Requirement	***RequirementSatisfied (Yes/No)***	***Vendor Response/Submission/Comments***
§170.302.s: Integrity		
Provide EHR documentation identifying the secure hash algorithm (e.g., security strength equal to or greater than SHA-1) used to provide the hash value.	**Yes**	See below
Provide unique test data elements to be used for the testing of this module only. 1) Data used to generate and compare hashes.	**Yes**	See below
Provide instructions on how to use the EHR functions to: 1) Generate and read hash values. 2) Output and store hash values.	**Yes**	See below

The initial data files used in this example differ by a single character, where the 'z' is replaced by an 's'.

```
gus@aGustin:~ $ cat her-name.orig.txt
Her name is Jane Elizabeth.


gus@aGustin:~ $ cat her-name.upd.txt
Her name is Jane Elisabeth.
```

A 'diff'erence between the two files yields:

```
gus@aGustin:~ $ diff her-name.orig.txt her-name.upd.txt
1c1
< Her name is Jane Elizabeth.
---
> Her name is Jane Elisabeth.
```

Confirmation of the contents at a 'binary' level shows that the only difference is the 'z' is replaced by the 's'.

```
gus@aGustin:~ $ od -xa her-name.orig.txt
0000000   6548   2072   616e   656d   6920   2073   614a   656e
   H  e  r sp  n  a  m  e sp  i  s sp  J  a  n  e
0000020   4520   696c   617a   6562   6874   0a2e
  sp  E  l  i  z  a  b  e  t  h  . nl
0000034
gus@aGustin:~ $ od -xa her-name.upd.txt
0000000   6548   2072   616e   656d   6920   2073   614a   656e
        H  e  r sp  n  a  m  e sp  i  s sp  J  a  n  e
0000020   4520   696c   6173   6562   6874   0a2e
       sp  E  l  i  s  a  b  e  t  h  . nl
0000034
```

DTR170.302.s -- 1: Generate hash values

1) *The Tester shall examine Vendor-provided EHR documentation to determine if the vendor-identified secure hashing algorithm used to provide the hash value is equal to or greater in strength than SHA-1 (per FIPS PUB 180-3)*

2) *The tester shall verify that the hash function used is equal to or greater in strength than SHA-1*

3) *Using the Vendor-identified EHR functions, the Tester shall generate two hash values for the Vendor-supplied test data*

```
gus@aGustin:~ $ openssl dgst -sha1 her-name.orig.txt
SHA1(her-name.orig.txt)= 542b4d40408cc58191c03841795918fecd9ae41c
gus@aGustin:~ $ openssl dgst -sha512 her-name.orig.txt
```

```
SHA512(her-name.orig.txt)=9f6778ff650fc878da3da52bb306a1606e12161839e5205bc135\
4a67afe5b5a21efdbf4354162d7121d500427e3cec3c7fd7c601721e1af6ff2a883e82cf0703
```

4) Using the Vendor-supplied test data set, the Tester shall modify the test data

Use her-name.upd.txt rather than her-name.orig.txt (see above for details).

5) Using the Vendor identified EHR functions, the Tester shall generate a hash value for the modified test data set

```
gus@aGustin:~ $ openssl dgst -sha1 her-name.upd.txt
SHA1(her-name.upd.txt)= 8d45a7c8ec566e2fc64e17cba3150f5986e43ad1
gus@aGustin:~ $ openssl dgst -sha512 her-name.upd.txt
SHA512(her-name.upd.txt)= aebfff23739cff4e4271ecb1e55cb78992c2c7b25f8c96b95889\
29f5cdc96cf698a2aff2f24f9c53970cc3cbfe465376971fc9d53dc11fa3f5a31f35946b056d
```

6) The Tester shall output and store the hash value for comparison

7) Tester shall verify that two hash values have been generated from the Vendor-supplied test data and that one hash value has been generated from the modified Vendor-supplied test data

```
gus@aGustin:~ $ sha1sum her-name.orig.txt
542b4d40408cc58191c03841795918fecd9ae41c  her-name.orig.txt
gus@aGustin:~ $ sha512sum her-name.orig.txt
9f6778ff650fc878da3da52bb306a1606e12161839e5205bc135\
4a67afe5b5a21efdbf4354162d7121d500427e3cec3c7fd7c601721e1af6ff2a883e82cf0703\
                                                            her-name.orig.txt
gus@aGustin:~ $ sha1sum her-name.upd.txt
8d45a7c8ec566e2fc64e17cba3150f5986e43ad1  her-name.upd.txt
gus@aGustin:~ $ sha512sum her-name.upd.txt
aebfff23739cff4e4271ecb1e55cb78992c2c7b25f8c96b95889\
29f5cdc96cf698a2aff2f24f9c53970cc3cbfe465376971fc9d53dc11fa3f5a31f35946b056d\
                                                            her-name.upd.txt
```

8) The tester shall document the test data used and corresponding hash values

See above documentation about the contents of her-name.orig.txt and her-name.upd.txt.

9) The tester shall document the hash function used

The SHA1 hash is specified in RFC 3174 – US Secure Hash Algorithm 1.

SHA-512 operates on eight 64-bit words, but the procedure it applies to them closely resembles that of SHA-256. For a description of the algorithm see: http://www.quadibloc.com/crypto/mi060501.htm

DTR170.302.s -- 2: Compare hash values

1) The Tester shall compare the hash values generated in the Generate hash values test using the Vendor-supplied test data

2) The Tester shall compare one hash value generated in the Generate hash value test using the Vendor-supplied test data and the hash value generated using the modified Vendor-supplied test data

3) Tester shall verify that the hash values are the same for the Vendor-supplied test data

4) Test shall verify that the hash values are different for the modified Vendor-supplied test data

DTR170.302.s -- 3: Generate, exchange and verify hash values

1) Tester shall generate a message digest of Vendor-provided test data

2) The Tester shall electronically exchange the Vendor-provided test data and the generated message digest from TE 170.302.s-3.01 to a receiving system (either a Tester's receiving system or a vendor-identified system) using the Vendor-identified transport technology of the EHR. This may require configuration on the part of the Tester's receiving system

3) The Tester shall generate a message digest on the receiving system of the electronically exchanged Vendor-provided test data

4) The Tester shall compare the electronically exchanged message digest and the message digest generated on the receiving system.

5) Tester shall verify that the electronically exchanged message digest and the message digest generated on the receiving system are the same for the Vendor-provided test data