Livingston County

E-Mail Encryption

Livingston County Support Center

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Document Purpose

1.1.1 THE PURPOSE OF THIS DOCUMENT IS TO GUIDE USERS OF LIVINGSTON COUNTY E-MAIL ENCRYPTION ON THE PROPER USE. **THE INFORMATION IN THIS DOCUMENT IS NOT INTENDED TO BE EXHAUSTIVE AND WILL BE UPDATED AS NECESSARY.** THIS DOCUMENT DESCRIBES WHEN TO USE E-MAIL ENCRYPTION, HOW TO SEND AN ENCRYPTED E-MAIL AND HOW TO RECEIVE AN ENCRYPTED E-MAIL.

1.2 Intended Users

Livingston County Employees

External Medical Professionals receiving ePHI from Livingston County.

Recipients of sensitive PII or PCI.

1.3 Supporting Documentation

The documents listed below are instrumental in determining when to send ePHI. Senders of ePHI should have a good understanding of these documents.

Resolution #	Date	Title
2013-04-107	04/9/13	*HIPAA-1 Protected Health Information (PHI)*
2013-04-107	04/9/13	*HIPAA-2* Security of Electronic Protected Health Information - All Employees
2013-04-107	04/9/13	*HIPAA-3* Security of Electronic Protected Health Information - IT Staff
2013-04-107	04/9/13	*HIPAA-4* Breach Notification for Unsecured Protected Health Information

2.0 USE OF E-MAIL ENCRYPTION

The following section will describe when to use e-mail encryption. This section is not intended to be exhaustive. E-mail encryption is not required within the Livingston County network. For example, e-mail encryption is not required when sending an e-mail from a domain of "livgov.com" to another "livgov.com" domain. E-mail encryption may be necessary when sending from a domain of "livgov.com" to a domain such as "yahoo.com", "Michigan.gov", etc.

2.1 ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

Livingston County Employees must use e-mail encryption for sending ePHI. Refer to the County HIPAA Policies for proper use of sending ePHI to a patient.

2.2 SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (SENSITIVE PII)

Livingston County Users should use e-mail encryption when sending sensitive PII to users external to Livingston County. Examples of Sensitive PII are Social Security Numbers (SSN), alien registration numbers, or biometric identifiers. Other data elements such as driver's license number, financial account number, citizenship or immigration status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII.

2.3 PAYMENT CARD INDUSTRY (PCI)

Livingston County Users should use e-mail encryption when sending PCI. In-scope cards include any debit, credit, and pre-paid cards branded with one of the five card association/brand logos that participate in the PCI-DSS - American Express, Discover, JCB, MasterCard, and Visa International.

2.4 OTHER INFORMATION AS REQUIRED BY LAW OR POLICY

3.0 GOOD PRACTICE WHEN SENDING AN ENCRYPTED E-MAIL

E-mail encryption is a relatively new practice to certain recipients. The following sections recommend good practice.

3.1 COMMUNICATE VERBALLY WITH THE INTENDED RECIPIENT

Contact the intended recipient and explain that an encrypted e-mail will be arriving in their e-mail in the future. Describe what the e-mail will appear like or refer the future recipient to this document link. If the recipient is a patient, you must follow the guidelines in the Livingston County HIPAA Policy and obtain a signed e-mail consent form.

3.2 SEND AN E-MAIL NOTIFYING THE RECIPIENT

Sometimes it is not possible to contact the recipient. In cases other than sending ePHI to a patient, the sender can send an e-mail prior to sending the encrypted e-mail.

Sample e-mail body

"This e-mail is to inform you that you will be receiving an encrypted e-mail shortly containing Protected Health Information (PHI) or information classified as sensitive. The e-mail subject line will contain a phrase of **[Send Secure].** The contents of the e-mail will guide you through registering an account which is only necessary for first time access. Once registered, you will only need your username and password to receive future encrypted e-mails from any department of Livingston County government.

Thank you for your understanding and helping Livingston County protect sensitive information!

