-- 1 gus gus 375 2011-06-14 06:06 her-name.orig.txt.gpg
gus@aGustin:~ $ diff her-name.orig.txt her-name.decrypted
gus@aGustin:~ $
```

*5) The tester shall document the encryption function used*

From the O'Reilly PGP: Pretty Good Privacy page appearing at:
http://oreilly.com/catalog/9781565920989

PGP is a freely available encryption program that protects the privacy of files and electronic mail. It uses powerful public key cryptography and works on virtually every platform. This book is both a readable technical user's guide and a fascinating behind-the-scenes look at cryptography and privacy. It describes how to use PGP and

provides background on cryptography, PGP's history, battles over public key cryptography patents and U.S. government export restrictions, and public debates about privacy and free speech.

DTR170.302.u – 2: Decrypt electronic health information

1) The tester shall decrypt the test data using the decryption function

2) The tester shall verify that the decrypted test data is readable