University of Alberta – Privacy and Security Best Practices

Security and Privacy of Email

Email is one of the most commonly used methods to send information on campus, perhaps the most common method.

The University attempts to provide secure, private and reliable email services by following sound information technology practices and due diligence, whether provided in-house or through an external service provider. However, the University cannot guarantee the security, privacy or reliability of its email services. All email users, therefore, should exercise caution in using email to communicate confidential or sensitive matters.

The University has created these best practices to help address questions related to secure information exchange. You may have other requirements to consider as well, such as faculty or department policies and procedures, Research Ethics Board requirements, and external stakeholder stipulations.

General Principles

1) Highly sensitive personal information (as defined below) should not be transmitted by email. It is also prudent to avoid sending birth dates by email if possible.

2) As a common alternative to email, uAlberta Google Docs is approved for use involving information that includes the University’s business, academic, research, and administrative information and records. Be conscientious and careful about who you share and grant document access to.

3) Identifiable health and patient records are not within the scope of approved uses for uAlberta Gmail or Google Apps/Docs.

For a quick summary of recommended guidelines, please see the summary table on page 4 of this document. If you would like more information on “why” and “how”, please keep reading!

Risks of Using Email

Email has many benefits. It is generally quick, convenient and easy to use. It is easy to send a communication to one person or many people. It is easy to forward information you have received. However, it also carries some risks, such as:

- **Misdirection** – one of the most common causes of privacy breaches is misdirected emails. This happens when two people have similar email addresses, and you send an email containing personal information to the wrong person. You can find more information on how to minimize this risk at:
Email Privacy and Security Best Practices

February 2016


- **Interception** – email travels through various nodes and hubs across the Internet backbone. As it does so, there are points where it may be accessible by hackers, or by government surveillance programs.

One of the fundamental tools used by email systems to prevent this type of interception is encryption. An email sent from one Gmail account to another is encrypted in transit – it is sent through an encrypted “tunnel”. Other internet transactions requiring a high degree of security, such as online banking, also use this type of transmission security. An email sent to/from aUAlberta.ca account from/to a different type of email provider may or may not be sent through an encrypted “tunnel”.

The University does have contractual safeguards against improper use of University emails by Google, but it is important to know that Google has the means to access the emails and may be bound to follow laws in its jurisdiction relating to disclosure of information to a government for security purposes.

Therefore, while email transmission security is useful, it does not prevent inappropriate and unauthorized disclosures to law enforcement and government bodies.

- **Handling by recipient** - You generally have no control over how the person receiving your email could be handling it. The fact that email can be easily copied, blind copied and forwarded to other email addresses is convenient, but this can also create risks, when the information is of such a nature that it should not be widely shared.

If the email address is a person’s home email address, family members may also have access to the contents of the email account.

There is also a risk in the way that the recipient stores your email. The person could be making multiple copies and saving them to insecure devices, like laptops, public desktop computers, or memory sticks. If an intruder happened to get access to one of those insecure devices they would also have access to all of the emails you had sent that person.

- **Possible vulnerabilities within an email account** – Examples include:

  - A weak email account password could leave personal information and confidential business information in the account vulnerable.
  
  - Email phishing scams (emails which appear to be sent from organizations or people that the recipient trusts) can trick the recipient into opening attachments, clicking on a link, or providing credentials, that allow someone to gain access to information within the email account.

For a further discussion about the risks of using email in the context of sending patient information, please see the following OIPC Practice Note:

**OIPC Practice Note**
It is important to consider these risks when considering whether to send information to someone by way of email.

**Personal Information – What is “Highly Sensitive” and What is “Moderately Sensitive”?**

As a general rule, highly sensitive personal information should not be sent by email. It is also prudent to avoid sending birth dates by email, if possible. To comply with privacy legislation, the University needs to have greater safeguards over personal information that is highly sensitive than it does over personal information that is less sensitive.

So, what is highly sensitive personal information?

University data can generally be assigned to one of four categories, which are described in Appendix A. You can see that information falling within the first 2 categories is considered highly sensitive.

Data that falls within the 3rd category is considered to be moderately sensitive.

The sensitivity of a particular piece of personal information can vary with context. For example, a person’s home contact information can be highly sensitive if that person is being stalked. As well, remember that if you are transmitting a high volume of personal information, the risks are greater than if you are transmitting the personal information of a very limited number of individuals.

**What is Confidential Information?**

You may also hear the term “confidential information” sometimes. Data that falls within the categories of “Restricted”, “Confidential” or “Protected” in Appendix A may be considered confidential information. Be sure to familiarize yourself with the expectations within your faculty of unit, and the requirements of other organizations whose information you handle.

**Guidelines Regarding How to Send Personal Information In the Custody or Control of the University**

The University has an obligation to make reasonable safeguards to protect personal information that it holds. In general, the higher the sensitivity of the information, the greater the safeguards should be.

When considering how to send personal information that is highly sensitive or moderately sensitive to another person, University employees should consider the risks of email described above, and should take precautions proportionate to the risk level described in Appendix A.

That being said, because of the risks described above, the University’s Information and Privacy Office and Chief Information Security Officer generally recommend that highly sensitive personal information should not be sent via email (unless contained in an encrypted attachment). It is also prudent to avoid sending birth dates by email if possible. While birth dates are generally considered to be “moderately” sensitive, they are often used by organizations to authenticate identity, and can be particularly useful for identity theft purposes.
For a summary of guidelines regarding whether to use email or an alternative method when sending personal or confidential information, please see the summary table below.

