# The Case for Secure Clinical Messaging

A CogentiX White Paper

March 2016

CogentiX

# Table of Contents

# Executive Summary

Modern patient care often involves a number of different clinical practitioners who work in a variety of multi-disciplinary clinical care teams. The success of such teams is maximised where team members can communicate freely and efficiently.

### Challenges

Patient care is shared across many departments, many medical disciplines and many practitioners across many clinical teams. In hospital facilities and clinics, clinical patient care may also be provided over a continuous cycle of shifts, 24 x 7. In an ideal world, practitioners would be available to communicate with their colleagues at all times. However, this is completely unrealistic. Busy practitioners may be available only at certain times, which makes collaboration more difficult.

The clinical workplace is a highly interruptive environment. There may be multiple interruptions in the communication processes between clinical practitioners. The activities of direct patient care, and the flow of conversations between clinical colleagues, are interleaved, leading to a state of ongoing interruptions. This consumes time and has the potential to increase the risk of error, and as a result, patient safety.

Patient healthcare information, by its very nature, is private. Certainly it must not be allowed to become available in the public domain. It should be restricted to ensure that only the clinical personnel who have a valid relationship to the patient's care are able to access it. For these reasons, all communication systems that deal with the exchange of patient information must be secure.

### Approach

The fundamental approach to improving the efficiency of communication events is to leverage modern mobile device technology to deliver collaboration messages between practitioners. This enables the exchange of collaboration messages in real time.

Studies into workflow analysis have proposed that the use of mobile device technologies for collaboration enhance inter-practitioner communication by reducing interruptions or by deferring interruptions to more appropriate times. [1] [2] [3]

SMS and email systems are not the answer. There are definite drawbacks with the use of SMS and similar messaging services, when used for any purposes beyond simple greetings and very short notes. In addition, the use of standard SMS and email systems runs the risk that both clinical and non-clinical communication messages will be mixed together, which greatly increases the risk to patient safety through missed or misinterpreted messages. However, the main concern regarding text messaging in healthcare is the inability to provide secure transmission of, and storage of, patient healthcare information. Standard SMS and email services simply do not provide this capability. Clinical messages need to be heavily encrypted to preserve the privacy of patient data. Finally, the use of email messages for clinical collaboration requires practitioners to extract patient information from one of the clinical systems, and then manually attach the information to the emails. This is a manual process that includes an element of potential human error. Hence SMS and email are not viable options.

A far better solution for collaboration in healthcare is secure messaging. Secure messaging is similar to other messaging services like SMS and email. However, it uses an approach with a dedicated secure server

and secure client devices that enable protected transmission of healthcare information between practitioners. One of the major objectives in the adoption of the secure messaging approach is to provide a single technological contact point for clinical practitioners to exchange secure private communication of clinical information, regardless of location and type of user device. In simple terms, regardless of vendor, device and operating system, the look, feel and behaviour of the secure messaging user interface should be the same. A message in-box is a mechanism that is familiar to users of both SMS and email systems. By leveraging this concept and providing a solution with a single standardised in-box for all communication messages, it enables greater efficiencies in the collaboration between practitioners.

Like email, secure messaging systems do not only allow text messages. They are also capable of exchanging a rich collection of other information types, such as audio, voice messages, photographs and video of patient problems. When a secure messaging system is extended to be patient oriented, it allows messages to directly include information about patients and/or clinical events (such as pathology results) to the messages. This provides the context to the secure message and obviates the need to manually cut and paste the information from other clinical systems.

## Benefits

One of the fundamental benefits derived from the use of clinical messaging is the enhancement of patient safety through clear unambiguous communication between practitioners. Direct secure messaging provides practitioners with real-time information in a single application. As it borrows from the philosophy of email, real-time secure messaging reduces the level of interruption for the users. The users are able to respond to messages when they are ready.

Therefore, the realisation of a secure clinical messaging solution on mobile devices has direct benefits to the daily working life of the practitioner. Practitioner-to-practitioner collaboration and workflow is vested in a single application. The practitioner only needs to consider one in-box for all clinical communication with colleagues. This greatly simplifies the process of communication.

