

# An encrypted e-mail application for paediatric and adolescent mental health teleconsultations

Liam Caffery<sup>1</sup>, Stephen Stathis<sup>2</sup> and Anthony C Smith<sup>1</sup>

<sup>1</sup> Centre for Online Health, University of Queensland, Brisbane, Australia

<sup>2</sup> Child and Youth Mental Health Services, Royal Children's Hospital, University of Queensland, Brisbane, Australia

## Abstract

We have developed an encrypted web-based e-mail application for the purpose of paediatric and adolescent telepsychiatric consultations. Open source libraries from OpenSSL were used for the development of our system. Our web-based architecture forced all communication between psychiatrist and patient to be encrypted using Secure Socket Layer or Transport Layer Security. The use of encrypted e-mail is an administrative recommendation of the Information Security Standard for the state health department. Our system was implemented for use by Child and Youth Mental Health Services in October 2005. During the first 13 months, between October 2005 and November 2006, 140 teleconsultations were performed via encrypted e-mail. Many of the patients lived in regional and remote areas of Queensland. We have found that e-mail teleconsultations are most useful as an adjunct to face-to-face consultations for these patients. We suspect from early experience that the e-mail service has allowed more consistent therapeutic contact with patients, resulting in positive patient outcomes. This case report demonstrates that e-mail-based telepsychiatry has both a place in under-served regional communities and for patients undergoing therapy, regardless of their geographical location.

**Keywords:** E-mail, email, psychiatry, adolescent psychiatry, child psychiatry, telemedicine

## 1. Introduction

In Queensland, public mental health services are provided to paediatric and adolescent patients in rural and remote areas by staff from the Child and Youth Mental Health Service (CYMHS). CYMHS is a statewide service with tertiary facilities located in Brisbane, the capital city of Queensland. Specialists based in Brisbane support peripheral centres located in regional and remote areas of the state in a number of ways. Some specialists travel to selected sites throughout the state to see patients during routine outreach clinics. In addition, specialists may offer

telepaediatric services which allow consultations and case discussions to be done via videoconference [1].

Telepsychiatry, via e-mail, has the potential for increasing therapeutic contact [2] and has been shown by a number of studies to be effective in the treatment of mental health disorders, for example, anorexia nervosa [3], bulimia nervosa [4] and behavioural weight loss [5]. Patients have reported high levels of satisfaction when they use e-mail to communicate with their doctor, and both patients and doctors have found it to be a convenient form of communication [6].

E-mail programs used for personal communication, depending on the

technology, may be inappropriate for psychiatric teleconsultations because they lack encryption. Encryption helps safeguard against unauthorised interception and tampering of e-mail messages. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) legislated against the transmission of unencrypted patient identifiable health information via e-mail [7]. The use of encrypted e-mail is not legislated in Queensland; but there is an ethical priority from many clinicians to do so, particularly in mental health [8]. There is also an administrative standard, *IS42A Information Privacy for Queensland Department of Health*

[9], that warns against communicating confidential information over public networks, like the Internet, unless an appropriate encryption process is in place.

To meet these considerations, we have developed a secure method for Internet communication to allow patients in regional areas online

access to psychiatric services. The resultant system is a web-based electronic mail application where the user logs onto a password-protected web-page to compose or read an electronic message. Figure 1 and Figure 2 are screenshots of these web-pages. In this system, all Internet communication uses Hypertext Transfer Protocol

over Secure Socket Layer (HTTPS). HTTPS uses public key certificates to provide encrypted communication for data transfers. By design, HTTPS will prevent unauthorised reading of Internet messages and also reduce the risk of tampering of the message by use of digital signature technology.

