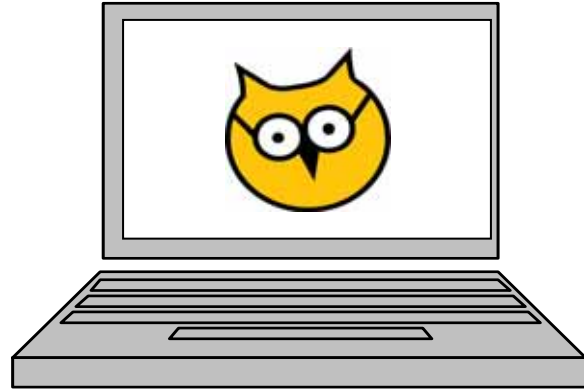


# Protecting PHI on Electronic Devices

For UHN Personnel (non-research)

Updated August 19, 2010



## TABLE OF CONTENTS

<b>PROTECTING PHI</b>	1
Why is this important?	1
What are my responsibilities?	1
<b>DELETING PHI</b>	1
Why should I delete unnecessary PHI?	1
What can I delete?	1
What do I need to keep?	2
How do I delete files from my UHN computer?	2
How do I delete unnecessary email?	4
How do I delete files from a non-UHN computer?	6
How do I to delete files from a network drive?	6
How do I move files to a network drive?	6
<b>STORING PHI</b>	7
Where should I store PHI?	7
Where do I find my network storage?	7
How do I get more network storage space?	8
How do I access network storage remotely?	8
<b>ENCRYPTING PORTABLE DEVICES</b>	9
When am I allowed to store PHI on a portable device?	9
How do I know if my laptop is encrypted?	9
I have a USB. How do I encrypt it?	9
<b>HELPFUL CONTACTS</b>	10
<b>PROTECTING MY DEVICE CHECKLIST</b>	11

## PROTECTING PHI

### Why is this important?

Protecting electronic files containing *personal health information* (PHI)...

- is the law - and you are personally accountable for outcomes, which may include personal fines
- is your responsibility to UHN and to your professional college

... because misusing or losing PHI...

- may cause distress to patients who must be told about incidents
- is costly to UHN to investigate and tell patients

### What are my responsibilities?

- ✓ Deleting unnecessary files containing PHI asap.
- ✓ Storing PHI in the most secure place – on the network, not a device.
- ✓ Encrypting any portable device where PHI is stored.
- ✓ Protecting portable devices when outside the hospital.

***PHI must not be copied or saved to any electronic device unless access to the information is absolutely required to complete job duties and access to a secure network is not possible.***

## DELETING PHI

### Why should I delete unnecessary PHI?

The hospital is responsible for PHI from the time it is created or collected to the time it is destroyed – even if it is no longer actively used. Deleting PHI decreases the risk of inappropriate use or disclosure.

### What can I delete?

- ✓ Information you are not required to keep by law (e.g. list of patients discussed at rounds)
- ✓ Information you don't need anymore (e.g. fax cover sheet)
- ✓ Copies of information stored in the medical record

### What is a portable device?

Any device that can store electronic files and is portable:

