



| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 1 of 15 |

| | |
|------------------------------|---|
| Approval Date | <i>March 29, 2012.</i> |
| Revision Date | <i>January 5, 2021</i> |
| Approved by | <i>Andree Robichaud, CEO</i> |
| Approver Signature |  |
| Scheduled Review Date | <i>January 2024</i> |
| Cross- Reference | <i>1-30 E-MAIL</i> |

PURPOSE

To promote authorized collection, use, disclosure and management of email messages as government records of Central Health business and activities, in compliance with legislative requirements, records management standards and fair information practices.


To support authorized use of Central Health e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

SCOPE

This policy governs all Central Health employees and Affiliated Individuals, including all email messages generated, transmitted and/or received through Central Health approved email systems and defined as government records.

This policy governs all records of Central Health business activities generated, transmitted or received by Central Health employees or affiliated individuals regardless of the email system and includes email records of Central Health business and activities having lasting value and generated through personal email accounts.


This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 2 of 15 |

DEFINITIONS


| | |
|-------------------------------|---|
| Affiliated Individuals | Individuals who are not employed by Central Health, but perform specific tasks at or for the organization, including, but not limited to, trustees, students, volunteers, pastoral care, researchers, contractors, vendors and individuals working at the organization, but funded through an external source. |
| Business Information | Information with respect to Central Health's business that is not publicly disclosed by the organization. Employees / affiliates may come in contact with such information that is not generally known to the public as they perform their duties. Examples include, but are not limited to: <ul style="list-style-type: none"> • legal matters involving the organization that are not public knowledge; • financial information that is not available in Central Health's annual report; • contractual agreements with vendors, consultants, contractors, and third parties (The confidentiality of this information may be written into the contract, e.g. non- disclosure of the cost of the service); • information about intellectual property such as development of new technology and treatments or unpublished reports; and • information pertaining to Central Health's information technology access and security systems. |
| Email | Email is defined as messages, including attachments sent and received electronically between personal computers, devices or terminals linked by communications facilities. This includes address information (to, from, cc, bc, subject and date) the message content, and attachments. |
| Express Consent | Express consent is direct, explicit, and unequivocal and may be provided in orally or in writing. |

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 3 of 15 |


| | |
|------------------------------------|--|
| Government Record | <p>A record created by or received by a public body in the conduct of its affairs and includes a cabinet record, transitory record and/or an abandoned record.</p> |
| Personal Health Information | <p>Identifying information in oral or recorded form about an individual that relates to:</p> <ul style="list-style-type: none"> • the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family; • the provision of health care to the individual, including information respecting the person providing the health care; • the donation by an individual of a body part or any bodily substance, including information derived from the testing or examination of a body part or bodily substance; • registration information; • payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care; • an individual's entitlement to benefits under or participation in a health care program or service; • information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service; • a drug as defined in the <i>Pharmacy Act, 2012</i>, a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or the identity of a person's representative as defined in Section 7 of the <i>Personal Health Information Act</i>. |
| Personal Information | <p>Recorded information about an identifiable individual including:</p> <ul style="list-style-type: none"> • the individuals name, address, or telephone |

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 4 of 15 |

| | |
|-----------------------------|--|
| | <p>number;</p> <ul style="list-style-type: none"> • the individual’s race, national or ethnic origin, color, or religious or political beliefs or associations; • the individual’s age, sex, sexual orientation, marital status or family status; • an identifying number, symbol or other particular assigned to the individual; • the individual’s fingerprints, blood type or inheritable characteristics; • information about the individual’s health care status or history, including a physical or mental disability; • information about the individual’s educational, financial, criminal, or employment status or history; • the opinions of a person about the individual; and • the individual’s personal views or opinions, except where they are about someone else. |
| Record | <p>A correspondence, memorandum, form, paper, parchment, manuscript, map, plan, drawing, painting, print, photograph, magnetic tape, computer disc, microform, electronically produced document and other documentary material regardless of physical form or characteristic.</p> |
| Secure File Transfer | <p>An approved and secure information transmission protocol that provides file access, file transfer, and file management through use of cryptography for encryption of two data flows over the internet. Central Health has approved use of secure file transfer via <i>Liquid Files</i> for secure transmission of identifiable personal/personal health information.</p> |

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health’s Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 5 of 15 |

| | |
|--------------------------|--|
| Transitory Record | <p>A government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record. Transitory records can be securely destroyed when no longer of value without required authorization.</p> <p>Transitory records include:</p> <ul style="list-style-type: none"> • Copies of convenience or reference • Personal messages • Messages that convey a minor or administrative action • Messages that contain content encapsulated in another record |
|--------------------------|--|


POLICY STATEMENT(S)

All employees and affiliated individuals are responsible to protect the information they create, share, and maintain on behalf of Central Health, including email records. Safe practices must be adhered to when creating, sending, receiving, and storing e-mail either through the Central Health internal network, via Central Health Webmail, and/or through secure file transfer.