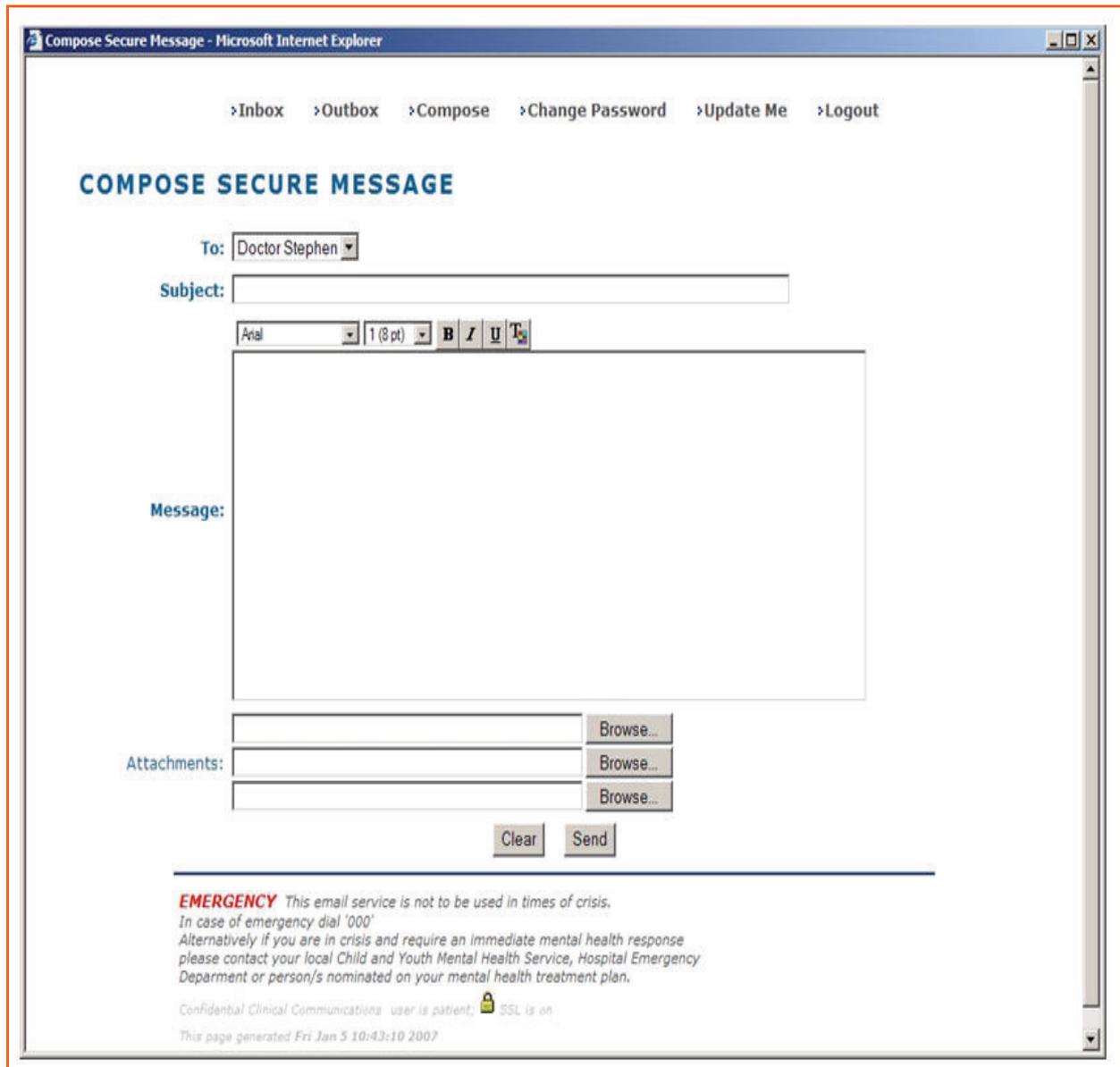


Figure 1: Screen shot of web-page where user composes e-mail message

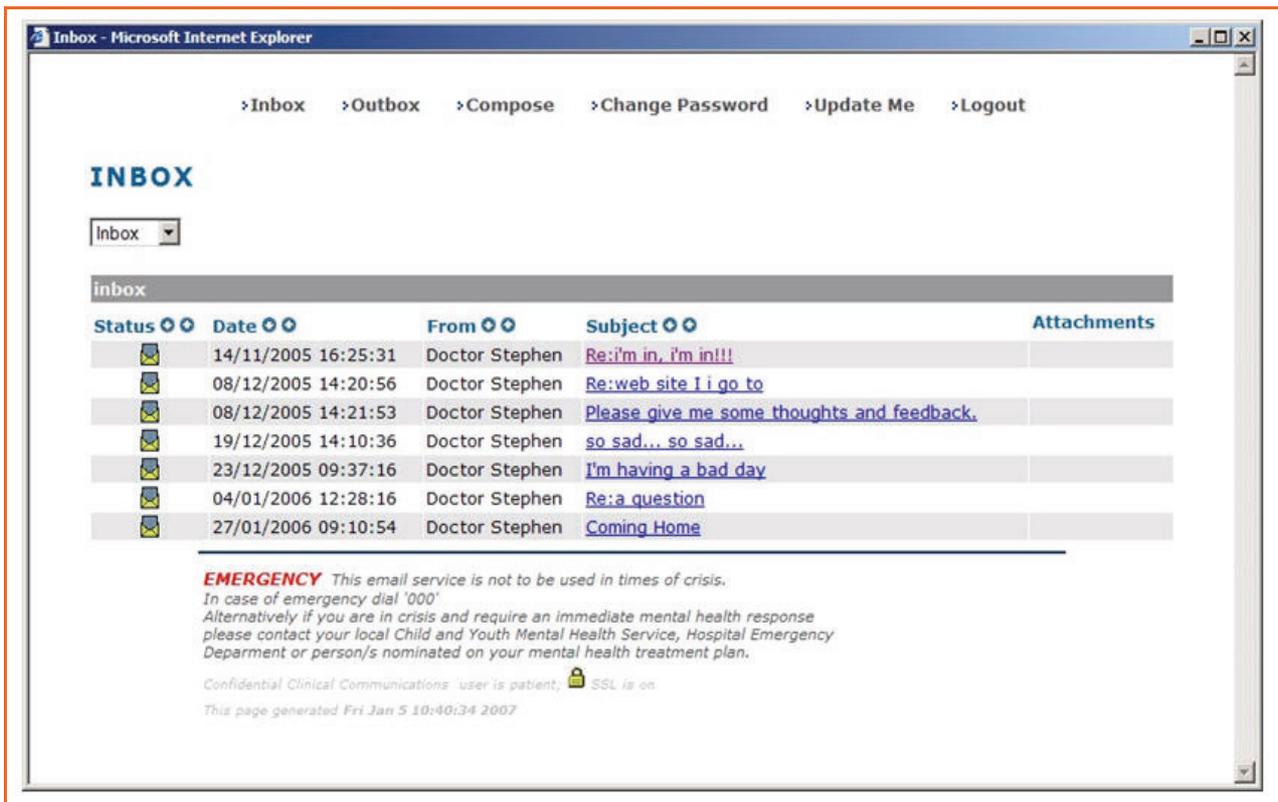


Figure 2: Screen shot of user's web-mail inbox

Encryption techniques address confidentiality issues but ultimately the security of a system can be compromised in multiple ways. For this reason we built into our web-mail application a number of security and privacy mechanisms.

## 2. Methods and Materials

Secure e-mail can be implemented by most commercial e-mail software. These applications use Secure Multi-part Internet Mail Extensions (S/MIME) protocols. They require both the sender and the receiver to install digital certificates to encrypt and decrypt communication. This has a number of shortcomings when trying to implement a paediatric telepsychiatry service. Primarily, the installation of certificates requires some technical knowledge. Difficulties in client setup may exclude some clients without the requisite technical ability, or may result in e-mails being unable to be read if the setup is incorrect. This

method also requires e-mails to be sent from computers where the certificates are installed.

### 2.1. System Architecture

To obviate the need for users to install digital certificates into their e-mail program, encryption can be implemented at a server level by using a web-based e-mail application. The web-pages that are the user-interface run off a secure web server and we developed them as a common gateway interface (CGI) script written in the Perl programming language. Users are compelled to use encryption using this architecture and, because the certificates are stored centrally, there is increased portability of access, consistent with child and youth computer usage culture.