### Summary Table of Guidelines

<table>
<thead>
<tr>
<th>highly sensitive - medical records</th>
<th>highly sensitive - credit card numbers and social insurance numbers</th>
<th>highly sensitive, other than records listed above – incl. personnel files, salary, discipline records, information related to a law enforcement investigation, 3rd party business information submitted in confidence</th>
<th>date of birth</th>
<th>other moderately sensitive info – grades, ccids, employee id #s and student #s, and personal contact information other than publicly displayed university email addresses</th>
<th>non-sensitive info – publicly displayed university email addresses, accounting chart of accounts, anything available on the university’s website</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>google drive</td>
<td>encrypted attachment or shared network site</td>
<td>secure fax</td>
<td>non-electronic methods</td>
<td>email</td>
</tr>
<tr>
<td>N¹</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

¹ For more detail, please see the OIPC Practice Note referenced on page 2 of this document.
Alternatives to Email/Enhancement to Email Security

What other options are available for sending personal information or confidential information?

1) **Encrypted Attachment** - One way to reduce many of the email risks identified above is to put the personal or confidential information in an encrypted attachment. Documents created using current versions of Microsoft Office and Adobe Acrobat can be encrypted with a fairly quick process. For more details, please see:


   When you encrypt the document, you will need to choose a password to be used for decrypting the document. The password should be shared with the recipient over the phone, or through another method that does not involve email. You should choose a strong password. Tips for choosing a strong password can be found at: https://myccid.ualberta.ca/help/password-tips.

   If you do this, we recommend that you consider the risks of losing the password on your end, and being denied access to the document yourself. You might address this by making a copy of the document and only encrypting the copy.

2) **uAlberta Google Drive, including Google Docs** – this is a better option than email for sharing sensitive personal information or confidential information. The Information and Privacy Office and the Chief Information Security Officer have assessed uAlberta Google docs through a Privacy Impact Assessment and Security Review, and have found that it has adequate privacy and security controls.

   Collaborative sessions on Google Drive only include those participants granted access by the document owner, if you have set your settings accordingly (please ensure that you educate yourself about the different settings available for sharing a document with others). If you mistakenly share a Google Doc with someone, you can immediately remove that person’s ability to access the Google Doc.

   Please note that Google Docs should only be used to share information and not to store it. Information in Google Docs should be saved to a hard drive and removed from Google Docs as soon as is reasonably possible. When you share a document using Google Docs, it is a good practice to tell people the period of time the document will be available on Google Docs (e.g. one week) before you will remove it.

   **Note:** Because health information including patient information was outside of the scope of the Privacy Impact Assessment conducted by the University for Google, and because there may be additional measures and controls required for health and patient information, these information types are currently not in scope for approved uses of uAlberta Gmail or Google Docs.

3) **Shared network drive** – If you wish to share a document containing personal information with a colleague in your office, consider whether you can save the personal information to a shared drive on
your faculty, department or unit network. Then, simply email or tell your colleague the location in which you saved the document.

4) Fax – while faxing documents involves its own set of risks, this tends to be considered a more acceptable practice within the medical community than email. When faxing personal or confidential information, it is prudent to follow the guidelines set out in this publication:

OIPC Guidelines on Facsimile Transmission

5) Non-Electronic Methods – sometimes it will be most appropriate to use traditional methods of exchanging information, such as mail, courier, campus mail, hand delivery, or a phone call.

For University policies and procedures regarding email use, and further resource materials, please see the next page.
Policies and Procedures Regarding Email Use

Information Technology Use and Management Policy:

Information Technology Security Policy:

Email Forwarding Restriction Procedure:
https://policiesonline.ualberta.ca/PoliciesProcedures/Procedures/Email-Forwarding-Restriction-Procedure.pdf

Resources Regarding Email Use

OIPC HIA Practice Note #5 - Communicating with patients via email: Know the risks

OIPC Practice Note

Preventing and avoiding Identify Theft:

The Get Cyber Safe site by the Government of Canada, specifically the Protect Yourself page:

The Identity Theft site by the Government of Alberta:
http://www.servicealberta.gov.ab.ca/560.cfm

Changing you Campus Computing ID Password, and in particular the Tips on choosing a new, secure password section provides guidance on strong password selection:
https://password.srv.ualberta.ca/passwords.html
APPENDIX A

4 Categories of Data Classification

Restricted / Highly Sensitive - This classification is for information that is extremely sensitive and could cause extreme damage to the integrity, image or effective service delivery of the University of Alberta. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. Restricted information is available only to named individuals or specified positions. (Examples include restricted spaces, credit card numbers, social insurance numbers, and personal medical records).

Confidential / Highly Sensitive - This is for information that is sensitive within the University of Alberta and could cause serious loss of privacy, competitive advantage, loss of confidence in University programs, or damage to partnership, relationships and/or reputation. Confidential information includes highly sensitive personal information. Confidential information is available only to a specific function, group or role. (Examples include personnel files, including personal salary data, discipline files, information related to a law enforcement investigation, and 3rd party business information submitted in confidence).

Protected / Moderately Sensitive - This is for information that is moderately sensitive within or outside the University of Alberta and could impact service levels or performance, or result in low to medium levels of financial loss to individuals or enterprises, loss of privacy, loss of confidence in University programs, or damage to partnerships, relationships and/or reputation. Protected information includes personal information, and financial information or details concerning the effective operation of the University of Alberta. Protected information is available to employees and authorized non-employees (contractors, sub-contractors and agents) possessing a need to know for business-related purpose. (Examples include grades, dates of birth, CCIDs, employee IDs and student IDs, and personal contact information other than publicly available University email addresses).

Unrestricted / Not Sensitive - This is for information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information includes information deemed public by legislation or through routine disclosure or active dissemination. Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the University. Or, where the information has not been made available to the public, if it were, it would not have any harmful or negative effect. (Examples include university email addresses, accounting chart of accounts, and anything available on the University's website).