E-mail use at Central Health must comply with all applicable laws and Central Health policies. Email records created by, sent, received, or stored by Central Health employees and affiliated individuals in the conduct of its affairs constitute government records in the custody or control of Central Health and as such are governed by the *Access to Information and Protection of Privacy Act, 2015*.

Employees must be aware that they have no reasonable expectation of personal privacy in e-mail transmitted, received, and stored on and/or through Central Health's network. E-mail, whether created or received, is the property of Central Health and is not a private employee communication.

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 6 of 15 |

- I. Appropriate use**
- II. Inappropriate use**
- III. Use of email for communicating personal/personal health information**
- IV. Secure file transfer**
- V. Email as a government record**
- VI. Monitoring and retention of e-mail**
- VII. Responsible use**

I. Appropriate use

Email is a business tool which is approved for Central Health use to support collaboration, sharing of information and communication within and external to the organization.

Individuals at Central Health are encouraged to use e-mail to further the goals and objectives of Central Health. The types of activities that are encouraged include:


- Communicating with fellow employees, business partners of Central Health, and external stakeholders within the context of an individual's assigned responsibilities;
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities;
- Participating in educational or professional development activities;
- As otherwise authorized for use.

Central Health allows limited personal use for communication purposes, independent learning, public service, and other approved uses where it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources.

II. Inappropriate use

The following activities are deemed inappropriate uses of Central Health e-mail systems and services, and are strictly prohibited:

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 7 of 15 |


- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses);
- Use of e-mail in any way that violates Central Health’s policies, rules, or administrative directives;
- Central Health’s e-mail systems and services are not to be used for purposes that could be reasonably expected to strain storage or bandwidth;
- Viewing, copying, altering, or deletion of e-mail accounts or files belonging to Central Health or another individual without authorization;
- Opening e-mail attachments or hyperlinks from unknown or unsigned sources. Attachments are the primary source of computer viruses and must be treated with utmost caution;
- Sharing e-mail account passwords with another person or attempting to obtain another person’s e-mail account password. Central Health e-mail accounts are only to be used by the registered user;
- Excessive personal use of Central Health e-mail resources;
- Unsolicited mass mailings, non-Central Health commercial activity, political campaigning, dissemination of chain letters, and use by non-employees; and/or
- Use of Central Health e-mail systems to campaign to raise funds or generate personal revenue.

III. Use of email for communicating personal/personal health information

Central Health’s e-mail communication systems are primarily a business tool and are not intended for clinical use. Email communications must not contain identifiable personal health information, except by express consent from the individual who is the subject of the information, including though not limited to the Central Health Appointment Notification System [ANS].

Where email is used for clinical purposes by express consent of the client, the

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health’s Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 8 of 15 |

email address must be verified, and the client must be informed of possible risks related to email use.

Copies of the email and attachments containing personal health information and relevant to service provision of the client must be maintained in the client's legal record. The date, time, addressee of the email must be apparent, and the integrity of the original communication must be maintained.


The following requirements apply when sending personal/personal health information via email:

- Limit the amount of personal/personal health information being sent to only what is necessary;
- Ensure that no personal/personal health information is in the subject line of the email;
- Only place essential information in the body of the email;
- Personal health information must be sent as an encrypted attachment through secure file transfer;
- Whenever possible, reduce the amount of sensitive information in the body of the email. For example, rather than disclosing a patient's prognosis or diagnosis in an email, instead refer generally to the contents – "a test" or a "procedure" and ask the recipient to refer to the encrypted attachment for further information.

A right of access and correction of personal/personal health information applies to email communications in the custody or control of Central Health. Email records are also subject to professional practice standards. Email records are subject to an investigation by the Office of the Information and Privacy Commissioner [OIPC] or other investigative authority as authorized by law.

All breaches of confidentiality are treated as an occurrence in accordance with the Central Health Occurrence Reporting Policy and a CSRS occurrence report must be completed. Unauthorized sharing or disclosure of personal or personal health information via email is considered a privacy breach. [Privacy Breach Policy](#) (1-50) must be followed if a privacy breach occurs.