We used the Apache Web Server [10] and the Secure Socket Layer (SSL) libraries from OpenSSL [11] to implement HTTPS protocol communication. OpenSSL supports SSLv2, SSLv3 and Transport Layer Security (TLS) v1. The version of encryption

is negotiated in handshaking between the web browser and web server. Most standard web browsers will support all these protocols and by default use the highest version of encryption supported. SSL and TLS both provide 128-bit encryption. For storage, we used the MySQL database engine. [12]

### 2.2. Security and Privacy

Security and privacy are also necessary in this type of system, security to prevent unauthorised access to the web-portal and privacy to inhibit the flow of electronic information to unintended recipients. Security features built into our application were designed not to hinder the usability of this system and, for this reason, many of these features are purposely transparent to the end user.

Communication between the psychiatrist and the patient could be read by the patient's family, if they share an e-mail account. Our secure web-based e-mail system has user authen-

tication, restricting access to the patient only.

One of the transparent security features is privilege and relationship checking before any clinical information is displayed. For example, a person may gain access to the system but, unless they are a registered psychiatric client, access to any clinical information is denied. Similarly, a relationship level of security is enforced, ensuring that a user is either the sender or recipient of a message before it is displayed.

Another potential privacy breach in e-mail-based telepsychiatry is when an e-mail is inadvertently sent to an unintended recipient [13]. We built a confirmation dialog box, designed to

ensure that the sender double-checks the recipient before an e-mail is sent.

A comprehensive audit trail was built into the system to allow the tracking of all user access and what operation the user performed.

### 2.3. Telemedicine-specific functionality

Commercial e-mail software is not an efficient modality for telemedicine applications. The ability to build specific telepsychiatry functionality was another important reason we chose to develop our own web-mail application.

Tracking whether the patient has read an e-mail is an important consid-

eration for the consulting psychiatrist, but not generally a well-supported feature in commercial software [14]. Mental health clinicians recently surveyed in Brisbane claimed that they would not use e-mail in any circumstance to communicate with patients because of the inability to check whether an e-mail message had been received by a patient [15]. We built into the system a flag that displays not only whether an e-mail message was read by the recipient, but also the date and time it was read. This flag is shown in Figure 3. This functionality reports on correspondence from the patient to the psychiatrist and vice-versa.

