TLS Connection with Smart Data Solutions

Part of SDS's ongoing training includes safeguarding against phishing attempts. To set our team up to be as successful as possible in safeguarding your data we are more aggressively flagging emails that contain links to external sites. Currently, many of the emails we receive from **your team** comes in as a 'secure shell', requiring us to go to a secure website to view the message.

To best keep your data safe SDS strongly encourages that we enable a TLS encryption between our mail servers. Typically, doing so takes about 10 minutes and involves just adding our domains (**sdata.us** and **smart-data-solutions.com**) to your email server, and have SDS add your domains (**@.com**) to our email server. After that, we both send an email to each other to verify that the message was indeed encrypted. We've gone through the process dozens of times and would be happy to provide details to your systems team if that would help.

Besides being more secure and helping to prevent successful phishing attempts, it also greatly helps SDS support your workflow. It's easier for our support team to manage and reply to emails if they come in directly into our email inbox rather than requiring we log into a secure shell. This solution also meets HIPAA requirements in protecting any PHI that may be sent via email, as the connection between our mail servers is completely encrypted.

Please let me know if that is something we could pursue.