4.0 SENDING AN ENCRYPTED E-MAIL USING MIMECAST FOR OUTLOOK

Livingston County employees: In order to transmit HIPAA protected information via email to a patient, the patient must have completed and submitted an *Email Consent Form*. The form is available on the Livingston County website at: http://www.livgov.com/HIPAA/Documents/email-consent-form.pdf

4.1 Using the Send Secure button

4.1.1 While in the main Outlook application select to compose a new message and navigate to the Mimecast tab. See Figure 1

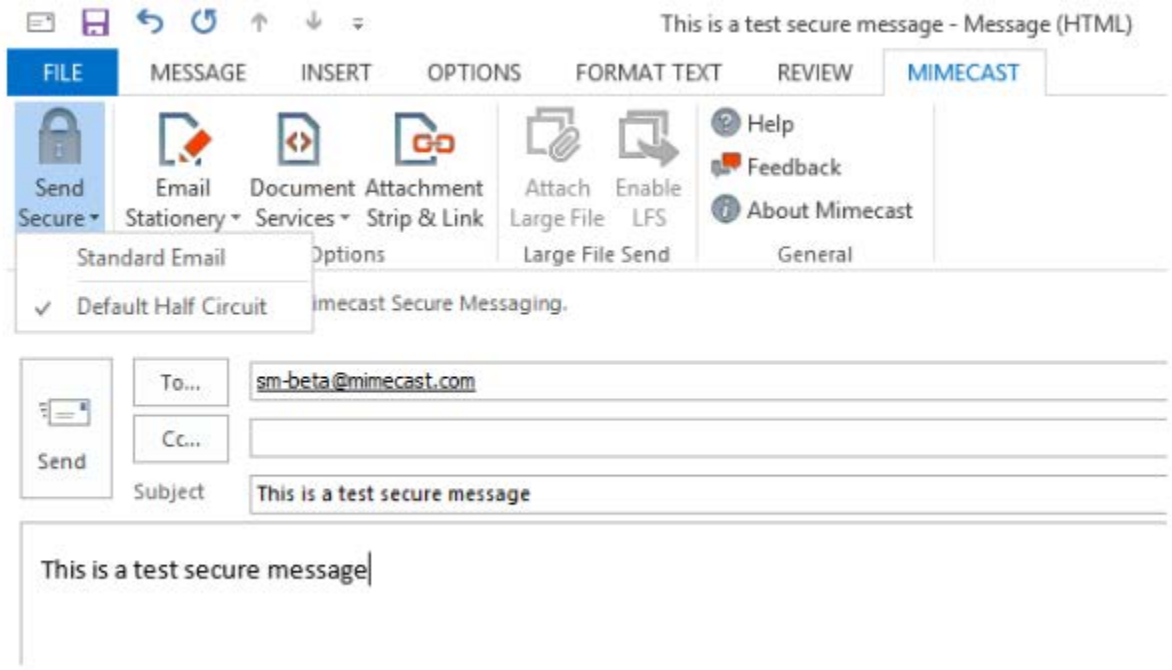

Figure 1

4.1.2 Click on the Send Secure button to reveal a list of Secure Messaging definitions published by your administrator. See Figure 1

