HIPAA security statement for Clinicminds CRM/EMR

The purpose of this statement is to outline and define security measures incorporated into Clinicminds to assist Clinicminds's customers in complying with HIPAA Security Regulations. This HIPAA security statement is applicable to those customers using the Clinicminds Saas application who are a "covered entity" as defined by the Health Insurance Portability and Accountability Act of 1996 and applicable regulations ("HIPAA"). Although responsibility for HIPAA compliance primarily rests with each customer who is a covered entity, the Clinicminds application provides the following features to assist our customers in administering their own security policies and procedures to comply with HIPAA regulations:

- Activity Log: records which user made modifications to patient records, employee passwords assigned and registers which employee is logged in.

- Password protection: Clinicminds has unique username and password protection available.

    1. The password is a single password assigned to an individual that must be entered before the application and database may be accessed. The database is where all business information is stored, including clients, totals, inventory, reports, etc. The password is typically entered when starting a new session or each time the user has logged out of the application.
    2. Employee access restrictions may be applied to over fifty areas within the program. Using the User Roles (rights) function, access to the client information screen and client treatment notes, which may contain client protected health information, may be limited to those with the applicable user role or denied completely. For example, some employees may be permitted to view client protected health information upon entry of their password. However, employees who have no need to access client protected health information can be prevented from accessing the client information screen, even if they have a password that permits them access to other areas of the program. The User Roles control function may also be restricted to control access.
    3. The U.S. Department of Health and Human Services recommends that users should logoff the system they are working on when their workstation is unattended. Clinicminds offers an automatic logoff feature, which is an effective way to prevent unauthorized users from accessing client protected health information.

- Database Security: Clinicminds databases are backed-up daily to prevent possible loss of information. Due to HIPAA regulations, certain technical assistance features such as Remote acces, database conversions or data import into Clinicminds are limited available to customers who are covered entities under HIPAA.

- Data transmission: All data that is transmitted to and from the Clinicminds databases is encrypted using 2048-bit SSL connections during transmission.