NeoCertified Review – HIPAA Compliant Email

Let's be frank.

You're probably not an expert on digital security or encrypted communication. You may not even know the difference between S/MIME and TLS (they're encryption protocols, if you're wondering)—let alone how to bring all of your communications into compliance with HIPAA and HITECH.

And to make things even more confusing, there are dozens of companies out there touting their own brand of HIPAA compliant e-mail solutions.

So, how do you choose the right one?

You could spend a significant amount of time researching the topic, learning about encryption, cross-referencing features, and grilling IT experts. Or you could hire an expensive consultant to take care of that for you.

But the option many budding health organizations are taking? Choosing a provider with a proven track record.

And for many American health organizations, that provider is NeoCertified.

NeoCertified Bio

Founded in 2002, this Colorado-based company originally provided digital security and encryption services to enterprise-size clients.

As the need for secure online communications increased for small and medium-sized businesses, NeoCertified took notice.

Recognizing this gap in the market, the digital security firm opened its doors to smaller clients, providing that same commercial-grade security to thousands of companies in need of cutting-edge encryption.

14 years later, NeoCertified has garnered a reputation as America's premier provider of commercial-grade communication security.

Working with industries where security is of the utmost importance (health, finance, law, etc.), NeoCertified provides communication encryption for more than half a million users.

NeoCertified Service Overview

[NeoCertified HIPAA Compliant Email Service](#)

The bread and butter of NeoCertified's service offering is their excellent email encryption. Having provided this service for a decade and half—helping thousands of health organizations to bring their communications into compliance—NeoCertified has become the de facto compliant email leader of the industry.

It is no surprise, then, that many of the security measures required by HIPAA are built right into their email client.

The level of security is apparent from the moment you register. NeoCertified will not allow you to choose a weak password (one that is susceptible to brute force attacks).

A two-factor authentication must be established before you're able to log in (in the form of security questions).

End-to-end encryption (we'll revisit this in detail) is built right into the email system, ensuring that your communications will not be vulnerable to a man-in-the-middle attack.

Custom email settings are aplenty, allowing you to set expiration times for your communications, disable replies, etc.

As is required by HIPAA, NeoCertified also monitors all activity, and can generate 4 report types (message, user, event, and domain reports).

And like any truly secure communications platform, you can easily retract a sensitive email before the recipient has opened it.

All of these features are available for $99 USD/per user/per year.

[HIPAA Compliant Outlook](#)

If you aren't too keen on using a web portal for all of your secure communications, NeoCertified provides the option of integrating their services into your Outlook client.

This is an incredibly useful way to streamline your organization's communication. Rather than requiring your employees to login to a web portal every time they need to send a secure email, they can do so right from their native email application.

This feature is available to every license holder.

Note: In order to make your Outlook HIPAA compliant, you'll need to download an Outlook plugin from NeoCertified's web portal (you must be logged in).

[Inbound Secure Email](#)

Have you ever seen those contact forms on an organization's website? The ones that allow you to contact the organization directly on the site, without having to open your email client?

NeoCertified has figured out how to make them completely secure (and HIPAA compliant!). Basically, CustomerConnect allows your clients to transmit sensitive ePHI directly through your website, without fear of it being compromised or intercepted.

This is incredibly useful for several reasons:

1. A client doesn't need to know the email of the department they are trying to reach—they can quickly choose it from a drop down.
2. A potential client will not need to navigate away from your webpage to get in touch with you, which is a proven conversion boost.
3. A client will not need to create an account on NeoCertified's web portal to securely transmit sensitive ePHI.

It is a timesaver, a conversion booster, and just incredibly convenient.

Subscribing to this service will cost you a modest $195 USD/year, with one email license included. Since a single email license costs $99 USD/year, you're actually getting the CustomerConnect feature for less than $100.

That is an absolute steal.

Customer Service

As I have done for the past several reviews, I called in to NeoCertified's support line to get a feel for their level of customer service.

Despite being greeted by an automated robo-voice, I was actually able to get in touch with a sales rep within 30 seconds of calling. The gentleman who picked up was courteous and helpful, giving me a general overview of NeoCertified's services as well as a breakdown of the prices.

Although he was unable to answer some of my unnecessarily technical questions, he offered to put me in touch with one of NeoCertified's IT specialists.

It was a fairly short conversation, and we were able to cover all of the topics I had prepared for the phone call. I can confidently say that I had no lingering questions left by the time we bid each other goodbye.