4.1.3 Once your message is composed and you are ready to send, click Send as you would normally.

4.2 Using [Send Secure] in the subject line. See Figure 2

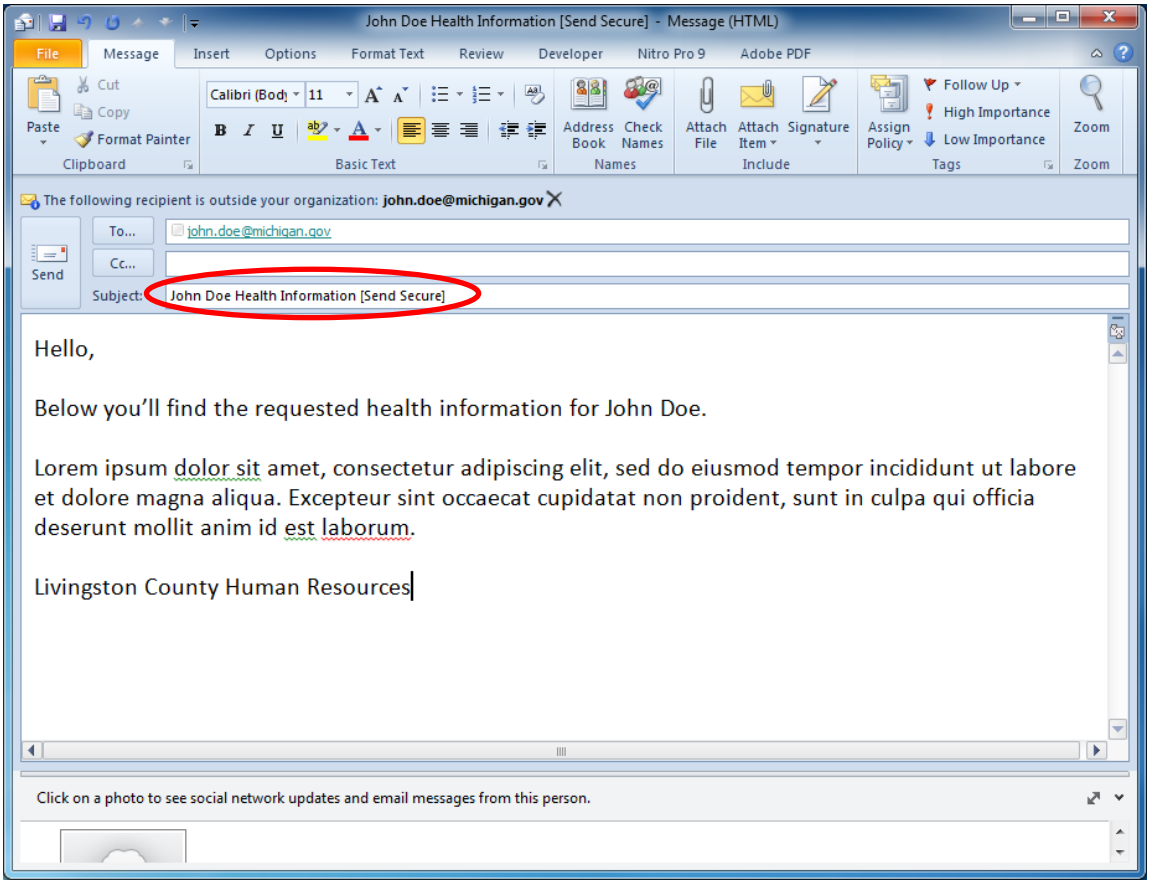

Figure 2

4.2.1 Add **[Send Secure]** to the subject line. You must include the "**[**"and"**]**" around the words "**Send Secure**", like in the example above. You may put "**[Send Secure]**" anywhere within the subject line, but it **MUST** be there.

4.2.2 Complete e-mail.

4.2.3 Click Send. The Livingston County system will encrypt the e-mail.

NOTE

Secure Messaging is only applicable to outbound messages to external recipients. When you use this option, external recipients will receive a notification inviting them to view your email in the Mimecast Secure Messaging Portal.

5.0 RECEIVING A SECURE MESSAGE EXTERNALLY

5.1 You have received a Secure Messaging notification from Livingston County. See Figure 3. Click “here” in the first sentence of the below message.