One of the overarching principles in the creation of a clinical collaboration solution is to ensure that the patient information being exchanged is secure at all times. Healthcare organisations are required to abide by national laws and professional ethics, which are designed to preserve the privacy of patient information whenever it is being exchanged. The secure messaging solution adheres to the principle by providing strong encryption of all patient information while it is being transmitted and may also when it is at rest in a collaboration repository. Where patient images and videos are being attached to a message, patient privacy is further protected by allowing patients to have the choice to provide their informed consent and thereby sanction the use of their information in the exchange.


All of these benefits are delivered with M-Stat. It provides all clinical practitioners with a single tool for clinical collaboration and workflow in the palm of their hands.

# Overview

The safe management of patient healthcare is a complex and diverse subject. Generally, a patient will not be cared for by an individual practitioner, but rather by a number of multi-disciplinary clinical care teams. The success of such care teams is maximised where team members are able to communicate with each other freely and efficiently.

This white paper discusses how the communication challenges faced by busy clinical practitioners can be addressed through the use of secure clinical messaging, using modern mobile devices, and sets out how the CogentiX collaboration solution addresses these needs.

# Challenges

Modern healthcare settings are able to provide the latest clinical care to a large population of patients. But the required scale and complexity in the delivery of sophisticated healthcare to so many patients together create unique challenges for clinical practitioners. Patient care is shared across many departments, many medical disciplines and many practitioners across many clinical teams. In hospitals and clinics, patient care may also be provided over a continuous cycle of shifts, 24 hours a day, 7 days a week. Medical practitioners must balance the care of the individual patients with the ongoing collaboration of their colleagues.

## Complex Communication

The key principal for modern patient care is to ensure that the quality and speed of patient care is maximised. [1] This is an essential ingredient of patient safety. However, many medical personnel in modern hospital facilities feel disempowered to deliver optimum patient care due to restrictions on their ability to communicate with their colleagues. This affects all clinical practitioners, including doctors, nurses, and allied healthcare professionals. [1]

Since the overall management of a patient may transcend a number of medical disciplines, it is important for clinical practitioners to be able to collaborate with their cohort and coordinate with them to provide the optimum patient care. Unfortunately, many doctors, nurses and other caregivers often have difficulty in reaching their colleagues. The situation is made more difficult because clinical personnel are a highly mobile work force who move around the hospital or clinic and deal with a variable number of patients. This

situation is a common source of inefficiency in the delivery of patient care, and a source of frustration for the clinical practitioners involved.

In a recent study of clinical communication events, it was confirmed that there are in fact a large number of individual communications, which occur routinely between clinicians during the collaboration process. [1] Content analysis revealed that messages were predominantly non-urgent. The two most frequent purposes for communications were to convey information (91%) and to request an action by the physician (36%).

In an ideal world, practitioners would be available to communicate with their colleagues at all times. However, this is completely unrealistic. Busy practitioners may be available only at certain times, which makes collaboration more difficult. To date, clinical personnel have attempted to address the problem with existing technologies. Mobile phone technologies have been trialled by both clinical practitioners and researchers. Practitioners have used their personal mobile devices to communicate with members of their own medical teams, with other medical specialties, and with other allied healthcare professionals. [4] Clinical practitioners understood the risks associated with communicating confidential health information via their personal smartphones, but appeared to favour efficiency over privacy issues. This is a serious problem.

## Ongoing Interruptions

The clinical workspace is a highly interruptive environment. Multiple interruptions in the communication processes between practitioners consume time and have the potential to increase the risk of error. [2]

The clinical work force is never static. Practitioners are in constant movement around the hospital or clinic, from ward to ward, patient to patient, etc. Studies of clinical collaboration have observed that clinicians spend the majority of their time on patient care (about 85%) with about three-quarters of that time spent on indirect patient care (e.g. charting). Clinicians were observed to prefer using synchronous communication modes, which led to multi-tasking and created a highly interrupted workflow. About 40% of communication events were regarded as interruptions. While each interruption was short-lived, they occurred frequently. Both attending physicians and nurses were the recipients of more interruptions than they initiated. [2]

## Security

Patient healthcare information is, by its very nature, private. Certainly it must not be allowed to become available in the public domain. It should be restricted to ensure that only the clinical personnel who have a valid relationship to the patient's care are able to access it. For these reasons, all communication systems that deal with the exchange of patient information must be secure. In the case of practitioner-to-practitioner (P2P) communication, security measures must be in force to preserve patient privacy at all times. This applies while the patient information is being passed from one practitioner to another, and when the information is at rest within a data repository.