- Laptop
- USB key
- External hard drive
- Smartphone: iPhone, Blackberry, PDA



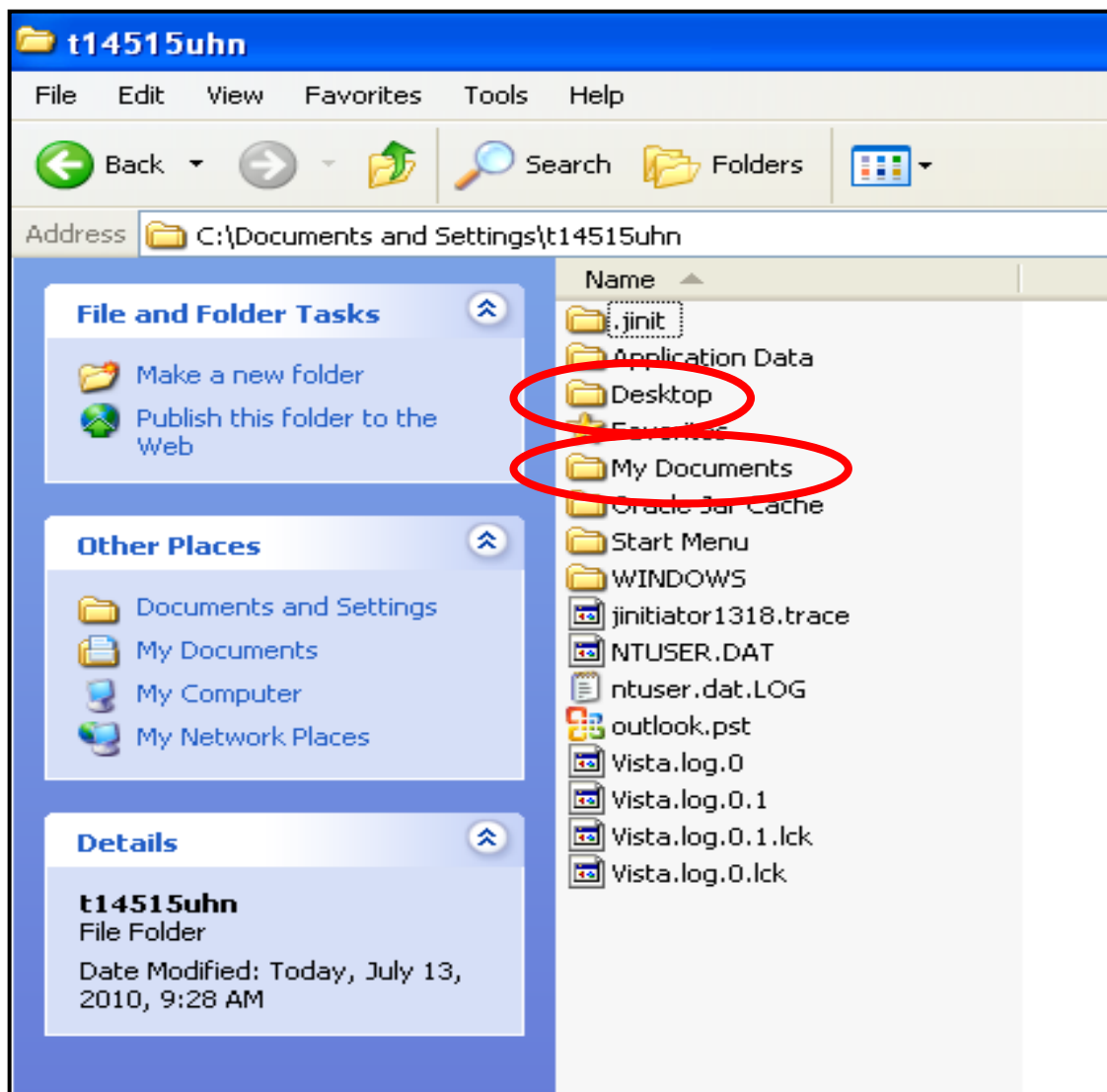
## What do I need to keep?

Document all clinically relevant information in the patient's paper or electronic record and consult the Medical Records policy for more detail.

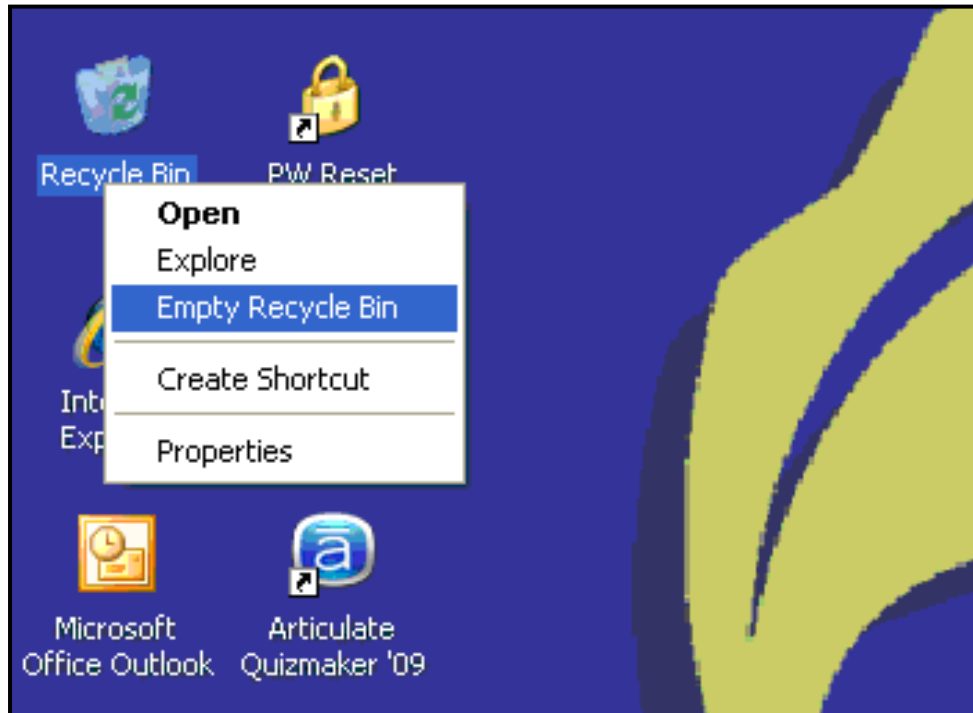
Consult the Administrative Retention policy to identify if and how long to keep legal, financial, HR and other types of corporate confidential information.