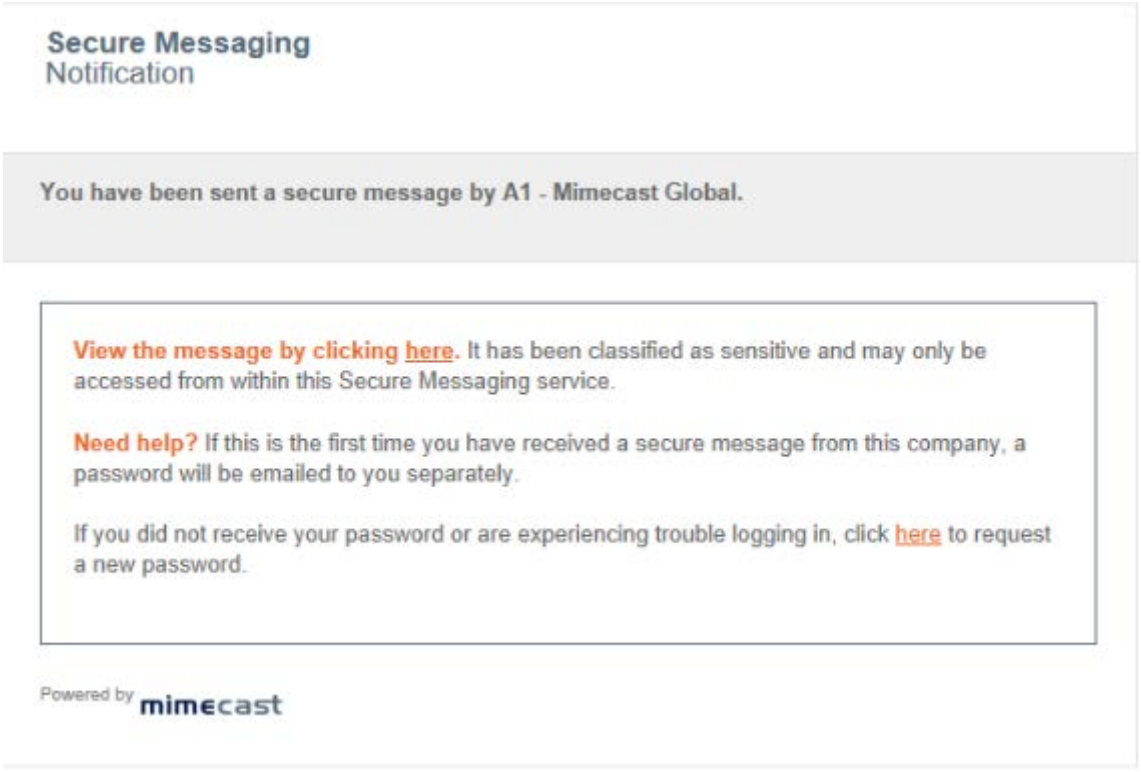

Figure 3

5.2 Follow the link in the email to open the Secure Messaging Portal. Add your email address, then click the Next button: See Figure 4

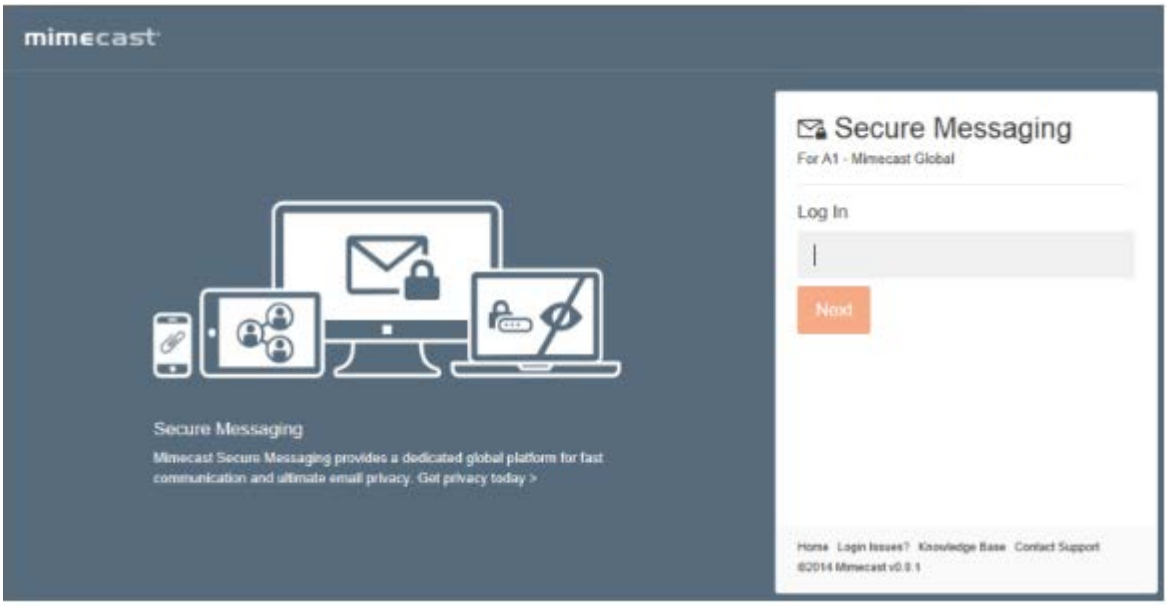

Figure 4

5.3 If this is the first time you have received a Secure Message, you must reset your temporary password before you can continue. Your current temporary password would have been sent to you in a separate EMAIL. SEE FIGURE 5

