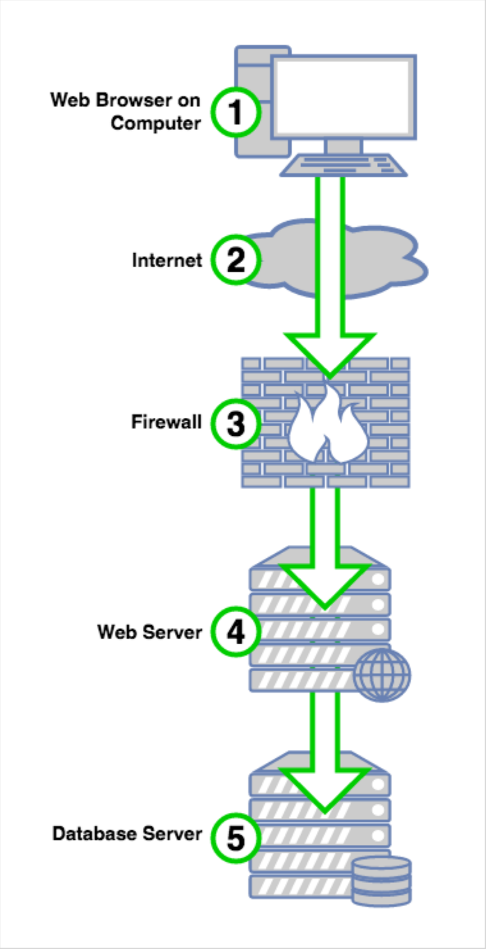
Itemized Statements Data Security

The diagram to the right displays the steps of submitting data to the Itemized Statements web application. Below is a description of each of these steps.



1. All of the web pages are loaded over a TLS encrypted connection. Access to the software requires a username and password. The software requires strong passwords (minimum length, includes an uppercase letter, includes a number, and includes a symbol) and a password must be changed every 4 months.

2. When a user sends or receives data it is transmitted over the internet over an encrypted TLS connection. The Requestor and Staff's browser will encrypt the data before it leaves and can only be decrypted by the web server.

3. The access to the webserver is protected by a firewall. The firewall will only allow web-based traffic onto the Web Server. The firewall will also detect and block malicious web traffic.

4. The Web Server will receive the data and decrypt the web request. Then the Itemized Statements application will validate the user's session and if they are not authorized it will redirect the user to the login page. If they are authorized then the software will continue and process the request.

5. The database is located on a separate server and only internal connections are allowed to it. The web server will connect to the database server to save and retrieve data for the Itemized Statements application. All sensitive data and documents are encrypted using 256 bit AES encryption before storing them on the database.

- This process is used both for the Requestor's and Staff's interaction with the web application.
- All messages sent from the software are internal and require the user to login with their username and password to view the message. Email is used to send alerts that they have a new message, but will require them to login to the software to view the message.
- Steps 3, 4, and 5 take place at the our secure HIPAA/HITECH compliant data center.