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 9 of 15 |

IV. Secure file transfer

Use of secure file transfer is required for transmission of personal/personal health information where express consent of the individual has not been obtained or the sensitivity of the information requires secure transmission of the information.

Central Health has an approved secure file transfer application for use for electronic transmission of confidential and/or sensitive information where a higher level of security is required, not afforded through the Central Health email system. (See Procedure section)

Records transmitted through secure file transfer constitute government records of Central Health. Secure File Transfer must not replace use of approved clinical documentation systems for communication of clinical information. Where secure file transfer is used for transmission of personal/personal health information concerning Central Health business activities, a record must be retained in the applicable information system (Meditech, CRMS, personnel file, etc.).

V. Email as a government record


Email is a government record when it is created or received in connection with the transaction of Central Health business (e.g. when it records official decisions; communicates decisions about policies, programs and program delivery; contains background information used to develop other Central Health documents; etc.). Government records exist in the custody or control of Central Health and as such must be retained in accordance with the applicable retention schedule as approved by law.

A transitory record is a government record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.

Transitory records include:

- Copies of convenience or reference;
- Personal messages; or

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 10 of 15 |

- Messages that convey a minor or administrative action.

Transitory records must be deleted and purged from Central Health electronic email folders or securely disposed of where they exist in paper copy once their temporary usefulness has been fulfilled. Where transitory records are retained, they are subject to the *Access to Information and Protection of Privacy Act, 2015* and may be compelled for disclosure.

It is an offense to destroy government records in any form, including transitory records after a request for access has been received by Central Health.

VI. Monitoring and retention of e-mail


The e-mail systems and services used at Central Health are owned by the organization and are therefore its property. This gives Central Health the right to monitor all e-mail traffic passing through its e-mail system. This monitoring may include, though is not limited to:

- inadvertent reading by designated IM&T staff during the normal course of supporting/ managing the e-mail systems;
- review by the legal team during the e-mail discovery phase of litigation, observation by management in cases of suspected abuse;
- observation by management in the employer's absence to ensure appropriate service to clients and review by the Privacy Officer during privacy and confidentiality investigations; and,
- as otherwise required by law.

Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

A public body that has custody or control of personal information that is the subject of a request for access to a record or correction of personal information shall retain that information for as long as necessary to allow the individual to exhaust any recourse that they may have with respect to the request.

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 11 of 15 |

VII. Responsible use

E-mail access at Central Health is controlled through individual accounts and passwords. Each user of Central Health’s e-mail systems is required to read and sign a copy of the [Network Access Request Form](#) prior to receiving an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.


Central Health delivers official communications via e-mail. Employees and affiliated individuals are expected to check their e-mail in a consistent and timely manner so that they are aware of important announcements and updates, as well as for fulfilling business and role-oriented tasks.

E-mail users are responsible for mailbox management, including organization and cleaning. All Central Health email users must:

- Verify the email address with the intended recipient(s) and re-check the email addresses, cc and bcc fields and attachments before sending;
- Ensure autocomplete or autofill options are turned off to avoid errors;
- Add a disclaimer to user signatures that indicates that the email is confidential and intended only for the intended recipient. It must also instruct anyone who receives the email in error to delete or shred the misdirected mail and notify the sender.
- Demonstrate care when using the “Reply All” and “Copy” command during e-mail correspondence to ensure the resulting message is not delivered to unintended recipients.
- Exercise caution when communicating personal, personal health and business information via e-mail. Do not communicate anything that you wouldn’t feel comfortable being made public.
- Email users must keep all login names and passwords confidential in order to protect the security of records. Any allegations of misuse must be promptly reported to the Central Health Helpdesk and privacy representative.

Prior to exit from Central Health, all Central Health email users must review all email folders and delete/purge transitory records and forward or retain

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health’s Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 12 of 15 |

government records to other record management systems to support availability and authorized access to records in the custody or control of Central Health.

When an employee is no longer affiliated with Central Health it is the responsibility of the People and Culture Department, in cooperation with the employee's immediate supervisor to notify the Central Health Helpdesk. This will ensure the termination of an employee's email account upon departure.

E-mail access will be terminated when the employee's or third party's association with Central Health is terminated, unless other arrangements are made. Central Health is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

Violations of this policy will be treated like other allegations of wrongdoing at Central Health. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of Central Health's e-mail systems and services may include, but are not limited to, one or more of the following:


1. Temporary or permanent revocation of e-mail access;
2. Disciplinary action according to applicable Central Health policies; and/or
3. Legal action according to applicable laws and contractual agreements.