Practitioners are already using personal smartphones for work-related purposes on the wards, and without adequate security measures in place, or the permission of their place of employment. With the increasing popularity of smartphone devices, it is anticipated that an increasing number of clinicians will use their personal smartphones for clinical work. [4]

The security of patient information is a very serious topic. The use of unencrypted email messages to communicate private patient information is regarded as a breach of medical ethics. Organisations in the healthcare sector do understand the risks associated with unsecured private patient information. As an example, the Royal Australian College of General Practitioners (RACGP) regards unsecured transmissions of patient information as a violation of its standards. Government bodies are also aware of these security risks. To illustrate this, the non-secure transmission of private patient information is a breach of the Australian Privacy Act, and carries with it a fine of up to $1.7 million. [5]

# Approach

## Direct Rapid Communication

The fundamental approach to improving the efficiency of communication events is to leverage modern mobile device technology to deliver collaboration messages between practitioners. This enables the exchange of collaboration messages in real-time.

When clinical practitioners communicate as directly as possible, tests and procedures can be ordered without delay, clinical test results can be analysed quickly, and therapies can be started appropriately. This leads to more efficient care, and potentially to a reduced length of stay. These are important factors for both the hospital and the patient.

Given all the transitions that patients may experience throughout the course of their period of care, the timely transmission of information is also critical. When a transition of care occurs, the hospital or clinic needs to ensure the right information is communicated, so the next caregivers have everything they need for a seamless and safe transition. [3]

## Reducing Interruptions

Studies into workflow analysis have proposed that the use of mobile device technologies for collaboration enhances inter-practitioner communication by reducing interruptions, or by deferring interruptions to more appropriate times. [2]

There has been a perceived improvement in the efficiency of collaboration communication over the use of more primitive devices, such as pagers, for clinical communication for doctors, nurses, and allied health professionals. In particular, resident doctors found that the use of smartphones helped to increase their mobility and multitasking abilities. [6]

## SMS and Email Are Not the Answer

At first glance, a solution to address these challenges may appear to be simple.

One approach might be to allow practitioners to simply use email and SMS messages available on mobile phones and other portable devices. However, this approach falls far short of addressing the requirements for clinical collaboration. This is especially true where BYOD mobile devices are used. General mobile device systems for SMS and email are very general capabilities. If a general mobile device SMS service or email service was used for clinical collaboration, then this would pose serious questions.

Although the Short Message Service (SMS) can be a quick and effective way to communicate, there are definite drawbacks to the use of SMS and similar messaging services. [7] When used for any purposes beyond simple greetings and notes, there are serious issues. SMS messages have a modest character limitation (e.g. 160 characters in a single SMS message). Along with this, the delivery of an SMS message is not guaranteed. Many SMS subscribers have no way to reliably confirm delivery. The main concern

regarding text messaging in healthcare is the inability to provide secure transmission and storage of patient health information. Unfortunately, it is currently not possible to guarantee the encryption of SMS messages end-to-end, in particular when they are sent between different cellular networks. That leaves users vulnerable to sending messages that contain private health information that can be intercepted, read by, and forwarded to virtually anyone. Such messages may also remain unencrypted on the servers of telecommunication providers, and persist indefinitely on senders' and receivers' mobile phones and tablets.

This approach would permit the transfer of sensitive patient information across open public telecommunications networks. Different mobile devices from different vendors support different message and email services. The experience on one device would differ from another, and service levels for the delivery of clinical collaboration messages on one device and service provider would differ from another. This could make the management of the clinical information being exchanged virtually impossible. [8]

According to an article from the American Society of Orthopaedic Surgeons, the Joint Commission[1] has "effectively banned physicians from using traditional SMS for any communication that contains ePHI (electronic Protected Health Information) data, or includes an order for a patient to a hospital or other healthcare setting." [8]

Email on mobile devices appears to be a superior choice over SMS. An email does not impose the strict character limitation that an SMS message does, and it provides the user with more options for including or attaching clinical information. However, if the email server is hosted by an external provider, then this approach will suffer from all of the same security concerns that SMS messaging does.

An alternative approach could be to use a central email service. While this is some improvement on the previous SMS approach, it is still not a suitable solution. Clinical email messages would be interspersed with other non-clinical messages, making it challenging for the clinician to confidently obtain all clinical collaboration messages. Clinical patient information exists in clinical systems (e.g. pathology, radiology, electronic health record, etc.), and not in email systems. Therefore, to use email messages for clinical collaboration would require practitioners to extract patient information from the clinical systems manually and then attach the information to the emails. This is a manual process that potentially includes an element of human error.

