Supplement No. 5 to Part 742—Encryption Registration

Certain classification requests and self-classification reports for encryption items must be supported by an encryption registration, *i.e.,* the information as described in this Supplement, submitted as a support documentation attachment to an application in accordance with the procedures described in §§ 740.17(b), 740.17(d), 742.15(b), 748.1, 748.3 and Supplement No. 2 to part 748 of the EAR.

1. Point of Contact Information
   1. Daniel Boice
   2. 520-250-9420
   3. 1527 E Ironwood Drv Unit A, Phoenix, AZ.
2. Contact Person
   1. Daniel Boice
3. Telephone Number
   1. 520-250-9420
4. Fax Number
   1. 602-674-5834
5. E-mail address
   1. [db@psycheweb.com](mailto:db@psycheweb.com)
   2. dbboice@stu.argosy.edu
6. Mailing Address
   1. 1527 E Ironwood Drv. Unit A, Phoenix, AZ 85020
7. Company Overview (approximately 100 words).
   1. PsycheWeb LLC is a software development company. We develop software applications for use by psychologists and other mental health clinicians.

(3) Identify which of the following categories apply to your company's technology/families of products:

(a) Wireless

(i) 3G cellular

(ii) 4G cellular/WiMax/LTE

(vi) Mobile communications, n.e.s.

(b) Mobile applications

PsyTrack Clinician Tools

(c) Computing platforms

iOS >5.0 iPhone, iPad, iPod

(j) Software

(i) Operating systems

iOS >5.0

(ii) Applications

(p) Other (identify any not listed above)

Developed an iOS application called PsyTrack that utilizes Apple keychain and file protection for the database. The database is encrypted when the phone is locked. The data is encrypted because it could contain private information about clients and clinicians which may be required by the HIPAA. The app has a lock screen that can be activated that requires a four digit pin number to access the app. The four-digit pin is encrypted in a one way hash algorithm and stored in the keychain. The lock screen does not provide additional encryption of the database file beyond the built in encryption provided by apple, but it does block the other views from being accessed by the user.

Section 2.3 of the iOS Developer Program License Agreement specifies,  "You certify that (i) none of the Licensed Applications contains, uses or supports any data encryption or cryptographic functions; or (ii) in the event that any Licensed Application contains, uses or supports any such data encryption or cryptographic functionality, You will, upon request, provide Apple with a PDF copy of Your Encryption Registration Number (ERN), or export classification ruling (CCATS) issued by the United States Commerce Department, Bureau of Industry and Security and PDF copies of appropriate authorizations from other countries that mandate import authorizations for that Licensed Application, as required."

(q) Not Applicable (Not a producer of encryption or information technology items)

(4) Describe whether the products incorporate or use proprietary, unpublished or non-standard cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body. (If unsure, please explain.)

The only use of encryption library (Security.framework provided by apple) is to encrypt and verify the pin number stored in the hash in the keychain when using the in app lock screen. The app also downloads an encrypted file from the internet for use in the application. The encrypted file is a list of drug names in an sqlite database. The file is located at the following URL: NSURL \*url = [NSURL URLWithString:@"http://dl.dropbox.com/u/96148802/pt/dFile-001.zpk"];

The file is then decrypted with the following string: NSString \*symetricString=@"8qfnbyfalVvdjf093uPmsdj30mz98fI6";

NSData \*symetricData=[symetricString dataUsingEncoding: [NSString defaultCStringEncoding] ];

PTTEncryption \*encryption=[[PTTEncryption alloc]init];

NSData \*decryptedData=nil;

if (symetricData.length==32) {

decryptedData=(NSData \*) [encryption doCipher:fileData key:symetricData context:kCCDecrypt padding:(CCOptions \*) kCCOptionECBMode];;

}

(5) Will your company be exporting “encryption source code”?

No.

(6) Do the products incorporate encryption components produced or furnished by non-U.S. sources or vendors? (If unsure, please explain.)

No.

(7) With respect to your company's encryption products, are any of them manufactured outside the United States? If yes, provide manufacturing locations. (Insert “not applicable”, if you are not the principal producer of encryption products.)

not applicable