Ontario Psychological Association

Guidelines for Best Practices in Electronic Communications

OPA Communications and Member Services Committee

February 2015

ONTARIO PSYCHOLOGICAL ASSOCIATION

Table of Contents

Acknowledgement

The OPA Communications and Member Services Committee would like to acknowledge with thanks the contributions of Drs. Amber Smith and Jane Storrie in the development of this Guidelines document.

Preamble

Technology has been changing communication between psychological service providers and patients, referral sources, other healthcare providers and third-party payers. Members may be aware of websites, applications, and email communication tools that can be used to improve the delivery of patient care. Many of us use email extensively because it is fast, reliable, and convenient. These same characteristics, however, bring legal and liability risks, including a higher potential for privacy breaches.

As regulated health professionals, we have an obligation to maintain the confidentiality of our patients' personal health information (PHI) and to comply with privacy regulations (see Appendix A). Members need to consider how to communicate with and about patients while still protecting patient privacy. While email is fast and convenient, it also is often the least secure and the least private way to communicate.

We are aware that many larger healthcare and academic settings now have policies stating that email should not be used to transmit any PHI. We are also aware that general guidelines for use of email suggest that it is not a secure form of communication for any personal information. Most guidelines for general email use suggest that information that is sensitive, confidential, potentially embarrassing, proprietary, personal, or classified should never be sent through email.

While members practicing within healthcare and academic settings may be familiar with their institution's policies, those in community-based practice may not be as familiar with regulations and expectations regarding electronic communication. To clarify the responsibilities of members, the Ontario Psychological Association's Communication and Member Services Committee is providing the following Guidelines for Best Practices in Electronic Communications.

General Information

- Email is not guaranteed to be private.
- Email is not an appropriate substitute for face-to-face clinical assessment and treatment.
- Email is not always sent and received instantly; messages can arrive several hours or days after they are sent. As a result, email is not an appropriate method for exchanging time-sensitive information.
- Emails are considered to be records. Therefore, they should be retained in the same way in a patient's clinical file as are records of other forms of communication, such as letters, faxes, and phone calls.
- Members should be aware that there is a possibility that emails related to a patient's health care can be disclosed in response to an access request.
- Privacy legislation generally requires that custodians adopt safeguards to protect the personal health information under their control. Despite the typical disclaimer seen at the bottom of some emails, health care providers remain responsible for protecting their patients' health information and the disclaimer is likely not sufficient for avoiding liability in the event of a privacy breach.

- The Information and Privacy Commissioner of Ontario (IPCO) has indicated the use of unencrypted email and messaging to communicate personal health information should be avoided.
- The IPCO has indicated that even when patients state that they are willing to accept the risk of unauthorized access or disclosure of their PHI, and have provided informed consent to communicate by email, it is still the health care provider's responsibility to safeguard the PHI that is in your custody.
- Members who communicate via email or web portals need to be mindful that they are governed by the same legal and professional standards as would apply in other professional settings (e.g. a hospital, family practice, or clinic).
- All PHI is covered under the same privacy legislation, regardless of whether it is contained in an email or some other format. As a result, confidentiality and privacy are important to consider if email is being used to communicate PHI to recipients who are not part of a secure internal network.
- Be aware that when using an employer's or a third party's email system (e.g. hospitals and clinics), these parties may have the right to access the email communications. If the third party is subject to federal or provincial privacy legislation, emails sent from the third party's computer system may also be at risk of being disclosed in the context of an access request, or privacy commissioner or College investigation. They may also be subject to disclosure in the context of litigation.

Risks of Using Email

Risks associated to using email include, but are not limited to:

- The privacy and security of email communication cannot be guaranteed.
- It is impossible to verify the true identity of the sender and guarantee that only the intended recipient will read the email once it has been sent.
- Emails can introduce viruses that damage or disrupt a computer or system.
- Email messages can be modified, forwarded, intercepted and shared, without your knowledge or permission, making it particularly vulnerable to fraud, privacy breaches, and unintended disclosures to third parties.
- The risks of interceptions or errors in sending email or text messages can be significant.
- Email messages are permanent. Even after deleting copies of the email, back-up copies may exist on a computer, with an Internet Service Provider (ISP), on a server in another country, or elsewhere in cyberspace.
- Your employer may have a legal right to inspect and keep emails that pass through their system if you use a work computer or mobile phone for communicating with patients.
- Email messages may be subject to access requests and used as evidence in a court of law.