Clinical email messages would need to be heavily encrypted to preserve the privacy of patient information. This would require extra encryption software to be installed on the mobile devices and on central email servers.

In addition, general email servers are subject to the stresses and strains of managing the ongoing load of general email messages. Real world experience shows that email delivery can often be delayed. The sender believes that the email has been delivered, and the recipients are completely unaware that an email is pending. Most standard email applications on mobile devices also support a disconnected mode, in

[1] The Joint Commission is an independent not-for-profit group in the United States that administers voluntary accreditation programs for hospitals and other healthcare organisations. The commission develops performance standards that address crucial elements of operation, such as patient care, medication safety, infection control and consumer rights.

which a certain proportion of email message content is left on the device, and this content is generally unencrypted. If these email applications are used for exchanging private patient information, then any person with access to the device also has access to the patient's information.

Therefore, email servers are not the preferred solution for the delivery of practitioner-to-practitioner messages.

## Secure Messaging

A far more appropriate solution for collaboration in healthcare is secure messaging. Secure messaging is similar to other messaging services like SMS and email. However, it uses an approach with a dedicated secure server and secure client devices, which enable secure and protected transmission of healthcare information between practitioners.

The overall approach of using secure messaging has already been endorsed in various countries by national healthcare authorities.

A report by the American Academy of Orthopaedic Surgeons (AAOS) aimed to assist in the development of compliant secure messaging systems. [8] It outlined four major areas that it considered to be critical to compliance:

- **Secure data centres**

  Patient information is usually stored in secure data centres that are either on-site or cloud-based.

- **Encryption**

  Electronic personal health information must be encrypted during transmission (client device to server, and server to client device) and while it is at rest (in storage).

- **Recipient authentication**

  All electronic communications of personal health information must reach (and only reach) its intended recipients. It should inform the sender when a message has been delivered and received.

- **Audit controls**

  Any compliant secure messaging system must also have the ability to create and record an audit trail of all communication events. This includes the ability to store messages and any associated metadata, so that the messages can be interrogated to be able to monitor the system.

Note that a secure messaging system is not simply an email application. It provides real-time transmission of messages with guaranteed delivery. It is a closed secure system of communication, which enables secure messaging to be used in conjunction with other electronic or mobile health services. The system should be tightly integrated with patient information systems (e.g. electronic health record (EHR)), so that related patient information is automatically accessible to the messaging application and transmitted within a communication event. This obviates the need for any manual process (of typing, cutting and pasting, etc.) to send patient information. As this further minimises human error, it minimises any risks to patient safety. These features therefore elevate secure messaging far above simple email.

## Standardised In-Box

One of the major objectives in the adoption of the secure messaging approach is to provide a single uniform contact point for clinical practitioners to conduct secure communication of clinical information. Regardless of the user's location, or the type of device being used, the look, feel and behaviour of the secure messaging user interface should be the same.

A message in-box is a mechanism that is familiar to users of SMS and email systems. By leveraging this user interface paradigm, and providing a solution with a single unified in-box for all communication of secure messages, it enables greater efficiencies in the collaboration between practitioners.

A standardised in-box was implemented in the Division of General Internal Medicine of the Mayo Clinic (Rochester, MN) to decrease the time physicians, physician assistants, and nurse practitioners spend on administrative tasks, and to increase efficiency. It provided a selection of standardised message types and associated content. The project demonstrated the successful implementation of the standardized in-box messaging system. This in turn resulted in a reduction of the number of administrative tasks completed by clinical practitioners. [9]

The benefits of improved efficiencies are especially important when considering the collaboration between doctors and nurses. Doctor-nurse communications are critical for patient safety and for the effectiveness of clinical workflow. In an Australian study [10], where a bespoke messaging information system using Android phones was used, it concluded that smart phone capabilities enhanced the efficiency, safety, and effectiveness of a time challenged work force. Nurses found they could provide more information to their colleagues, and that it was easier to portray how unwell a patient was. Doctors found they were better able to prioritise their time, and that urgent tasks were more apparent for immediate action. Each of these benefits led to improvements in the efficiencies of the clinical workplace.