PROCEDURE

For Use of Secure File Transfer

1. Where secure transmission of information is required, secure file transfer is accessed through the following link: <https://securefiles.centralhealth.nl.ca/>.
2. Enter your Central Health email address (firstname.lastname@centralhealth.nl.ca) and your Central Health network password.

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 13 of 15 |

Central Health Secure File Transfer



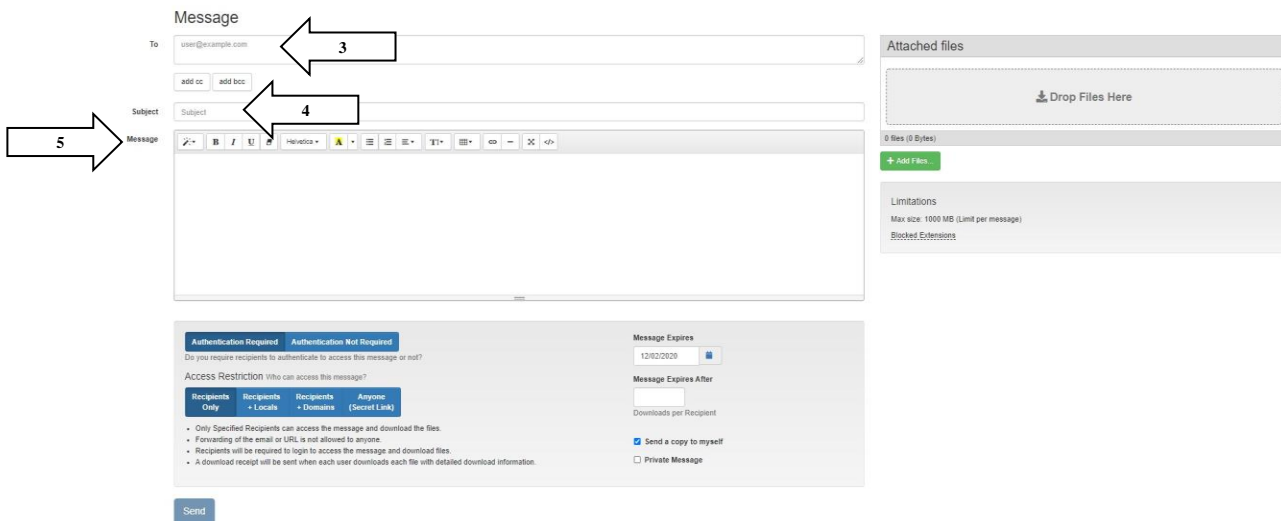
Central Health logo

2 → [Email] [Password] [Login]

Remember me for two weeks

[Password Reset]

3. Enter and verify recipient's email address.
4. Enter subject of secure file transfer.
5. Enter message in text box.



Message

To: user@example.com ← 3

add cc add bcc

Subject: Subject ← 4

Message ← 5

Attached files

Drop Files Here

0 files (0 Bytes)

+ Add Files

Limitations

Max size: 1000 MB (Limit per message)

Blocked Extensions

Authentication Required Authentication Not Required

Do you require recipients to authenticate to access this message or not?

ACCESS RESTRICTION Who can access this message?

Recipients Only Recipients + Locals Recipients + Domains Anyone (Secret Link)

- Only Specified Recipients can access the message and download the files.
- Forwarding of the email or URL is not allowed to anyone.
- Recipients will be required to login to access the message and download files.
- A download receipt will be sent when each user downloads each file with detailed download information.

Message Expires: 12/02/2020

Message Expires After: []

Downloads per Recipient: []


