THE UNIVERSITY OF BRITISH COLUMBIA

UBC Health

Guidelines for Sharing Student Information Electronically

To provide guidelines to UBC Health Programs regarding electronic information sharing

APPROVAL DATE: APRIL 19, 2015
LAST REVISION: APRIL 19, 2015
DOCUMENT NUMBER: PEC – 1 DRAFT V.1

THE UNIVERSITY OF BRITISH COLUMBIA

UBC Health

CONTENTS

APPLICATION, BACKGROUND/INTRODUCTION 2

GUIDELINES 3

DEFINITIONS 6

KEY RELEVANT DOCUMENTS 6

DOCUMENT MANAGEMENT AND CONTROL 6

TITLE

Sharing Student Information Electronically

APPLICATION

These guidelines apply to preceptors, staff, faculty and pre-licensure students in *UBC Health Programs*

BACKGROUND/INTRODUCTION

Prepared for review by the UBC Health Practice Education & Curriculum Committees
This document is governed by UBC's Information Security Standard #03, Transmission and Sharing of UBC Electronic Information, which is based on Office of the University Counsel's recommendations regarding the Acceptable Use and Security of UBC Electronic Information and Systems.

Some *UBC Health Programs* provide their preceptors, staff, faculty, and pre-licensure students with a secure online interface, to allow for safe transmission of personal information. For example, the Department of Physical Therapy preceptors utilize *HSPnet* to complete student assessments and feedback documentation. However, not all *UBC Health Programs* have a secure online interface. Therefore, this document describes three options for securely sending student assessment information. For the electronic options, all information transmitted is at risk of interception or copying. It is the responsibility of UBC employees and students to protect confidential or sensitive information shared electronically.

GUIDELINES

1. OPTION 1

1.1 It is preferable for you to have a secure online interface that would allow the preceptors to enter their feedback directly into the system.

2. OPTION 2

2.1 In the absence of this, the preceptors can enter their feedback in a Microsoft Word file and send it by email. However, as email is not a secure method of communication, the file must be *encrypted* (as per section 9 of the above Information Security Standard). You can give all the preceptors the same password to use, and just change it once a year.

2.2 **How to *Encrypt* files using common applications:** Information Security Standard

2.3 **How to *Encrypt* a Word Document with a Password**

Note: Microsoft Word, Excel, and PowerPoint 2007 (or newer, with the exception of Office 2011 for Mac) *encrypts* information using a "Protect" function; this function does not simply password protect a file, but fully *encrypts* it using AES *encryption*.

Difficulty: Easy **Time Required:** Less than 5 Minutes

Here's How:

2.3.1 Select the **Office Button Icon - Prepare - *Encrypt* Document** or for earlier versions select **File - Protect Document - *Encrypt* with Password**.

2.3.2 Type in password (*password will be provided by UBC program*) and click OK.

2.3.3 Re-enter the password for verification and click OK.

Tips: To remove password *encryption*, follow the same sequence except you will erase the passwords by clicking in that box and backspacing. To set a password for those who can edit a document (meaning for all others it will be read-only), click the **Office Button Icon or File - Save As - Tools - General Options - Password to Modify: type a new password - Re-type the**

password - OK - Save.

2.4 How to *Encrypt* a PDF Document with a Password:

2.4.1 Open the PDF and choose **Tools** > **Protect** > ***Encrypt*** > ***Encrypt* with Password**.

2.4.2 If you receive a prompt, click **Yes** to change the security.

2.4.3 Select **Require a Password to Open the Document**, then type the password in the corresponding field. For each keystroke, the password strength meter evaluates your password and indicates the password strength.

Password Security - Settings let you save a password to open a PDF

2.4.4 Select an Acrobat version from the **Compatibility** drop-down menu. Choose a version equal to or lower than the recipients' version of Acrobat or Reader.

Options control compatibility with previous versions and type of encryption

The **Compatibility** option you choose determines the type of *encryption* used. It is important to choose a version compatible with the recipient's version of Acrobat or Reader. For example, Acrobat 7 cannot open a PDF *encrypted* for Acrobat X and later.

Acrobat 6.0 And Later (PDF 1.5) *encrypts* the document using 128-bit RC4.
Acrobat 7.0 And Later (PDF 1.6) encrypts the document using the AES *encryption* algorithm with a 128-bit key size.
Acrobat X And Later (PDF 1.7) *encrypts* the document using 256-bit AES. To apply 256-bit AES *encryption* to documents created in Acrobat 8 and 9, select Acrobat X and Later.

2.4.5 Select an *encryption* option:

2.4.5.1 *Encrypt* All Document Contents. *Encrypts* the document and the document *metadata*. If this option is selected, search engines cannot access the document *metadata*.

2.4.5.2 *Encrypt* All Document Contents Except *Metadata*. *Encrypts* the contents of a document but still allows search engines access to the document *metadata*.

Note: The iFilter and the Find or Advance Search commands of Acrobat do not look into the PDF's *metadata* even when you select the ***Encrypt* All Document Contents except *Metadata*** option. You can use a search tool that takes advantage of XMP *metadata*.

2.4.6 ***Encrypt* Only File Attachments.** Requires a password to open file attachments. Users can open the document without a password. Use this option to create security envelopes. This option encrypts only file attachments while they are stored in the .pdf document.

3. OPTION 3

3.1 The preceptors can mail student assessments (in paper format).

DEFINITIONS

The following definitions apply to these guidelines:

Encrypt/Encrypts/Encryption - this is the process of making information unreadable, in order to protect it from unauthorized access. Encryption creates a secret key or password that is necessary to unencrypt information and make it readable.

HSPnet – the Health Sciences Placement Network (HSPnet) is a web-based system to manage practice education in the health sciences across Canada

Metadata – this may include document elements such as title, file format, language, creator, and date. Metadata standards vary among repositories, disciplines, and organizations

UBC Health Programs – inclusive of Faculty of Dentistry, Faculty of Medicine, School of Nursing, Faculty of Pharmaceutical Sciences, School of Social Work

KEY RELEVANT DOCUMENTS

Include the following:

Information Security Standard #05: Encryption Requirements

DOCUMENT MANAGEMENT AND CONTROL

Owner: UBC Health

Content manager: UBC Health Practice Education Committee

Date approved: Consideration of draft V.1: October 2015

Review date: This document shall be reviewed every (2) years and after approval, and thereafter as deemed necessary by PEC