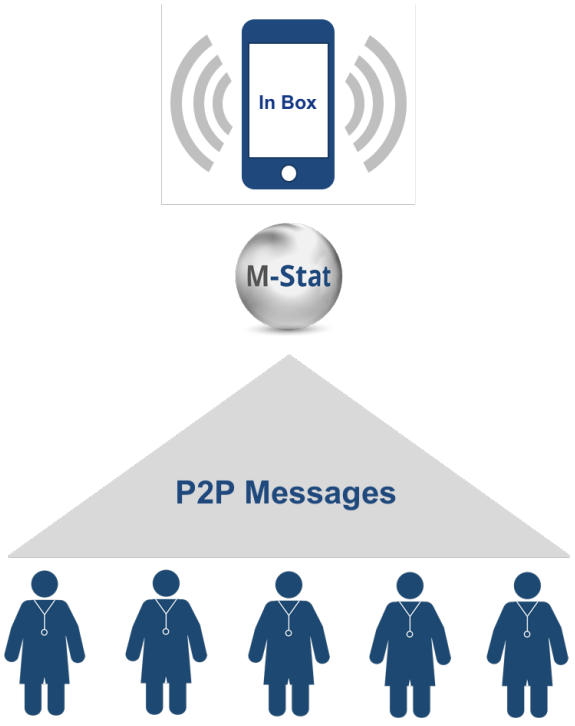
## Informed Patient Consent

Like email, secure messaging systems do not only allow text messages. They are also capable of exchanging a rich collection of other information types, such as audio, voice messages, photographs and video. This is particularly useful when communicating patient problems between colleagues. The approach of using secure messaging systems enhances collaboration efficiency, but at the same time, introduces a new challenge. Message content that includes patient photographs or video should not be exchanged without the patient's informed consent.

Informed consent includes both processes and information. The process part involves the clinical practitioner explaining the reasoning behind acquiring the photographic image or video, so that the patient understands why (i.e. they are informed). The information part involves recording the patient's consent to share the information with clinical practitioners.

There are also manual workplace mechanisms (using oral and hand written techniques) that are used to capture patient consent. The USA Federal Drug Administration (FDA) believes that obtaining a subject's oral or written informed consent is only part of the consent process. [11] It supports the belief that patient consent requires a general holistic collection of workplace security processes. Electronic and manual consent mechanisms are parts of these processes. It points to the need for a sound overall consent policy that should be followed whenever patient information is being shared across the healthcare landscape.

The CogentiX M-Stat collaboration solution addresses all of the concerns regarding collaboration between clinical practitioners by offering a holistic enterprise-wide mobile device communications solution, based around secure messaging, but tightly integrated with patient and practitioner information. The M-Stat collaboration solution has been designed from the ground up with patient safety and security in mind.




CogentiX M-Stat leverages the Convergent Mobility Platform (CMP), which manages the delivery and storage of all clinical messages exchanged between practitioners. The CMP forms the central hub for patient information and clinical messages, and delivers the information to the practitioner's mobile device in real-time and with guaranteed delivery.

M-Stat Collaboration is focused squarely on the provision of secure practitioner-to-practitioner (P2P) messaging. It manages P2P collaboration messages in a single in-box on your mobile device. The look and feel is familiar to those who are used to the ubiquitous email user interface.

Clinical practitioners collaborate using a simple but powerful clinical practitioner team structure to ensure that only the right practitioners receive P2P messages in their in-boxes. The practitioner can send new collaboration messages, and forward received messages to their colleagues in real-time. The target recipients of a P2P message may be one or more individual colleagues, or clinical team members. The user can assign a priority to a message to signify its level of importance to the recipients.

The user can easily forward a received test result (i.e. pathology, radiology, cardiology) to a colleague. The user may compose a new message and add patient information directly to the message. In fact, the user can compose a P2P message using a combination of patient details, results, text, picture, audio, and video content. This is especially useful when sharing pictures and video of patient conditions. Where a message contains patient images or video, M-Stat prompts the practitioner to obtain the patient's consent prior to

sending it. This protects the privacy of the patient's health information and provides the practitioner with peace of mind.

As security is all-important, M-Stat Collaboration comes with strong security measures out-of-the-box. Access to the M-Stat collaboration application is granted only when a user successfully logs on to the Convergent Mobility Platform (i.e. the CMP). All communication between the M-Stat application on the mobile device and the CMP server is encrypted using Transport Layer Security (TLS) / Secure Socket Layer (SSL). The M-Stat application on the mobile device establishes a secure session using aged session tokens based on the OAuth2.0 standard.

