Sending PHI via E-Mail: HIPAA Requirement

After much discussion with the NYSARC Guardianship Committee and staff at the NYSARC State Office, we must adhere to the following when it comes to transmitting Protected Health Information (PHI): (a) encrypt emails (b) send PHI without using encryption using the free-standing facsimile (fax) machines or (c) using regular mail. PHI generally includes individually identifiable health information, including demographic data, relating to the individual's past, present, or future physical/mental health/condition, provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual.

Note on faxes: Using free-standing fax machines is compliant—this includes the printer/copier/fax machines that utilize regular telephone lines.

Using the Barracuda Secure Message Service

Our email system uses the *Barracuda Email and Virus Firewall* appliance, which has the ability to implement a secure email "gateway" between parties. To ensure that both ends of the transmission are secured, this gateway should be used when sending email that contains PHI outside of our own system. This system can be used to replace zip encryption; in fact it is much easier.

Using this system is very simple. To initiate the gateway, simply include this text anywhere in the SUBJECT line of your message (think **S**t. **L**awrence **N**ysarc-SECURE):

`SLN-SECURE`

This text is not case-sensitive. This will not initiate the gateway when sending email inside our own system (to anyone @slnysarc.org). Mail sent inside our system is already considered secured.

Your recipient will receive an email with the following subject line:

`You have a new encrypted message from user@slnysarc.org`
("user@slnysarc.org", of course, will be your email address)

The body of the message:

You have a new encrypted message from

user@slnysarc.org

ST. LAWRENCE NYSARC

You have received an email message from *user*@slnysarc.org that has been encrypted for privacy and security by the Barracuda Email Encryption Service.

To view the email message, click here to log into the Barracuda Message Center. You'll be prompted to either create a password or enter the one you may already have. You can also paste the following URL into your browser to access the Barracuda Message Center:

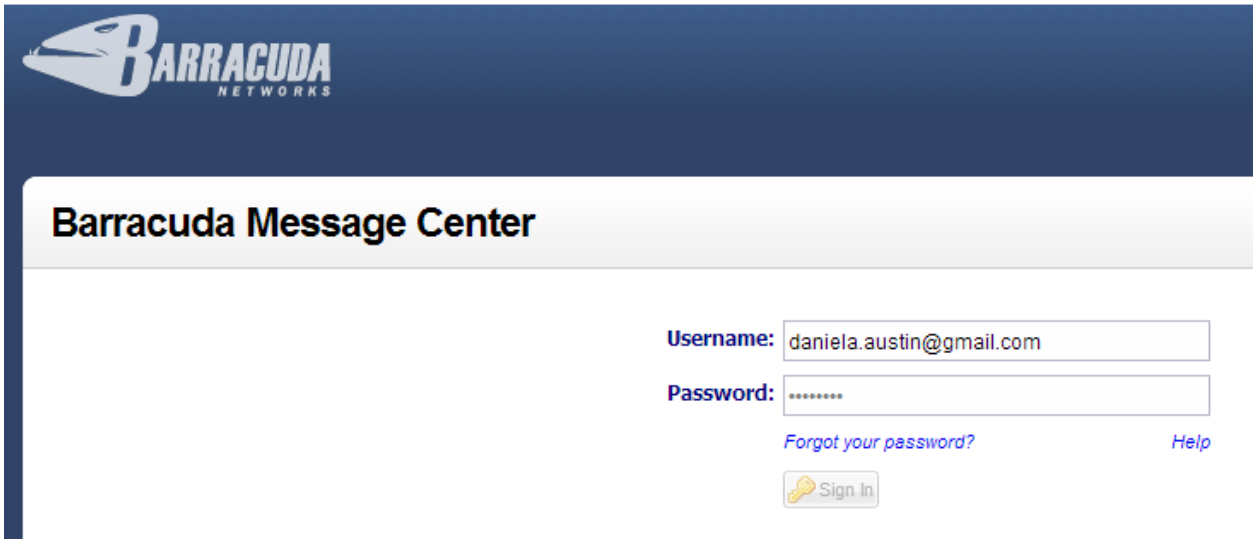
https://encrypt.barracudanetworks.com/login?nid=U2FsdGVkX18aKT%2FLPIMS8bQF1o1tKHGk4o9YphxuiD7n9OLCRuOV6v8XpNPrGcSZMOp746Nq1oH7oq9uKhdbwXJEKI64pq%2BgwYfTnOMPtz6utW9VsNqGYS0ILfeBptsTllZni0bGtRkdETV5JLCCa33D2RZXVtkljtXUALUyiCVN6IPHpJHPZUKXsW16exDaYpbaWeUJpn1ZeeRzLBCVPat71r1RKfhJS47nMH0SezEylnxk3rDZ9fJ%2FzDJ%2FD5a77Mn5DyjOeWK1kvIlx%2Feg2g%3D%3D

The secure message will expire in 30 days. Need Help?

Disclaimer: This email is confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender.