Send a copy to myself

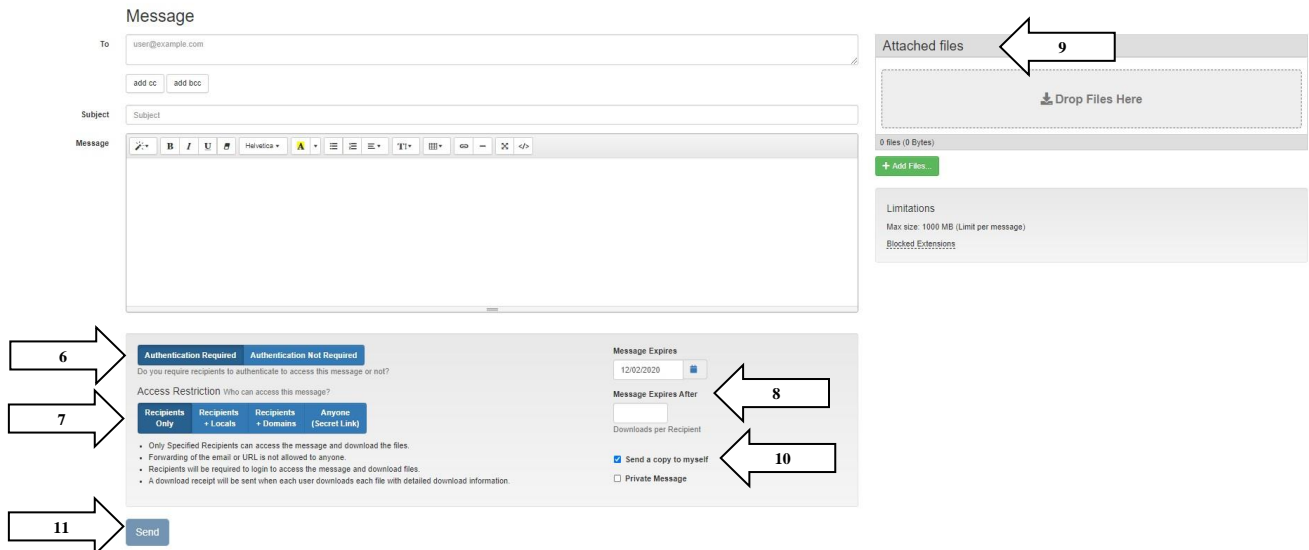
Private Message

Send

6. Always select *Authentication Required* to ensure secure access to the message/attached file(s).
7. Restrict access to recipients only.
8. Allow one download per recipient and limit the time period allowed for download of confidential information to the minimal time period required for retrieval.
9. Attach any documents requiring transfer through secure file transfer.
10. Click "send a copy to myself" and "private message".
11. Click send.

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: | Policy Number: IPR-0004 |
| | E-MAIL | |
| | Policy | Policy Level: Level I |
| | Accountability: | Page 14 of 15 |
| | Information, Privacy and Regulatory Oversight | |



12. Secure file transfer will provide email confirmation of receipt of information by the recipient.

REFERENCES


Access to Information and Protection of Information Act, Statutes of Newfoundland and Labrador (2015, c. A-1.2). Retrieved from the House of Assembly Newfoundland and Labrador website:
<http://www.assembly.nl.ca/Legislation/sr/statutes/a01-2.htm>

Canadian Medical Protective Association. (October 2013). Using electronic communications, protecting privacy. Retrieved from: <https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2013/using-electronic-communications-protecting-privacy>

Management of Information Act, SNL M-1.01. (2005). Statutes of Newfoundland and Labrador. Retrieved from:
<https://www.assembly.nl.ca/Legislation/sr/statutes/m01-01.htm>

Office of the Chief Information Officer. (2009). Government of Newfoundland and

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.

| | | |
|---|--|--------------------------------|
|  | TITLE OF THE POLICY: E-MAIL | Policy Number: IPR-0004 |
| | Policy | Policy Level: Level I |
| | Accountability: Information, Privacy and Regulatory Oversight | Page 15 of 15 |

Labrador Email Policy. Retrieved from:
<https://www.gov.nl.ca/exec/ocio/files/publications-policies-email-policy.pdf>

Office of the Chief Information Officer. (2016). Use of Non-Government Email Accounts. Retrieved from: <https://www.gov.nl.ca/exec/ocio/files/im-employees-non-government-email-directive.pdf>

Office of the Information and Privacy Commissioner for Newfoundland and Labrador. (2018, February 26). OIPC Use of Email for Communicating Personal Health Information. Retrieved from <https://www.oipc.nl.ca/pdfs/UseOfEmailForCommunicatingPersonalHealthInformation.pdf>

Office of the Information and Privacy Commissioner for Newfoundland and Labrador. (2018, February 26). Use of Personal Email Accounts for Public Body Business. Retrieved from <https://www.oipc.nl.ca/pdfs/Use-of-Personal-Email-Accounts-for-Public-Business.pdf>

Personal Health Information Act, Statutes of Newfoundland and Labrador (2008, c. P-7.01). Retrieved from the House of Assembly Newfoundland and Labrador website: <http://assembly.nl.ca/legislation/sr/statutes/p07-01.htm>

RESOURCES

[OCIO, Information Protection: Safe E-mail Practices](#)
[OIPC, Use of Email for Communicating Personal Health Information](#)
[OIPC, Use of Personal Email Accounts for Public Body Business](#)
[CMPA, Using Electronic Communications, Protecting Privacy](#)

This is a controlled document. Printed copies of this document are not controlled. Users must view the electronic version of this policy located on Central Health's Intranet to ensure the most up to date policy is consulted.