One thing that stuck in my mind about this interaction was the lack of sales pressure.

After my last few customer service interactions, I was on guard for a hard sell. I kept waiting for him to ask for my email address, so he could send me a "provisional" contract with my name on it (a sales technique I encountered frequently with other HIPAA services).

But he never did.

He was simply there to answer my questions and offer his help. The choice to move forward would be entirely mine.

Because NeoCertified was so confident in their quality of service, they didn't need to submit potential clients to high-pressure sales techniques. At least, that was the impression I got.

And I have to say; it was a very refreshing customer service experience.

Expertise

Aside from having on-call IT professionals to answer any technical question you may have, NeoCertified also regularly publishes a stream of informative content to help you better understand digital security and HIPAA compliance.

The cornerstone of this content is a fantastic 14-page whitepaper detailing the importance of secure communications: [The Case for Secure Email](#).
Another excellent article featured on their website details [preventing identity theft](#) through the use of secure email.

Their blog is also regularly updated with educational content, detailing new trends in secure communication and answering questions like ["what is inbound secure email?"](#), ["how to choose a secure password?"](#)etc.

Given the company's focus on email, the scope of their educational content is quite impressive. These articles aren't just a way to sell you their services (as web content usually is). They are also a way to inform you and your employees on the best digital security practices for your business and personal life.

And once again, the hard sell is absent. This content paints a picture of a company confident in its offerings and generous with its expertise.

And I would expect nothing less of an industry leader.