Use of Smartphones and Other Mobile Devices

Advancements in technology are prompting many healthcare providers to communicate via mobile device. We are aware that use of mobile devices such as smartphones and tablets can improve communication and provide quick, easy access information, but they also increase the risk of a privacy breach. To that end:

- Exercise caution when using mobile devices to communicate in public places, as others may eavesdrop or be able to see these communications. Further, mobile devices can be lost or stolen.
- Ensure that PHI stored on mobile devices is encrypted.
- Unless you have specific security features, messages from most mobile devices should be avoided since they are more vulnerable to interception.

Guidelines

Email

Keep separate work and personal email addresses. If you need to use email to communicate sensitive personal information, consider using a personal email account accessed from a computer you control rather than your work email, an account that is accessed from your place of employment, or a computer that is shared with others.

PHI should not be transmitted via email without appropriate safeguards such as encryption or transmission within a secured, firewalled environment.

Emails sent between accounts within private, secured network environments are relatively secure, if they are protected by appropriate firewalls and virus protection.

Transmission of information by email from private, firewalled networks to external addresses usually is not confidential or secure. Email transmission outside firewalled environments is open and available to others to intercept. Members are advised to exercise extreme caution when emailing personal information (and other information of a confidential or sensitive nature) to outside email addresses, and to do so only if the information is encrypted in compliance with the Information and Privacy Commissioner's recommendations for secure encryption.

Members should inform patients of the risks if they plan to communicate PHI by email outside a secure internal network.

Check email addresses carefully before sending any information, and confirm that the intended recipient is authorized to receive the information and is the only one with access to the email address.

If communicating PHI, do so in an encrypted attachment rather than in the body of an email.

Members should limit distribution of emails with patient information to individuals who are on a "need to know" basis, or within the patient's circle of care.

Use patient initials or ID numbers to de-identify patient information in all un-protected email communications.

Use common language. Avoid using acronyms and medical terms that can be misunderstood.

Ensure your consultants, referral sources, and employees are informed of the risks associated with inappropriate email communication.

Messages received from or about the patient containing any details related to diagnosis or treatment should be printed in full and made part of their health record.

Members should not forward emails from patients to third parties without the patient's prior written consent, except as authorized or required by law.

Web-Based Email Services

Avoid using web-based email services (Gmail, Hotmail, etc.) for communication of PHI and other sensitive work matters. In general, these services are less secure and more vulnerable; they do not provide the kind of security features needed to be appropriate for transmission of sensitive information. If you intend to use email to communicate PHI about patients, use a dedicated and firewalled internal email system.

Security

Privacy regulators agree that the use of encryption software to protect electronic messages is a reasonable safeguard. PHI should not be transmitted via email without appropriate safeguards such as encryption or transmission within a secured, firewalled environment.

Keep your security systems, firewalls, filters, and virus protection software up-to date. Even within a secure internal network, special software may be needed to protect the server and all devices connected to a network (e.g. desktop computers, laptops, smartphones, etc.) if you intend to use them all in a connected, protected way to communicate PHI seamlessly.

Informed Consent

Patients should be informed about the risks of using email, and their agreement and the discussion should be documented in the record. Informed consent to electronic communication should be obtained and documented, either through a notation in the patient's health record or by a signed consent form or terms of use agreement, and include information about who will have access to emails, how they are processed, who will reply, and when and how any reply can be expected.

Members should consider using a written consent form to document the patient's consent to using email communication and to acknowledge the associated risks. Ensuring you use such a form could decrease the risk that the patient might make a complaint or bring an action for breach of confidentiality or invasion of privacy.

IT Services

If you are responsible for your own IT services, obtain an agreement in writing from your IT service provider that your email system meets regulatory requirements for transmission of PHI.

Digital Privacy Act

The Federal ***Digital Privacy Act***, known as Bill S-4, became law on 18 June 2015. This Act amends the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and underscores the necessity of having top-notch security for all digital and electronic information.

There are several sections which may impact psychological practice:

Mandatory Notification Provisions for Breaches of Security Safeguards
There is a requirement to provide notification of any breach of security safeguards involving personal information which creates a real risk of significant harm to an individual.

Breaches are broadly defined to include any loss of, unauthorized access to, or unauthorized disclosure of personal information. This expressly includes both failures of existing security safeguards and failure to establish adequate safeguards in the first place.