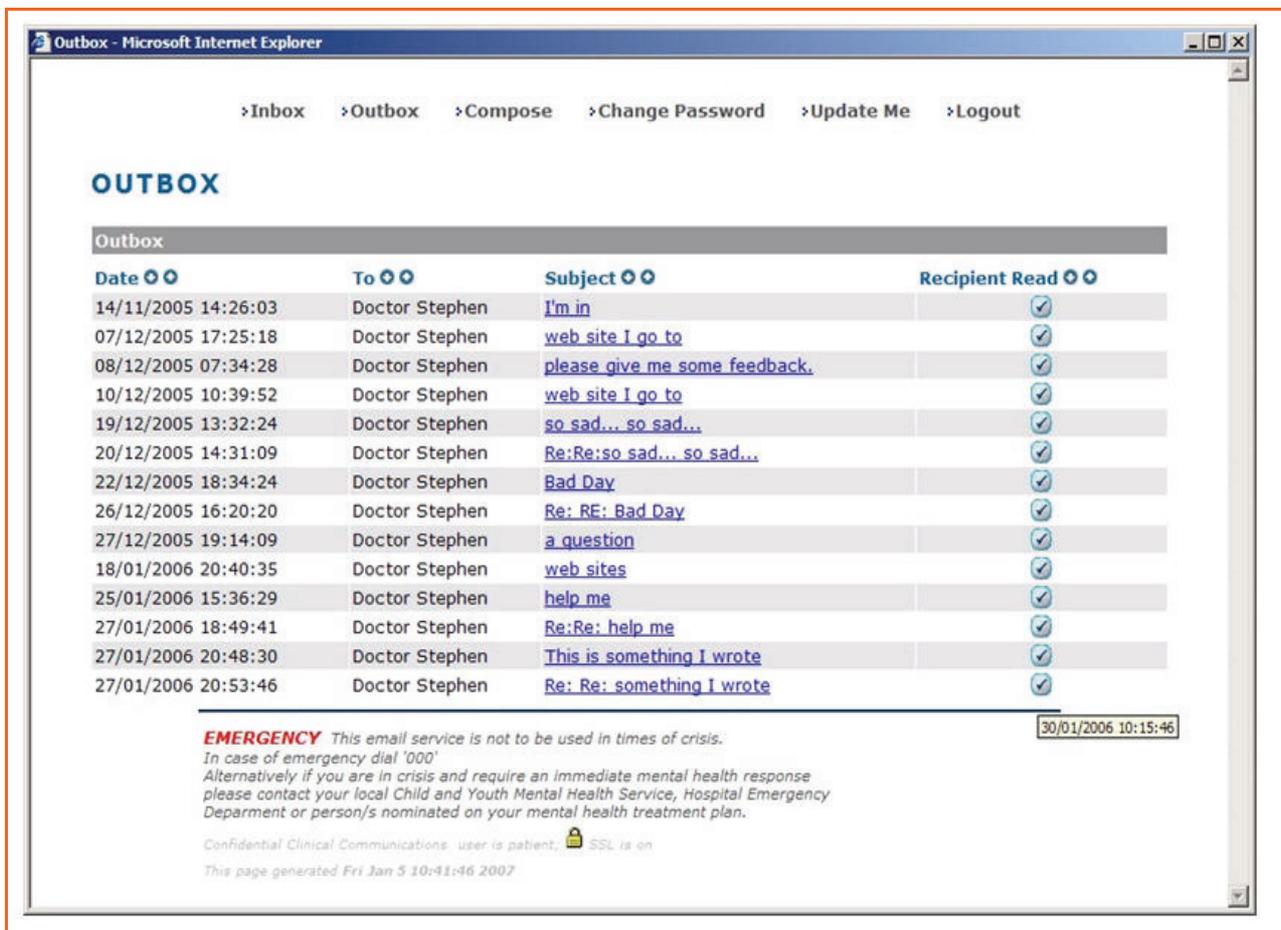


Figure 3: User's outbox with 'Recipient Read' flag. The date and time the message was read is shown when the mouse is hovered over the flag.

One of the failures of telemedicine has been to integrate into the day-to-day clinical practice delivery. To assist the integration of our secure e-mail system, we used automated, non-

secure notification e-mails. These notifications alert the user to new web e-mails without them having to log into the secure system to check.

## 3. Results

After development of the secure web-application, the system was

tested by staff from CYMHS and put into clinical practice in October 2005.

Patients were offered the use of the system during face-to-face consultations with their psychiatrist. It was during this face-to-face consultation that the patient was registered and an online relationship, necessary for security, set up. The patient was coached in the use of the system and the terms of usage. Patient registration triggers an automatic e-mail, containing a hyperlink to the secure web portal, to the client's e-mail

address. Currently, there are 29 patients and 1 psychiatrist enrolled in the service. Since inception there have been 280 e-mails, the psychiatrist sending 139 of these and the patients accounting for 141 e-mails. If we make the assumption that a teleconsultation is made up of an e-mail from both the patient and clinician, approximately 140 teleconsultations have been performed using our system. A median of 21 e-mails were sent per month (IQR 9-31) in the period from October 2005 to Novem-

ber 2006. Usage data are displayed in Figure 4. Figure 5 shows the proportion of patients living within and outside of the metropolitan region. 71% of consultations involved patients living in non-metropolitan areas. Table 1 describes the specific towns where patients involved in this study lived. The system continues to operate to date, and new patients are enrolled in the program subject to the discretion of the treating psychiatrist.

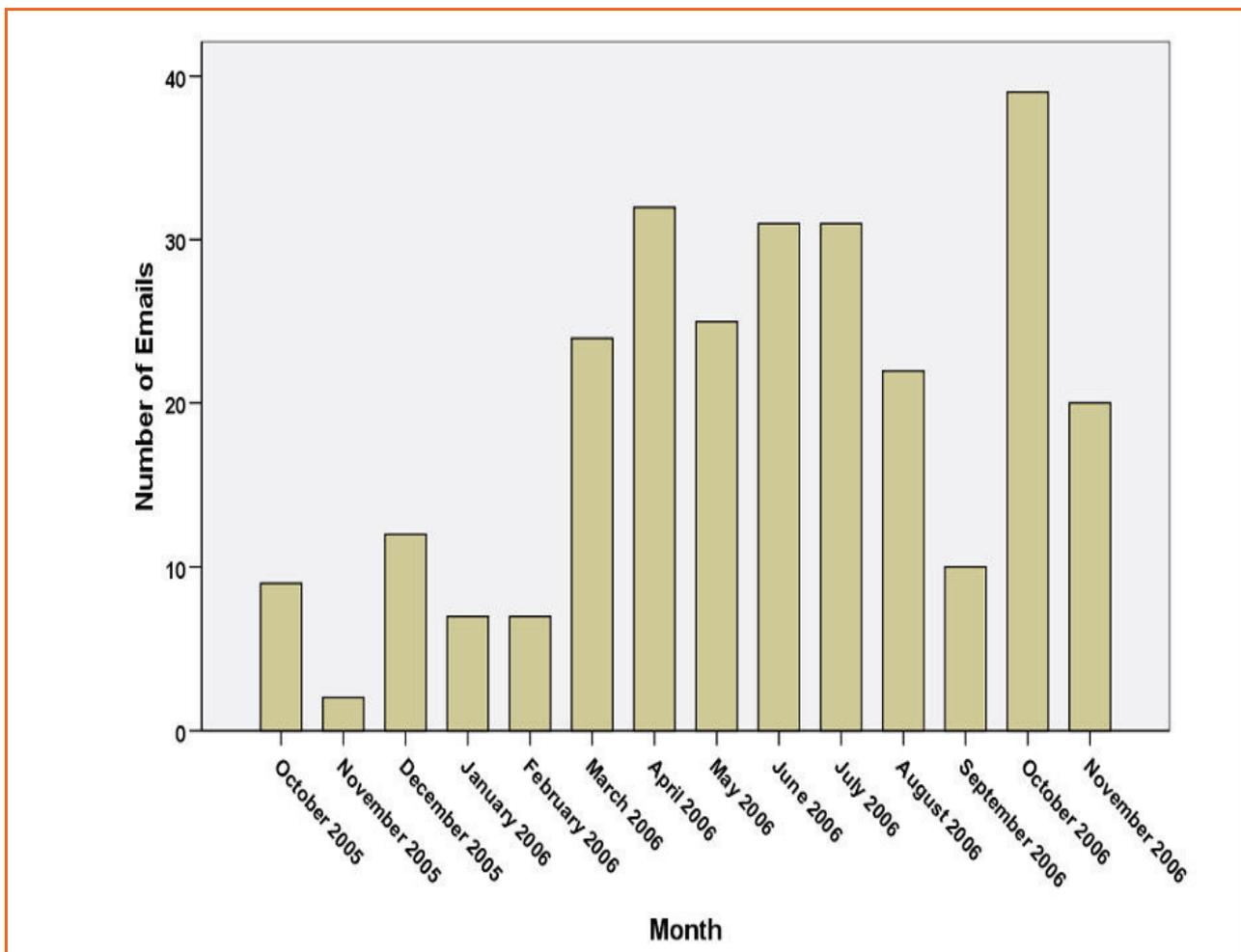


Figure 4: Number of secure e-mails per month (October 2005 to November 2006)

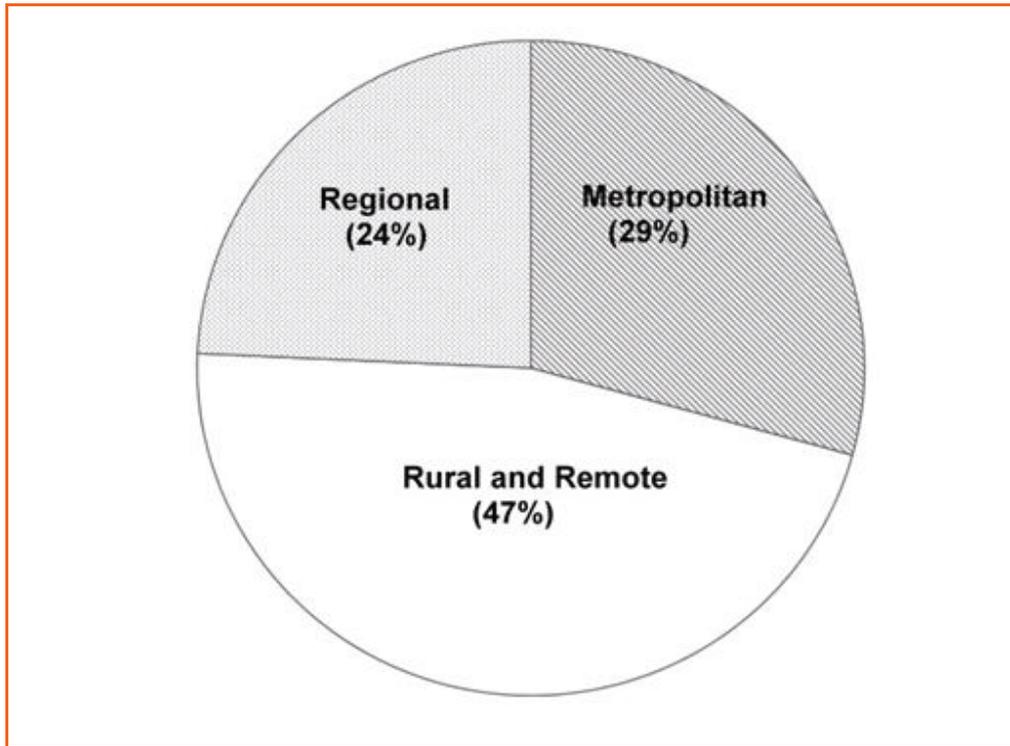


Figure 5: Proportion of consultations (n=140) according to patient's geographical location

Geographic Classification	Cities or Towns
Metropolitan	Brisbane
Regional	Sunshine Coast, Gold Coast, Redcliffe
Rural and Remote	Barcaldine, Blackall, Clermont, Longreach, Winton

Table 1: Towns and cities, with their associated geographic classification, where users of the secure e-mail system live

#### 4. Discussion

The use of encryption is imperative for running an e-mail-based telepsychiatry service. The key reasons are either legislative, policy-related or ethical in nature. The web-based client/server architecture used in our system not only improves compliance in the use of encryptions but adds telepsychiatry-specific functionality, hence the justification of our dedicated web-mail application. None of the statutory bodies make any recommendations on what type of encryption to use. For example, Queensland Health's IS42A policy states an "appropriate" encryption [8] and the American Informatics Association recommends encryption be implemented by "commercial encryption

programs or commercially available e-mail software" [16].

E-mail teleconsultations are likely to be more economical than video-conference appointments or "fly-in-fly-out" face-to-face consultations. However, e-mail cannot be used exclusively or for all types of consultations. E-mail is best used as an adjunct to face-to-face consultations. By its use in this manner, it may avoid the need for some of the more expensive face-to-face consultations. E-mail is not appropriate for emergency consultations and may not be appropriate for complex conditions.

Manhal-Baugus warns that secure web-based message systems offer better security than e-mail, but they are expensive to implement [13]. By using Open Source components, we

have been able to keep software costs to a minimum. One enhancement that we shall to add to our system is a timeout that would force a user to re-authenticate after a period of inactivity.