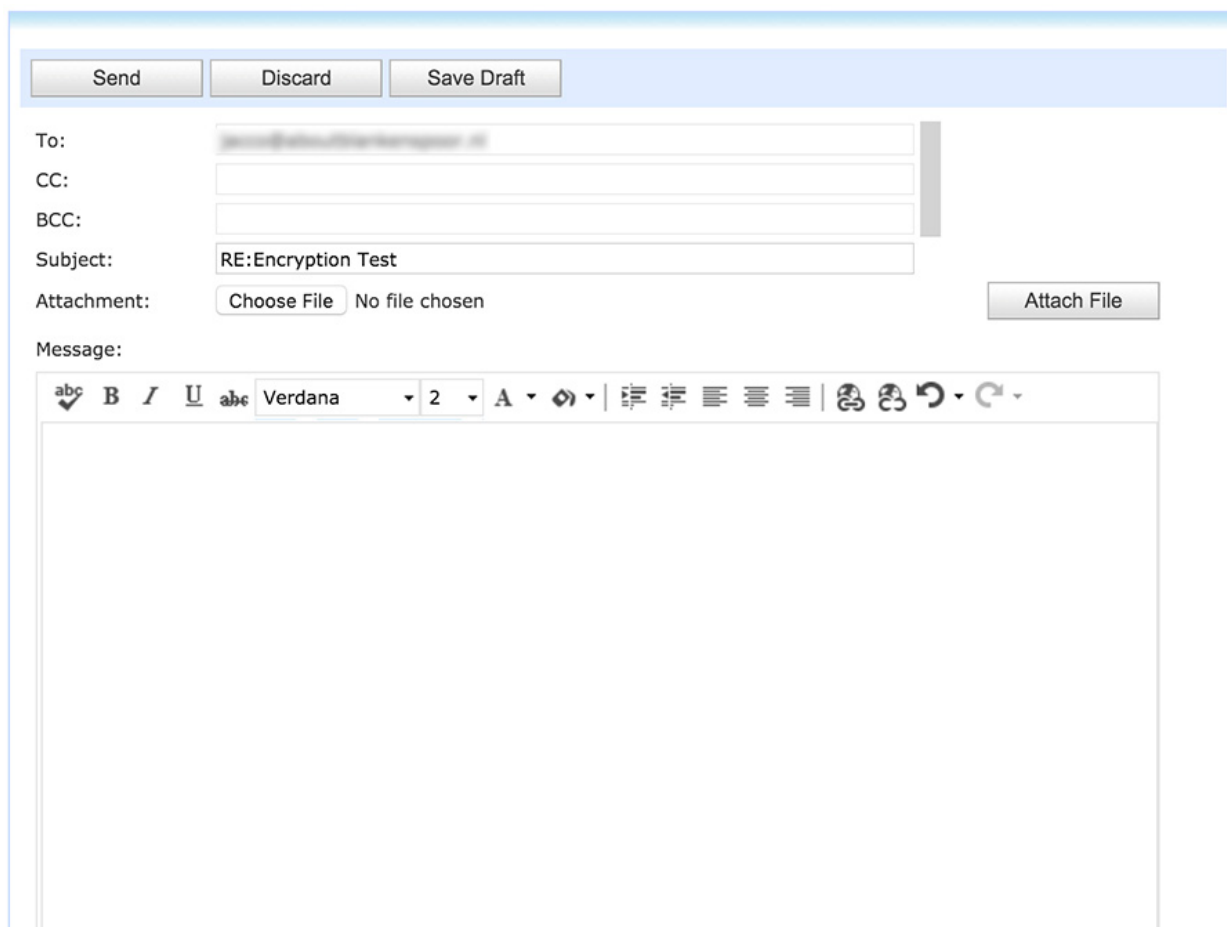# Interface/Usability

There's no sugarcoating it.

NeoCertified's web portal email interface is quite dated. In fact, it looks like it hasn't seen an update in more than a decade.

It's not just the aesthetic that seems stuck in the early 2000s. It is also the navigation.

While everything was easy to find, and worked just as well as you can expect it to, I found myself missing the streamlined organization of modern email services.

For example, when I attempted to send an attachment, I ended up sending out a blank email. First believing the client to be bugged, I looked again. Turns out I was simply spoiled by Google's and Microsoft's "one-click" simplicity.

On NeoCertified, after choosing a file from your computer, you must also find and click the dubiously placed "attach file" button to complete the process.


Another minor annoyance is NeoCertified's lack of threaded messages.

Most modern email providers organize email correspondences with the same subject line in a single "thread." These threads can hold hundreds of back and forth emails without cluttering up your inbox.

This is not the case for NeoCertified's web portal. Each "Re:" email takes up a single space in your inbox. As you can imagine, things become cluttered very quickly.
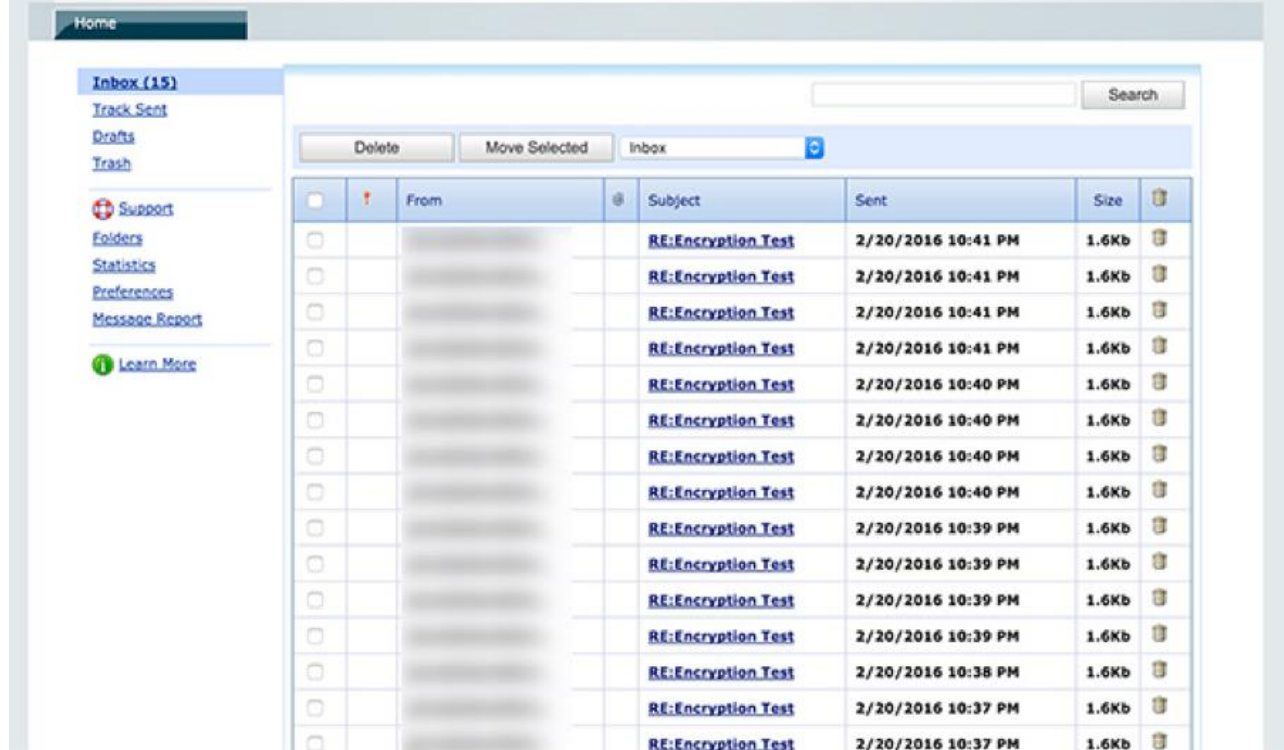
While most of the web portal gripes can be easily remedied by using NeoCertified's fantastic Outlook integration, this doesn't apply to your clients. In order to respond to your secure email, your clients must be logged in NeoCertified's portal.