In the event of a breach, organizations would have to conduct a risk assessment of the likelihood of "*significant harm*", which is an open concept defined to include *"bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property".*

If a risk of significant harm is identified, the breach must be reported to both the Privacy Commissioner and the individual(s) at risk.

Required reports must be provided "*as soon as feasible*" upon learning of the breach unless there is a request from law enforcement to delay notification to protect a criminal investigation relating to the breach. Failure to provide the required reports or to keep the required records would be an offence subject to fines of up to $100,000 per affected individual.

Records of Breaches of Security Safeguards
Whether or not any notification is necessary, organizations would be required to keep records of all security breaches involving personal information. The Privacy Commissioner retains the right to request and review these records at any time.

Valid Consent for the Collection of Personal Information
According to the *Act*, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. We believe that members already meet this requirement under the College of Psychologists of Ontario's Standards of Professional Conduct.

It should be noted, however, that the Act states that an organization may disclose personal information without the knowledge and consent of the individual if the disclosure is made to another "*organization, the government institution or the part of a government institution that was notified of the breach under subsection*" and if the disclosure "*is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm*". We believe that we would still need to obtain informed consent to meet the requirements of the College's Standards.

Resources

Using Email Communication With Your Patients: Legal Risks (Canadian Medical Protective Society)
http://www.hamiltonfht.ca/docs/public/using-email-communication-with-your-patients-legal-risks

Mobile Devices in the Workplace and the Legal Risks of Email (Canadian Nurses Protective Society)
http://www.cnps.ca/upload-files/pdf_english/email1.pdf

Communicating with Clients via Email (College of Dietitians)
http://www.collegeofdietitians.org/Resources/Document-Type/E-Learning-Modules/Member-Learnign-Modules/Communicating-with-Clients-Via-Email/Communicating-with-Clients-via-Email.aspx

Psychotherapy Documentation and Communication Guidelines (University of Toronto)
http://psychiatry.utoronto.ca/wp-content/uploads/2011/01/Psychotherapy-Charting-and-Communication-March-26-2013-Pfn.pdf

Medical Records Policy (College of Physicians and Surgeons of Ontario)
http://www.cpso.on.ca/policies-publications/policy/medical-records

Email Use Best Practices (University of Alberta)
http://www.vpit.ualberta.ca/encryption/docs/Email%20Best%20Practices-Jan-2012.pdf

Privacy Fact Sheet: Privacy of Email Systems (UBC Office of the University Counsel Access and Privacy Manager)
http://universitycounsel.ubc.ca/files/2012/11/Fact-Sheet-Privacy-of-Email-Systems.pdf

Email and Text Messaging (Interior Health)
http://www.interiorhealth.ca/AboutUs/Policies/Documents/Email%20and%20Text%20Messaging.pdf

Security and Storage of Personal Health Information (Winnipeg Regional Health Authority Policy)
http://www.wrha.mb.ca/about/policy/files/10.40.120.pdf

Help Desk Support (London Health Sciences Centre/ St. Joseph's Health Care)

https://www.londonhospitals.ca/departments/medical_affairs/post_grad/documents/HelpDeskSupport.pdf

Tips & Best Practices: Email Management System (University of Ottawa)
http://www.ccs.uottawa.ca/email/overview.html#tips

IPC Fact Sheet- Health Care Requirement for Strong Encryption. 2010.
https://www.ipc.on.ca/images/Resources/fact-16-e.pdf

IPC Fact Sheet- Safeguarding PHI
https://www.ipc.on.ca/images/Resources/fact-01-e.pdf

IPC Fact Sheet- Encrypting Personal Health Information on Mobile Devices
https://www.ipc.on.ca/images/Resources/up-fact_12e.pdf

IPC Fact Sheet- Wireless Communication Technologies: Safeguarding Privacy and Security
https://www.ipc.on.ca/images/Resources/up-1fact_14_e.pdf

IPC Fact Sheet- The Secure Transfer of PHI
https://www.ipc.on.ca/images/Resources/fact-18-e.pdf

Appendix A—Privacy Legislation

Federal Privacy Legislation

Privacy Act, 1985
http://laws-lois.justice.gc.ca/eng/acts/P-21/

Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA)
http://laws-lois.justice.gc.ca/eng/acts/p-8.6/

Provincial Privacy Legislation

Freedom of Information and Protection of Privacy Act, 1990
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm

Personal Health Information Protection Act, 2004
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm