**Transfer of Paper Documents via the IMITS Secure File Transfer Platform (SFTP)**

**Responsibilities of the Provider**

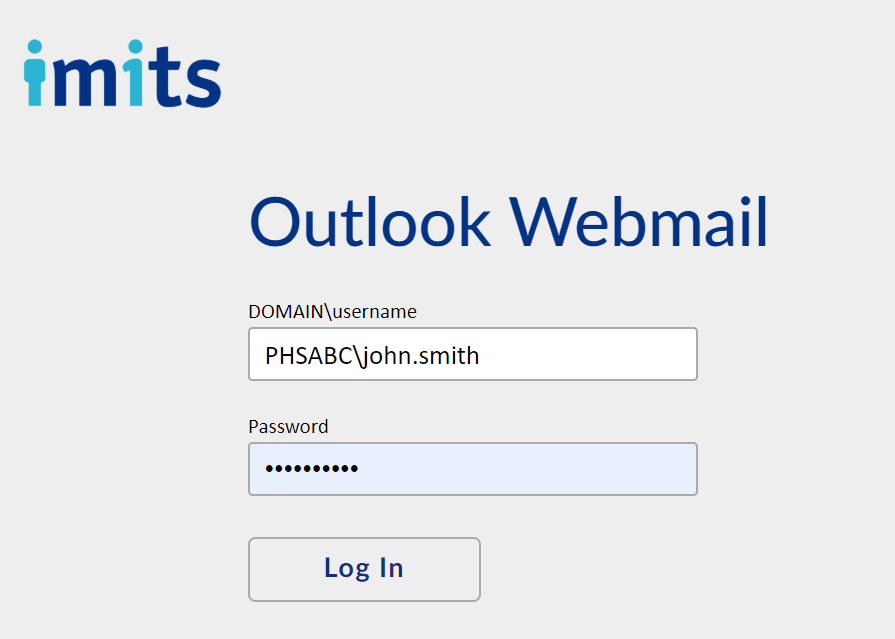
* Clinicians and providers working remotely are responsible for securely storing any paper files when not in use. This means locking files away and not leaving any files in your vehicle. If you are working remotely and not using a PHSA-issued laptop, do not share a laptop or desktop computer used for working with personal information with other individuals, including family members and friends.
* PHSA staff and physicians must complete the mandatory course on privacy and confidentiality: <https://learninghub.phsa.ca/Courses/3544/privacy-and-security-101>.
* Clinicians and providers must use their PHSA email address to securely transfer and receive paper documents.
* On-site clinicians are to ensure the secure transfer of paper documents requested by clinicians and providers working remotely.
* Clinicians and providers working remotely are responsible to ensure the secure transfer of paper documents sent back to the site. This includes transferring paper documentation back to the site electronically using the IMITS Secure File Transfer Platform AND ensuring a process is in place to a) confirm receipt and b) ensure legibility of document image. The paper documents can then be confidentially shredded once a) and b) are met. If you do not have access to a shredder when working remotely, upon return to the site bring in paper documents to shred or mail the documents back to the site to be shredded.

**Remote Email Access**

When working remotely, PHSA email can be accessed by visiting: <https://wm.phsa.ca>

The provider can then log in using their PHSA credentials:

* **Username:** PHSABC/john.smith
* **Password:** same as your usual PHSA password



**Password Protection:**When Sharing Microsoft Office documents, consider password protecting them, so the files remain protected even if they are distributed to others by your recipient. This particularly applies if the files contain sensitive information.

**Microsoft Office Adding or removing protection article:**<https://support.office.com/en-us/article/Add-or-remove-protection-in-your-document-workbook-or-presentation-05084cc3-300d-4c1a-8416-38d3e37d6826>

**Process – Paper to Electronic Chart Transfer**

* Clinicians can request documentation by submitting a completed Documentation Request Form to their site administrative contact or nurse by email. If you do not know who to email, please contact your site for instructions. The request form has 3 tabs, so clinicians must select the appropriate site (FPSC, FPH, or HCW) at the bottom of the document before filling out the form.



* The requested paper-based client charts will be collected by a designated staff member.
* The requested information will be scanned into the IMITS Secure File Transfer System (<https://sftp.phsa.ca/WebInterface/login.html>) and then returned to the paper file.
* Clinicians should request all required documentation no less than 2 business days before their session with a client. Depending on the volume of information requested, the documentation will be sent to the clinicians via the IMITS Secure File Transfer System within 24 hours of their appointment with the client.
* Clinicians can access the information by logging into the IMITS Secure File Transfer platform (see process below).
* All files uploaded to the IMITS Secure File Transfer platform will be automatically deleted after 7 days. Files may be deleted sooner than this by the staff who uploaded them if they are confirmed to no longer be useful.

**Process – Secure Electronic Transfer of Documents via the IMITS Secure File Transfer Platform**

* If a fax machine is not available, this is the next preferred method.
* To use SFTP, Internet Explorer 11 (or higher) or Google Chrome is required
* The maximum file size for transfer is 100MB, and maximum folder size for transfer is 100MB.
* Media files and executable files cannot be uploaded to the service for transfer.
* There is a 15-minute [IMITS Secure File Transfer Training online course](https://learninghub.phsa.ca/Courses/8388/imits-secure-file-transfer-training) to take and is found on the LearningHub.
* Instructions on how to use SFTP are:



* **Note:** once documents transmitted via SFTP are no longer needed, clinicians working remotely must delete them from their computer, and then empty the recycle bin **in order to permanently delete the records**. Otherwise the personal patient information still remains on their local hard drive.

**SFTP User Support:**For service support, please contact the service desk at **604-675-4299**. **Support is available during business hours (Monday-Friday, 09:00 to 17:00).**

**Provider User Agreement**

***I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, hereby acknowledge that I have reviewed the responsibilities and procedures described above, and will adhere to these requirements when using the IMITS SFTP to transmit personally-identifying information.***

***Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***