I have a few other small nitpicks about the design—but that's all they are. Nitpicks.

You're not looking for a pretty interface. You're looking for a secure way to communicate with your clients. You're looking to be in full compliance of HIPAA and HITECH.

And what NeoCertified lacks in shine, it more than makes up for in security.

Security Specifications

HIPAA stipulates that all online communications with ePHI must use an adequate level of encryption to protect patients.

NeoCertified goes beyond adequate.

In fact, they use the same level of encryption used by governments (including the United States federal government).

All communications sent through NeoCertified's service are encrypted with AES (Advanced Encryption Standard). NeoCertified uses the most secure version of this protocol, opting for 256-bit cryptographic keys. In simple terms, the longer a cryptographic key, the harder it is to hack it. And NeoCertified uses the longest key-length available.

To secure the digital interaction between your computer (or phone) and their webmail application, NeoCertified uses the newest version (1.2) of the TLS protocol (Transport Layer Security). It is simply the most secure way to share information on the web available—and even giant financial institutions use it to ensure the safety of their client's online bank accounts.

NeoCertified's datacenters are SSAE16 Type II certified. Meaning that the controls and access of their physical servers are heavily monitored and stringently audited.

NeoCertified is compliant to the US government's highest encryption standards (FIPS 140).

They are also internally compliant to HIPAA's most stringent requirements, which is an absolute must for a company specializing in compliant communication.

Conclusion

NeoCertified has long legacy of providing commercial-grade encryption services for the health industry.

They are simply the best at what they do.

And although you'll be able to find slightly cheaper alternatives, few companies have a track record that can stand next to NeoCertified's. This, combined with their fantastic HIPAA compliant Outlook integration and their secure inbound email feature, makes the service an amazing value for its price.

The only reason I'm not giving NeoCertified a perfect score is the dated user interface. But this is admittedly a small gripe, given that most webmail applications geared towards organizations are equally dated (Horde, Round Cube, etc.).

If you're a covered entity looking to bring your communications into HIPAA compliance, you simply can't go wrong with NeoCertified.

Interview - 4 Questions To Get To Know Them Better

1) Why should people choose NeoCertified for their HIPAA compliant email solution?

People should choose NeoCertified because of our unparalleled level of 24/7 customer support, which is available for both paid users and their recipients. Also, our security methods have been proven for over a decade without incident.

2) On your site you mention you are the number one trusted secure email solution company since 2002. Can you give some example of how this will benefit a customer?

The client or paid user needs to understand how their information is protected, but more importantly, that their information will be protected in its entirety for years to come. We are an established security company that has paved the way for secure email for nearly two decades, and will continue to do so.

3) To what extent can you help a customer become HIPAA certified?

We can ensure that the NeoCertified Subscriber is compliant with all HIPAA related requirements (164.312 a-e) for secure email, in less than one business day (usually within an hour), with virtually no training.

4) How does the sales process work, what happens after a customer has signed up with your email solution, how long does it take before a customer can have its HIPAA solution up and running?

After receiving their user list, which includes first & last name and email addresses, our team begins initiating each individual account, which comes with an assigned Microsoft Outlook plug-in unique to their name. Our turnaround time varies depending on the size of the client, but generally, a new user list can be registered and set up within an hour. We always guarantee at most one business day for any size user list and account.

Thank you NeoCertified for this interview!

And this concludes this NeoCertified review. If you have additional questions, please leave them in the comment section.

Full disclosure: This is a paid review performed by an independent writer, according to our [guidelines](). No additional edits were made to this review by NeoCertified before it was published.

Review Overview

Pricing level - 95%

Extra services included - 100%

Level of support - 100%

NeoCertified scores high point on both services included and level of support, while offering all this at a competitive price.

98%