## How do I delete files from my UHN computer?

1. From the 'Start Menu' go to 'My Computer'. Click on the 'C' drive. Click on 'Documents & Settings' and look for a folder with your tID. Delete files from the following sub-folders by right clicking on the file and selecting 'Delete':
  - Desktop
  - My Documents folder



2. After you have deleted files, don't forget to empty the Recycling Bin (found on Desktop or Start Menu) by right clicking on the icon and selecting "Empty Recycle Bin". Copies of deleted files are saved in the Bin until you empty it.



### What is Personal Health Information?

Any information about an individual (living or deceased) that (a) identifies a specific patient and (b) connects them to UHN.

It's not just information in the medical record – it could be in any record or system, in any form (e.g. microfilm, photo, video, audio recording, email, Excel file, etc.).

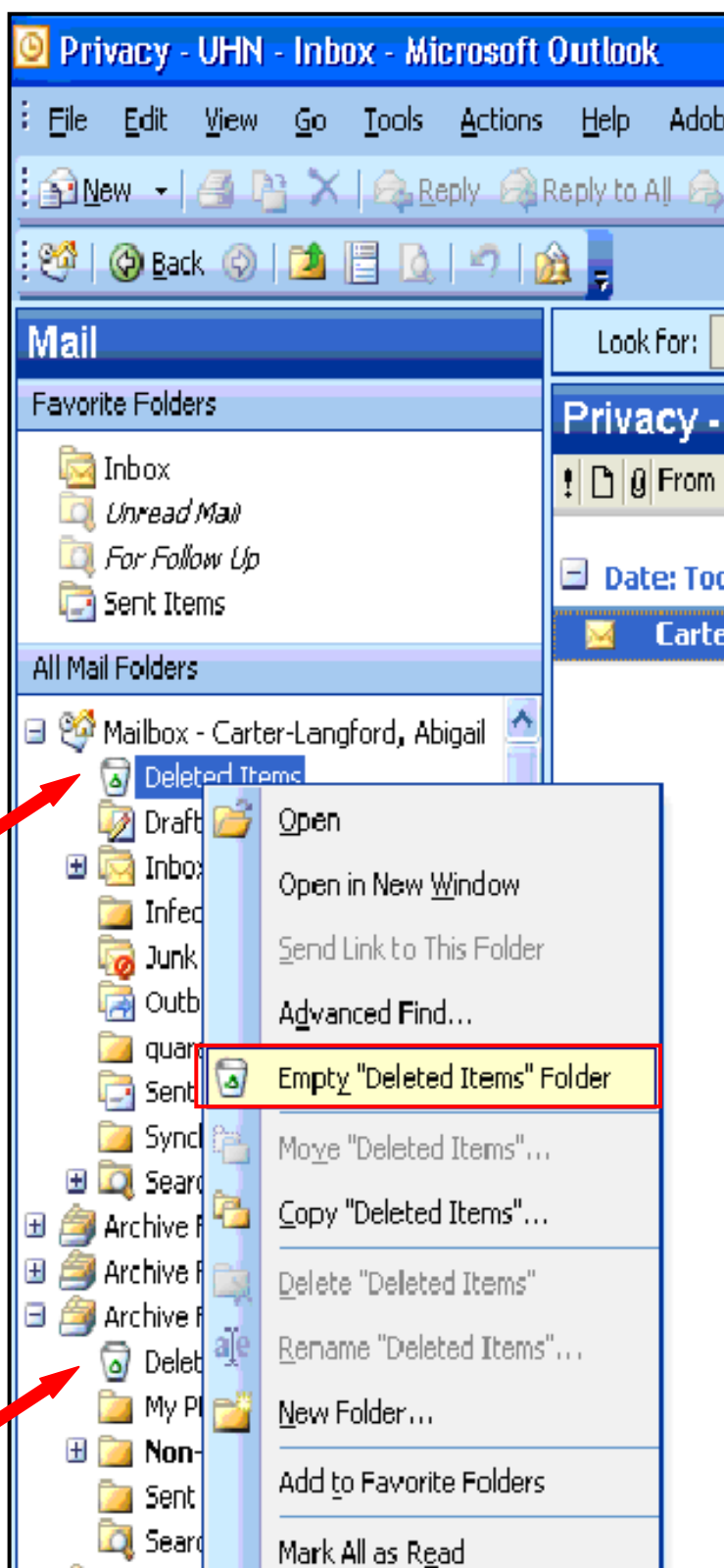
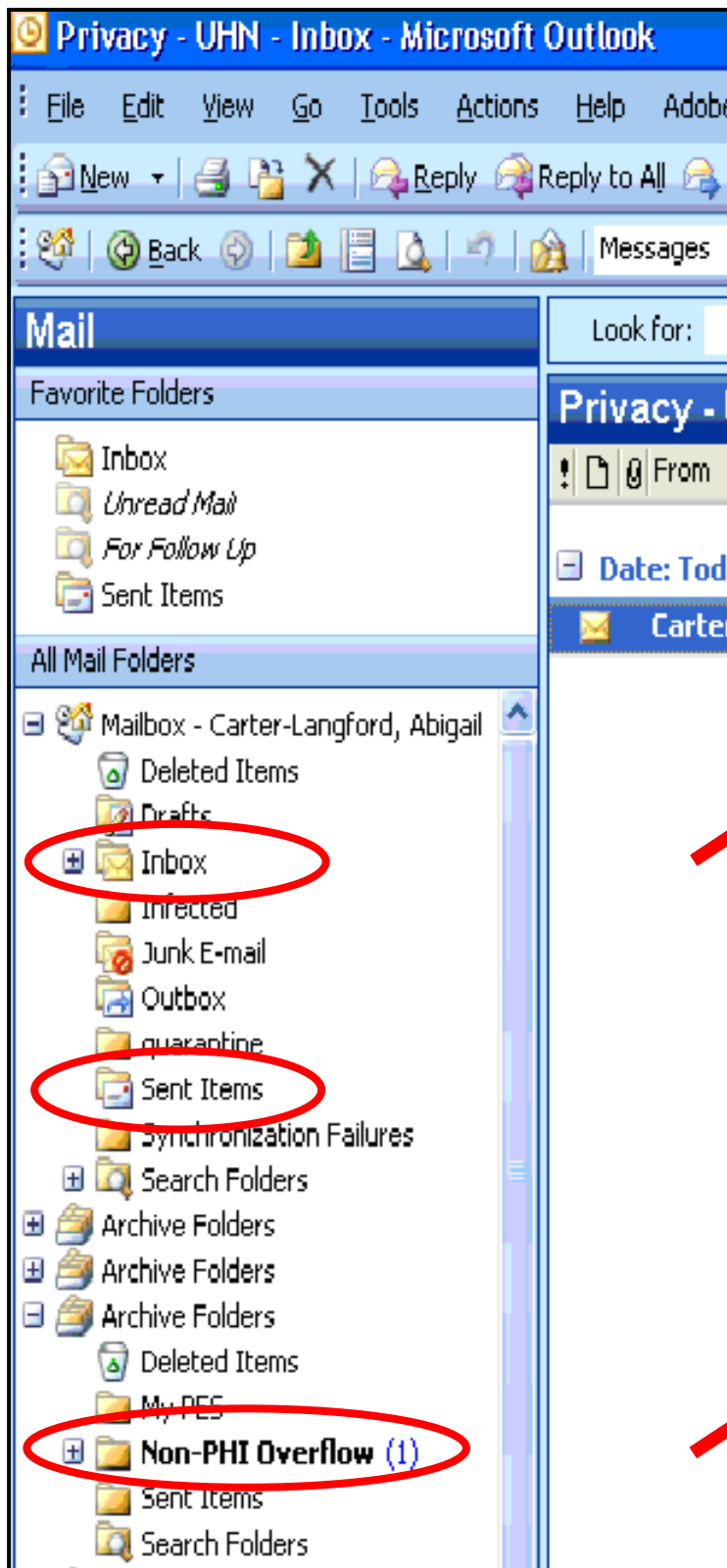
#### Examples

- physical or mental health conditions, test results, treatments, medications, blood type, images, consult notes
- name of physician, other care provider, or SDM
- organ or tissue donation
- OHIP, MRN or other identifying numbers
- Research participation, data or test results