All interactions between the M-Stat application and the CMP are logged on the CMP server, which is hosted in a secure data centre. The P2P messages and the associated content are stored securely in the CMP database. No clinical information is ever stored on the mobile device. All logged data is stored in structured format for intelligent interrogation, audit and reporting.

# Benefits

By creating a unified approach to clinical messaging based on a secure messaging system, several important benefits can be realised.

## Enhanced Patient Safety and Quality of Care

One of the fundamental benefits derived from the use of clinical messaging is the enhancement of patient safety through clear direct unambiguous communication between practitioners. Studies of clinical communication inferred that because clinical messaging would improve collaboration between clinical practitioners, due to the timely availability of information through real time messages, eventually this would lead to improvements in the quality and safety of patient care. [5] [8] This aspect of improvement in patient care may be deduced directly from the capability of clinical messaging to connect practitioners more quickly for important conversations.

## Improved Practitioner Collaboration

Direct secure messaging provides practitioners with real-time information in a single application. As it borrows from the philosophy of email, real-time secure messaging reduces the level of interruption. Collaboration messages are sent asynchronously (i.e. send and forget), which reduces the burden of 'communication tag' between practitioners.

Since text, photographs, video and audio files can be included in the message, this provides a rich palette for the clinician to compose a message. One message can bundle together many elements, including: the patient record, with its encounter / visit records, their associated results, combined with a collection of multimedia attachments, and the full history of the ongoing conversation. This enables the communication to be more coarse-grained, and can therefore reduce the overall number of message exchanges required to communicate with colleagues.

## Enhanced Practitioner Efficiency and Satisfaction

The realisation of a secure clinical message solution on mobile devices has direct benefits to the daily working life of the practitioner. Practitioner-to-practitioner (P2P) collaboration and workflow is vested in a single application. The practitioner only needs to consider one in-box for all clinical communication with colleagues. This greatly simplifies the process of communication.

The findings of a number of studies support this position. Some suggest that clinical messaging provides increased clinical and allied health efficiency, satisfaction, improved practitioner work-life balance, and decreased workplace complexity because of the need to complete fewer administrative tasks. [9]

## Preservation of Patient Privacy

One of the overarching principles in the creation of a clinical collaboration solution is to ensure that the patient information being exchanged is secure at all times. Patient information must be treated as confidential. Healthcare organisations are required to abide by national laws and professional ethics, which are designed to preserve the privacy of patient information whenever it is being exchanged.

The secure messaging solution adheres to the principle by providing strong encryption of all patient information, while it is being transmitted and when it is at rest in a collaboration repository. Where patient images and videos are being attached to a message, patient privacy is further protected by allowing patients to have the choice to provide their informed consent and thereby sanction the use of their information in the exchange.

## In Conclusion

The healthcare work place will continue to be both a complex and challenging environment. High quality patient management in hospitals and clinics draws on a variety of disciplines across multiple clinical care teams. Practitioners work in an environment with a high percentage of ongoing interruptions. The challenge is to provide clinical practitioners with the optimum suite of tools for them to collaborate with their colleagues. An efficient collaboration solution should decrease the number of unnecessary interruptions imposed on the busy practitioners, and along with this, it must ensure the security of the patient information that they share.

The consensus in the industry is that traditional SMS and email systems are definitely not the solution. They do not offer an integrated solution that meets the requirements of the clinical workplace, and they fall well short of providing a solution that protects private patient information.

The preferred option is a dedicated secure messaging solution, which integrates with existing clinical systems and offers full protection to patient information.


The M-Stat Collaboration solution provides a secure messaging solution for mobile devices and workstations. It delivers all the capabilities of a real-time secure messaging system and also integrates with existing clinical systems via the Convergent Mobility Platform (CMP) to directly access patient information. It provides all clinical practitioners with a single tool for clinical collaboration and workflow in the palm of their hands. M-Stat Collaboration messages are received in a familiar email style in-box, and provides the capability to create rich multimedia messages by attaching patient records, test results, other messages, voice, photos and video content.

With the M-Stat Collaboration module, CogentiX offers its customers all of the benefits of a secure messaging solution as a part of the M-Stat mobility application suite.

