What is TLS?
Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The TLS protocol is based on Netscape’s SSL 3.0 protocol; however, TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0. The most recent browser versions support TLS. The TLS Working Group, established in 1996, continues to work on the TLS protocol and related applications.

How do we get my school setup to use TLS?
How you get started using TLS depends on the MTA you’re using (i.e. the Message Transfer Agent that is sending and receiving email for your domain). There are several MTA’s on the market and depending on what you have you will need to look into the configuration specifics of that device.

At a high level, to setup TLS you will do the following:

1. Acquire an SSL Certificate from a Trusted Root (Verisign, Thawte)
2. Import that SSL Cert into your device
3. Enable TLS Encryption for outbound and inbound.
4. Test

When you are ready to test, you will contact tlssupport@uhcsr.com and we will work together to verify your domain is encrypting over TLS. In your email please include the following:

- Your Domain Name you would like us to test
- Technical Contact: Name, Email and Phone
- Alternate Technical Contact: Name, Email and Phone
- Business Contact: Name, Email and Phone

Once outbound TLS is confirmed and configured to TLS required for all future UHCSR Outbound communication, we will turn off outbound PHI (Private Health Information) Scanning for emails destined to your domain and all email will be encrypted over TLS from UHCSR.COM to your destination domains MTA. If in the future TLS is turned off on your side or does not work as specified for some reason, outbound emails will queue up until the TLS service is restored. We monitor these queues on a daily basis and will use the original contact information to alert you of an issue that needs your attention.

For more information please contact Partner Center Support (1-888-754-8089) or partnercentersupport@uhcsr.com.