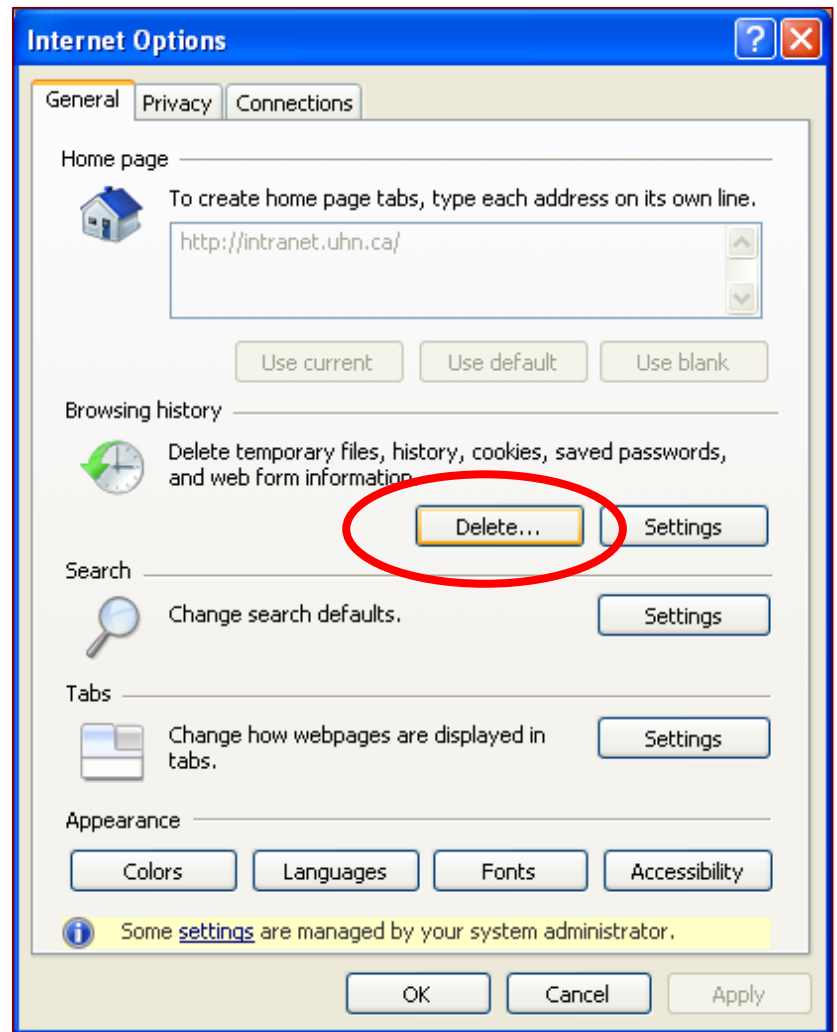
## How do I delete unnecessary email?

1. Right click and select 'Delete' to delete emails from your Inbox and each archive (or 'Personal Storage Folder') you have. Don't forget Sent Items.
2. Right click and select 'delete' on each 'Deleted Items' folder under your Inbox and each of your archives or 'Personal Storage Folders' to empty them.



3. Every time you open a document from your webmail or another internet page a copy is saved to your computer. To delete these files:

- open your web browser (e.g. Internet Explorer)
- from the 'Tools' menu, select 'Internet Options'
- under 'Browsing History' click 'Delete' then 'Delete All' (or select the types of files to delete).



## How do I delete files from a non-UHN computer?

PHI must be saved on a UHN network, except where permitted by the [Storage, Transport & Destruction of Confidential Information](#) policy. If PHI has been saved to a non-UHN computer (e.g. past work from home):

1. Delete all files with PHI ASAP using the methods on pages 2-5.
2. Before throwing out, recycling or reselling the computer, contact the [Information Security Office](#) for suggested tools to ensure all copies of confidential files have been deleted.