# Bibliography

[1] C. N. C. Smith, S. D. Quan, P. G. Rossos, H. Khatibi, H. Wong and R. C. Wu, "Understanding interprofessional communication: a content analysis of email communications between doctors and nurses," *Applied Clinical Informatics,* vol. 3, no. 1, pp. 38-51, February 2012.

[2] A. Edwards, L.-A. Fitzpatrick, S. Augustine, A. Trzebucki, S. L. Cheng, C. Presseau, C. Mersmann, B. Heckman and S. Kachnowski, "Synchronous communication facilitates interruptive workflow for attending physicians and nurses in clinical settings," *InternationalJournal of Medical Informatics,* vol. 78, no. 9, pp. 629-637, September 2009.

[3] M. McKenna, "Improving Clinician-to-Clinician Communications," *Hospital and Health Networks (H&HN) Daily,* 2013.

[4] K. Tran, D. Morra, V. Lo, R. Quan and R. Wu, "The use of smartphones on General Internal Medicine wards," *Applied Clinical Informatics,* 2014.

[5] C. Bollen, "The Real World of Secure Messaging," BMP Consulting, 2104.

[6] R. Wu, P. Rossos, P. Quan, S. Reeves, V. Lo, B. Wong, M. Cheung and D. Morra, "An Evaluation of the Use of Smartphones to Communicate Between Clinicians: A Mixed-Methods Study," *Journal of Medical Internet Research,* vol. 13, no. 3, August 2011.

[7] R. V. Alali, "Implementing a CTRM solution for a Hospital inpatient workflow - Challenges & important factors to consider," 2012. [Online]. Available: https://www.linkedin.com/pulse/20140801015358-4685451-implementing-a-ctrm-solution-for-an-inpatient-workflow-challenges-important-factors-to-consider.

[8] T. Strome, "SMS doesn't translate to secure messaging in healthcare," 2014. [Online]. Available: http://searchhealthit.techtarget.com/feature/SMS-doesnt-translate-to-secure-messaging-in-healthcare.

[9] K. E. Cook, G. M. Ludens, A. K. Ghosh, W. C. Mundwell, K. C. Fleming and A. J. Majka, "Improving Efficiency and Reducing Administrative Burden through Electronic Communication," *The Permanente Journal,* vol. 17, no. 1, pp. 26 - 30, 2103.

[10] B. Cusack and D. Parry, "Customising doctor-nurse communications," Edith Cowan University, 2014.

[11] U.S. Department of Health and Human Services, Food and Drug Administration, Center for Drug Evaluation and Research (CDER), Office of Good Clinical Practice (OGCP), Center for Biologics Evaluation and Research (CBER), Center for Devices and Radiological H, "Use of Electronic Informed Consent in Clinical Investigations - Questions and Answers - Guidance for Industry," Food and Drug

Administration, 2015.

[12] The Royal Australian College of General Practitioners, “Compliance indicators for the Australian Privacy Principles,” The Royal Australian College of General Practitioners, 2014.

[13] M. Gibbs and H. Quillen, “The Medical-Grade Network: Helping Transform Healthcare,” CISCO Systems, 2007.

[14] MBS Online, “MBS FACT SHEETS AND CONSENT ISSUES,” 2012. [Online]. Available: http://www.mbsonline.gov.au/internet/mbsonline/publishing.nsf/Content/connectinghealthservices-patients-QA. [Accessed 2016].

[15] J. Ash, H. Singh and D. Sittig, “Self Assessment Clinician Communication,” The Office of the National Coordinator for Health Information Technology, 2014.

[16] L. Schilling, G. Bennett, S. Bull, A. Kempe, M. P. Wretling and E. Staton, “Text Messaging in Healthcare - Research Toolkit,” Centre for Research in Implementation Science and Prevention (CRISP), 2013.

CogentiX



## About CogentiX

CogentiX provides the next generation of intelligent clinical informatics software solutions for high performance healthcare. Our solutions supply medical practitioners with real time patient information on their smart phones and mobile devices, which empowers them to optimise decision support and patient care. The CogentiX solutions leverage a common mobility platform which integrates with clinical back end systems to provide a single window of access into patient information and delivers clinical workflow in the palm of their hands.

### Want More Information?

To learn more about CogentiX and any of our solutions, contact your CogentiX representative, visit our website or call us.



**CogentiX Pty. Ltd.**
www.cogentix.com.au
(M) 0408 885 644

PO Box 237
Stones Corner
Queensland 4120
Australia