Data Protection

All servers are isolated from each other and from outside traffic by firewalls, only explicitly allowed traffic is allowed to pass. All logins that are not https will be converted to https.

The database server is not directly accessible by users. All user access to data is done through the web server that retrieves the data from the database server through a firewall. Backups of both servers are stored off site and are transmitted over a point to point private fiber connection.

There is a 1 hour RPO (Recover Point Objective) and RTO (Recover Time Objective) protection in case of disaster. We have a Disaster Recovery as a Service (DRaaS) solution with the Data Center. With DRaaS our live server change blocks are continuously streamed to our recovery server in Indianapolis Indiana. The data is transmitted through a point-to-point dedicated private fiber cable. All data storage and transition of data inside any of facilities are HIPAA compliant, which means all data at rest or in transit is encrypted.

If there is a disaster, where users can't get access to their data, a disaster will be declared. A disaster will initiate the spinning up of the DRaaS site. Once the servers are up, user's access is directed to a recover site at an offsite location (Indianapolis).