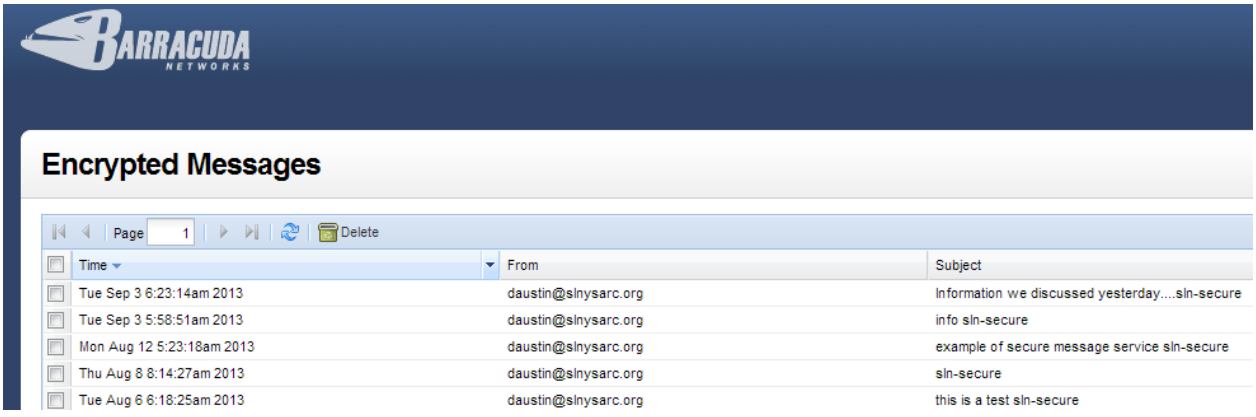
Copyright 2013 Barracuda Networks, Inc. All rights reserved

When you log into this site, you will be prompted for your password:

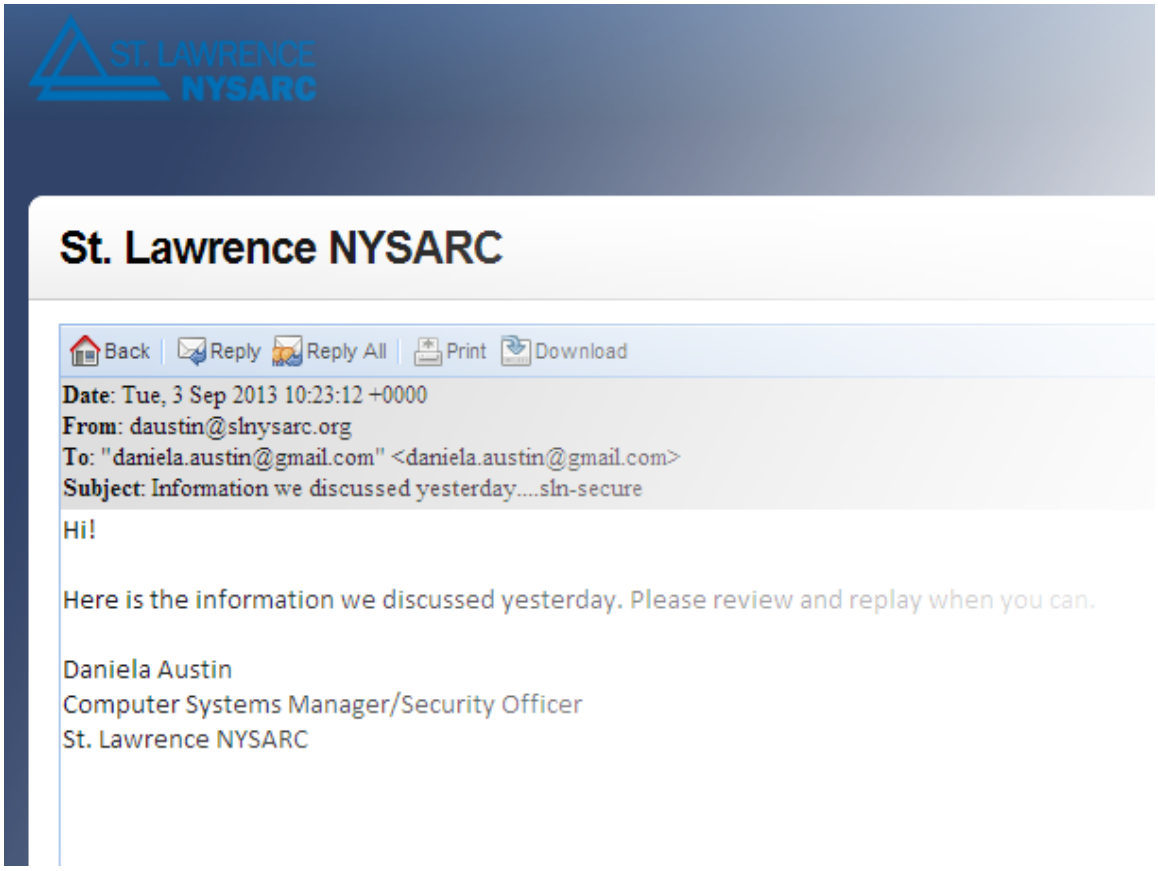


If this is the first time you have logged in, you will create a new password. **NOTE**: *This password is for the Barracuda site, NOT for any slnysarc site. It is not your domain password or your slnysarc email password*.

Once logged in, you can retrieve your message:



Click on your message and work with it in the usual way. You will have a simple email editor:



Email is kept on the gateway for 30 days and then it is deleted.

Please realize this is *not* a full-fledged email client, it is a third-party service for carrying out secure communication between two entities. It does not integrate with *Outlook* in any way.

Replies to this message will use the same gateway interface. That is, when your recipient replies to you, you will get a "`You have a new encrypted message from somebody@somewhere.org`" message and go through the gateway to retrieve it and respond to it.

Please keep the password to this site confidential; your account name on the Barracuda Secure Messaging System will be your email address.

To summarize:

- Use this procedure *every time* you send outside email containing PHI. Mail within our own system does not need to use this method; that is, mail to *only* @slnysarc.org accounts! Mail containing PHI to *everywhere* else *must* use the encryption service.
- This system replaces zip encryption. In fact, it is much easier.
- Add the following text anywhere in the subject line to initiate the secure gateway: **`SLN-SECURE`**
- Only regular, stand-alone fax machines that use our own telephone lines are OK.
- This is a simple, no-frills secure email system that many chapters are using to address unknown security protocols at the other end of the transmission—it is not intended to operate like *Outlook* or a full-fledged email client. Emails expire after 30 days.