Improved psychiatric access for regional and remote patients was the original catalyst for developing our encrypted e-mail system. However, our psychiatrist has enrolled a number of metropolitan patients. Although not formally analysed, the psychiatrist also reports that the increased therapeutic contact has improved compliance to treatment regimes. This increased contact would unlikely have been cost- or time-justifiable with face-to-face consultations, whereas e-mail consultations were more efficient.

## 5. Conclusion

The development of a secure, encrypted web-based e-mail system for use in paediatric and adolescent telepsychiatry has proved feasible. The system was developed using commercial SSL libraries, namely OpenSSL. Trust in the system, assessed by usage, is apparent from both the psychiatrist and his patients and, anecdotally, positive patient outcomes have resulted. The system has met the ethical considerations of the psychiatrist and Queensland Health's administrative guidelines. We believe that the system would technically comply with the stricter legislative requirements of the United States' HIPAA legislation. This case report demonstrates that e-mail-based telepsychiatry has both a place in underserved regional communities and for patients undergoing therapy, regardless of their geographical location.

## References

1. Ryan VN, Stathis S, Smith AC, Best D, Wootton R. Telemedicine for rural and remote child and youth mental health services. *J Telemed Telecare* 2005;11 Suppl 2:S76-8.
2. Murdoch JW, Connor-Greene PA. Enhancing therapeutic impact and therapeutic alliance through electronic mail homework assignments. *J Psychother Pract Res* 2000;9(4):232-7.
3. Yager J. E-mail as a therapeutic adjunct in the outpatient treatment of anorexia nervosa: Illustrative case material and discussion of the issues. *Int J Eat Disord* 2001;29(2):125-38
4. Robinson PH, Serfaty MA. The Use of E-mail in the Identification of Bulimia Nervosa and its Treatment. *European Eating Disorders Review* 2001;9(3):182-193.
5. Tate DF, Wing RR, Winett RA. Using Internet technology to deliver a behavioral weight loss program. *Jama* 2001;285(9):1172-7.
6. Leong SL, Gingrich D, Lewis PR, Mauger DT, George JH. Enhancing doctor-patient communication using email: a pilot study. *J Am Board Fam Pract* 2005;18(3):180-8.
7. Voelk R, Geyer A. Get a grip on E-mail security. What are the options for fulfilling the HIPAA e-mail encryption rules? *Healthc Inform* 2002;19(4):50.
8. Silk KR, Yager J. Suggested guidelines for e-mail communication in psychiatric practice. *J Clin Psychiatry* 2003;64(7):799-806.
9. Information Standard No 42A Information privacy for the Queensland Department of Health  
[http://www.qgcio.qld.gov.au/02\\_infostand/standards/is42a.pdf](http://www.qgcio.qld.gov.au/02_infostand/standards/is42a.pdf)
10. The Apache Software Foundation  
<http://www.apache.org/>
11. The Open Source toolkit for SSL/TLS  
<http://www.openssl.org/> MySQL The world's most popular open source database  
<http://www.mysql.com/>
12. Manhal-Baugus M. E-therapy: practical, ethical, and legal issues. *Cyberpsychol Behav* 2001;4(5):551-63.
13. Austin S. E-mail: so fast, so convenient, so ... risky? *Nursing* 2006;36(2):76.
14. Cartwright M, Gibbon P, McDermott BM, Bor W. The use of email in a child and adolescent mental health service: are staff ready? *J Telemed Telecare* 2005;11(4):199-204.
15. Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. The AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic-Patient Electronic Mail *J Am Med Assoc* 1998;5(1):104-111

## Correspondence

Liam Caffery  
Centre for Online Health  
University of Queensland  
Level 3, Foundation Building  
Royal Children's Hospital  
Herston Road  
Herston Qld 4029  
Australia

Phone: +61 (0)7 3346 4754  
Fax: +61 (0)7 3346 4705  
l.caffery@coh.uq.edu.au

<http://www.uq.edu.au/coh>