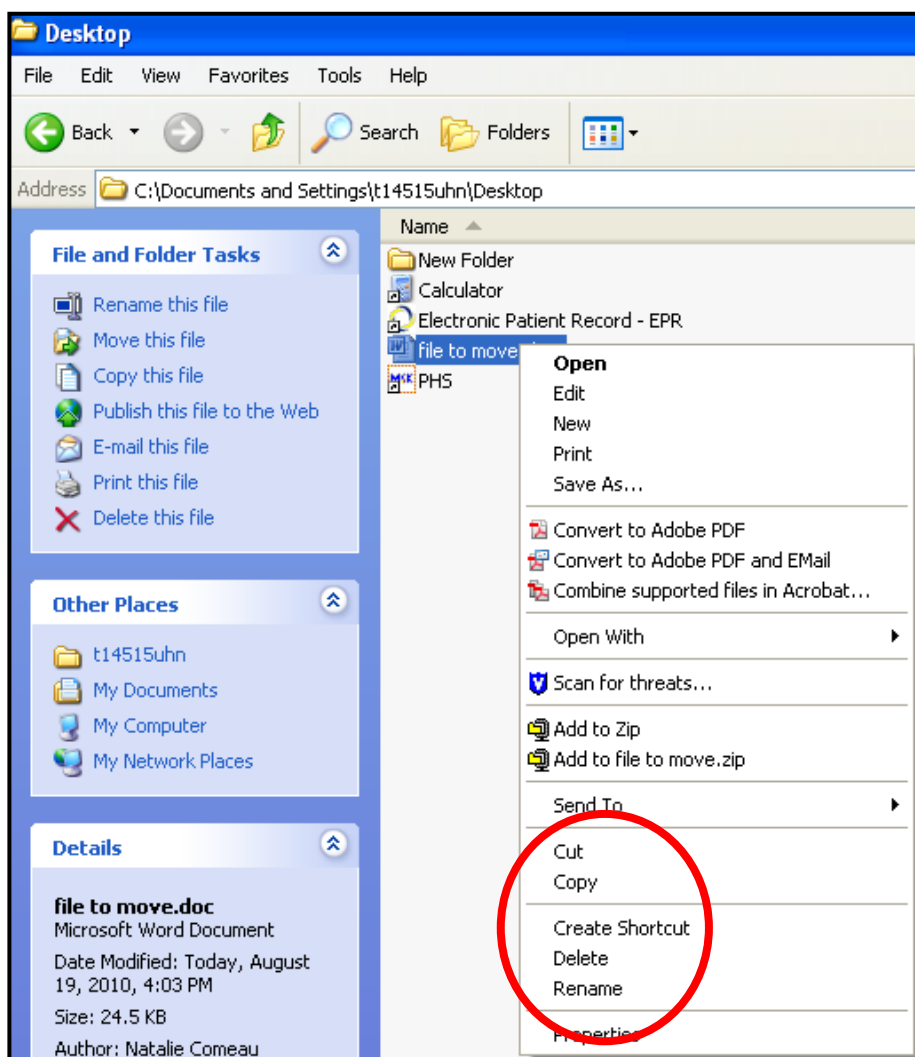
## How do I delete files from a network drive?

Right click and select 'delete' to delete the file. Note: Once deleted, there is no guarantee of recovery.

## How do I move files to a network drive?

A UHN network is the most secure place to store confidential files.

1. In a 'My Computer' window, click on the drive and/or folder where the file is stored (e.g. 'Documents and Settings' or a USB drive).
2. Click on the file you want to move, right click, and select 'copy'.
3. Open your network drive folder, right click, and select 'paste'. Verify that the pasted file can be opened.
4. Go back to the original drive & folder where you cut the file from, right click on the file, and select 'delete.'



## STORING PHI

### Where should I store PHI?

Store all electronic files containing PHI on a **UHN network**.

Files stored on a UHN network are:

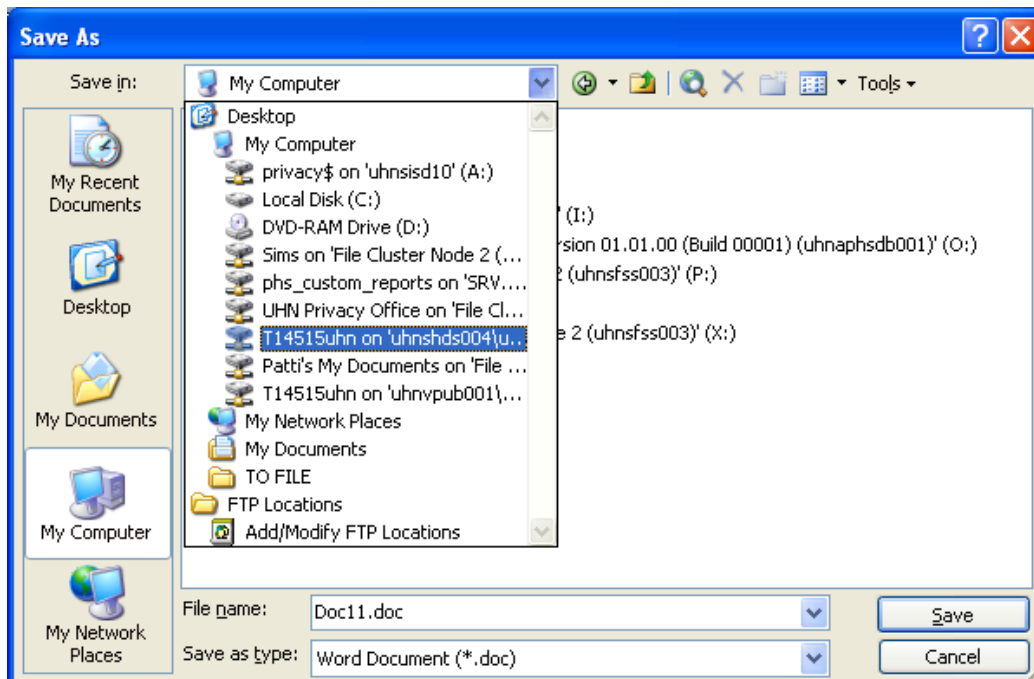
- ✓ stored in a secure location,
- ✓ backed up regularly,
- ✓ accessible from any computer across UHN, and
- ✓ accessible securely from home or away (via VPN)!

Alternatives to saving to the network:

1. **De-identify the PHI** – remove enough information from the file so that individual patients cannot be recognized.  
or
2. **Encrypt the device** - if identifiable PHI is necessary.

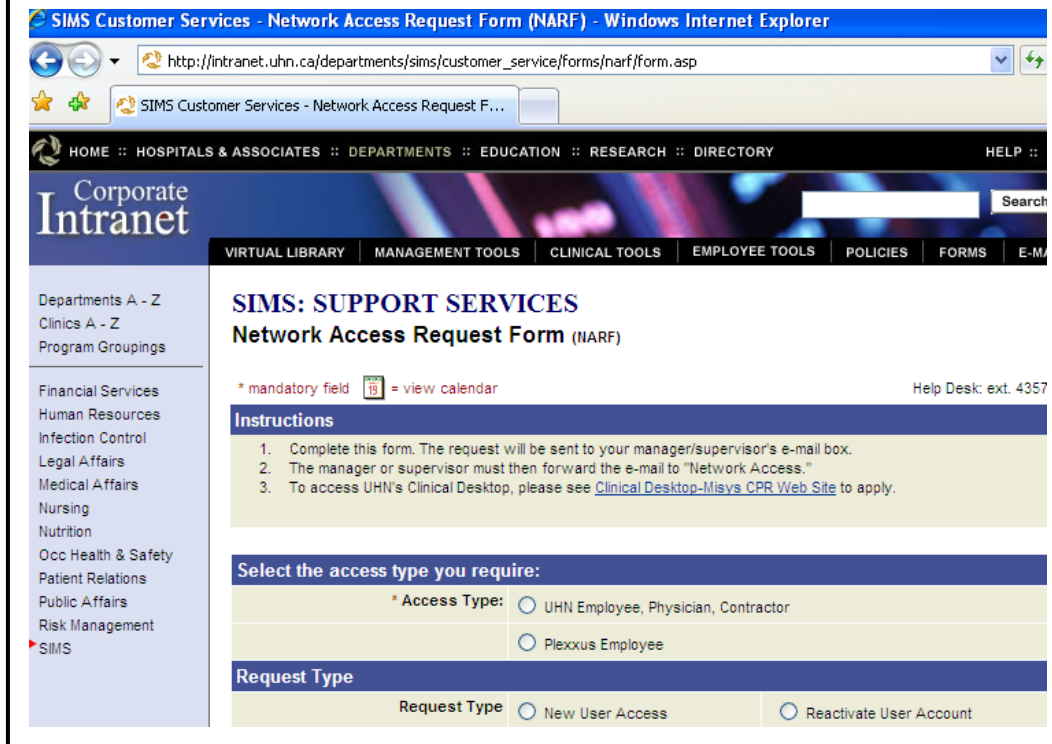
### Where do I find my network storage?

Look under “My Computer” for a drive that starts with your t-ID number or call the Service Desk for help if you can’t find it. This is your personal storage space on the UHN network. Only you can access the information stored on this drive.



## NARF (Network Access Request Form)

The [NARF](#) is found on the Intranet under 'Online Forms':



The screenshot shows a web browser window titled "SIMS Customer Services - Network Access Request Form (NARF) - Windows Internet Explorer". The address bar shows the URL: [http://intranet.uhn.ca/departments/sims/customer\\_service/forms/narf/form.asp](http://intranet.uhn.ca/departments/sims/customer_service/forms/narf/form.asp). The page header includes navigation links: HOME :: HOSPITALS & ASSOCIATES :: DEPARTMENTS :: EDUCATION :: RESEARCH :: DIRECTORY. The main content area is titled "SIMS: SUPPORT SERVICES" and "Network Access Request Form (NARF)". It includes a sidebar with a list of departments, a "Instructions" section with three numbered steps, and a form section with radio buttons for "Access Type" (UHN Employee, Physician, Contractor or Plexxus Employee) and "Request Type" (New User Access or Reactivate User Account).

You may have access to a **shared network drive** where some or all of a team or group of people can access the same documents. Ask your manager to submit a NARF if you need access to a shared drive.

### How do I get more network storage space?

Submit a NARF if you need more space on a personal or shared drive.

### How do I access network storage remotely?

Securely access files stored on a network drive by using **Virtual Private Network (VPN)**. You can also access networked applications (e.g. EPR, Outlook) through VPN. Access files using your UHN laptop, software installed on the laptop, and a special VPN token that provides part of the password needed to gain access to the network.

If you must access networked applications or drives from a home computer, special VPN software is provided for installation. Access to EPR may be provided from any PC with an Internet connection.

To request VPN access, fill out a NARF or check out the [Remote Access](#) page on the Intranet.

## ENCRYPTING PORTABLE DEVICES

### When am I allowed to store PHI on a portable device?

Only if (a) you can't access it on the network through VPN *and* (b) you can't de-identify it (because you need to identify patients) *and* (c) the device is **encrypted** (whether it's a UHN or personal device).

### What is a 'strong password'?

A 'strong' password is one that is sufficiently complex to deter password cracking. To create a strong password, choose:

- 8 or more characters
- numbers & letters, in upper & lower case

### How do I know if my laptop is encrypted?

SIMS	All SIMS-issued laptops are encrypted.
RIS	If you have a personal or purchased device used for research, check with RIS (18-7777).
Other	Departments with internal IT (e.g. MI, RMP, Rehab Solutions) can verify the status of non-research devices.
Personal	If you have a personal or purchased device that will not be used for research, watch for upcoming instruction and tools.



### I have a USB. How do I encrypt it?

To see if you have encryption software on your UHN computer:

- plug in your USB
- go to "My Computer" and right click on the drive
- look for the "Encrypt media" option
- follow the instructions

Once you encrypt a USB, you will need to [download](#) and install the free version of the Winmagic SecureDoc Media Viewer to access your files from a non-UHN computer.

Note: Smartphones, MP3 players, any other multi-function devices may be damaged if you try to encrypt them.

## HELPFUL CONTACTS

Contact	Service
<b>Service Desk</b> ext. 4357 (any site)	<ul style="list-style-type: none"> <li>• Setting up (mapping) personal and shared network drives.</li> <li>• Questions or problems using Winmagic encryption software.</li> <li>• Supporting remote access.</li> <li>• Deleting files or moving files from a device to a network drive.</li> </ul>
<b>Computer User Support Program (CUSP)</b> AskCUSP@uhn.on.ca	<ul style="list-style-type: none"> <li>• Training on creating folders, deleting files, and moving files from a device to a network drive.</li> <li>• Training on using webmail.</li> </ul>
<b>SIMS Education</b> 14-5091 simseducation@uhn.on.ca	<ul style="list-style-type: none"> <li>• Training on using webmail.</li> </ul>
<b>Information Security Office</b> iso@uhn.on.ca	<ul style="list-style-type: none"> <li>• Recommendations for protecting non-UHN devices.</li> </ul>
<b>Privacy Office</b> 14-6937 privacy@uhn.on.ca	<ul style="list-style-type: none"> <li>• Identifying files containing PHI.</li> <li>• Managing a device loss or theft.</li> </ul>

### Don't forget corporate confidential information!

Along with PHI, other types of business information including policies, procedures, financial information and intellectual property need to be protected to avoid damage to UHN or to specific individuals.

#### Examples...

- HR information (e.g. disciplinary actions)
- Data security plans
- Research activities



## PROTECTING MY DEVICE CHECKLIST

### To protect PHI I have:

- Deleted unnecessary files containing PHI.
- Saved PHI to the network – not to my device.
  - I de-identify PHI before copying it to my device.
  - I use an encrypted device if I need a copy of identifiable PHI.
- Encrypted USB keys and hard drives where I intend to save PHI.
- Chose 'strong' passwords' when setting up encryption on a USB or external hard drive.
- Locked up / handed off devices at the end of my shift.

### When outside the hospital I:

- Avoid working in public areas, whenever possible.
- Position myself away from people who could look over my shoulder or overhear my conversation.
- Remember to gather my devices and papers when leaving a public area (e.g. food court, public transportation).
- Never leave devices unattended when in public (e.g. at an appointment) or in transit (e.g. on public transit).
- When in transit, lock up devices where not visible (e.g. in the trunk of a car; place in a locked and unmarked carrying case).
- Safely store devices when at home (e.g. away from family and friends; in a locked drawer).

### For more information

Refer to the following policies:

- [Storage, Transport & Destruction of Confidential Information](#) policy
- [UHN Medical Record of Personal Health Information](#) policy
- [Management, Retention & Disposal of Administrative Records](#) policy
- [Appropriate Use of Technology](#) policy

or visit the [Privacy Office](#) intranet site for quick tips.