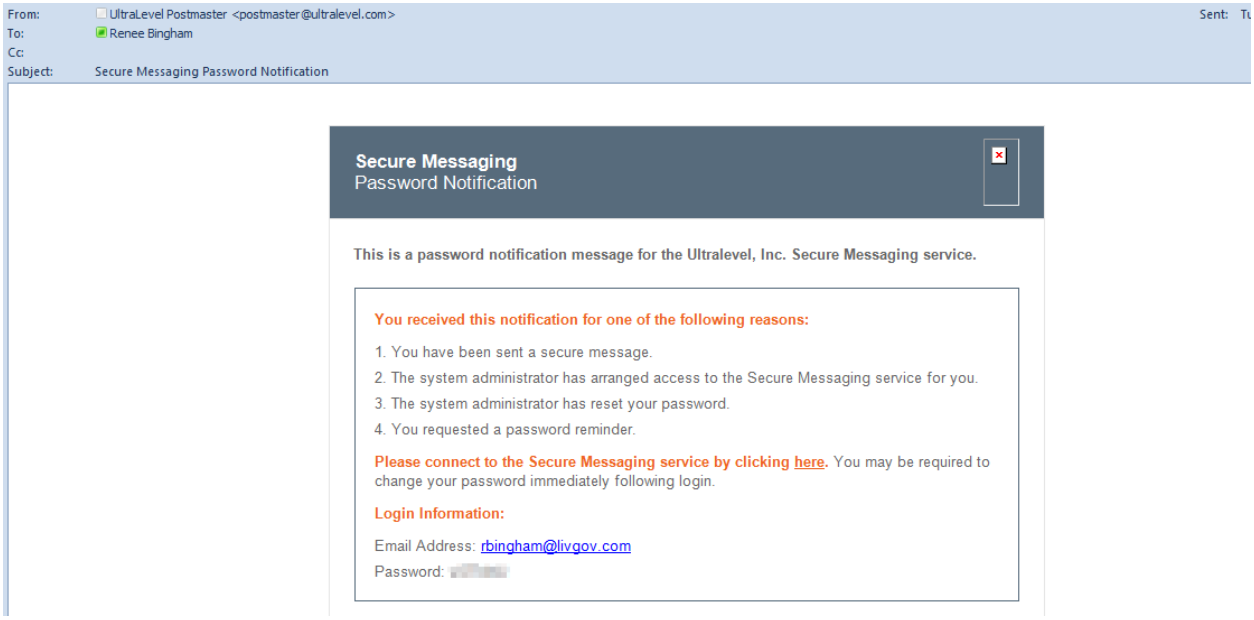

Figure 5

5.4 Once you have successfully logged in the Secure Messaging inbox is displayed. See Figure 5

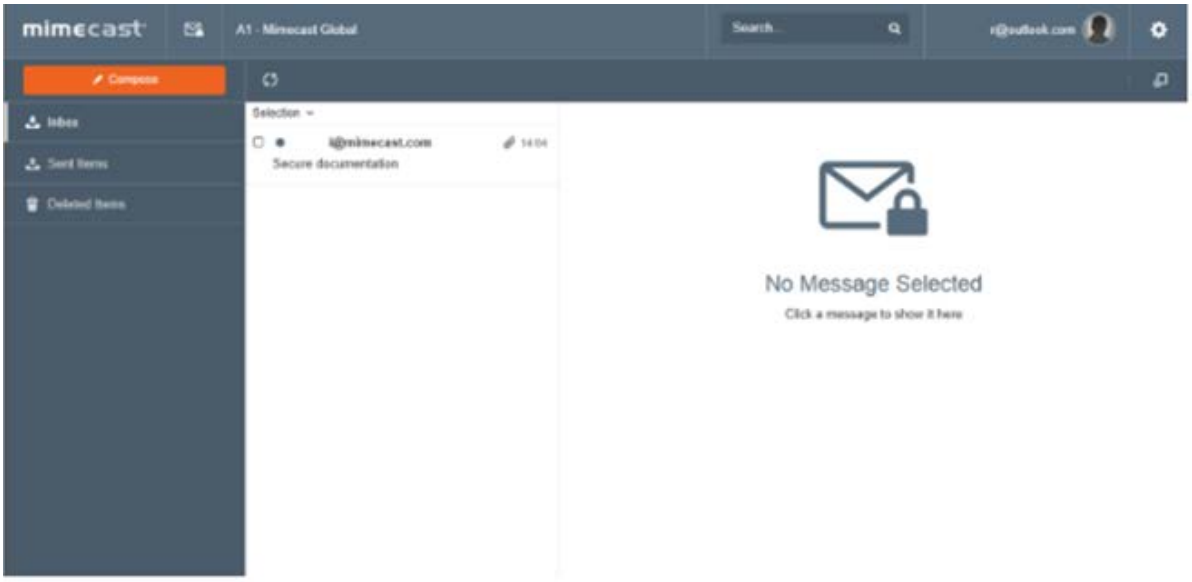

Figure 5