



## **PsychNotesEMR Meets all HIPAA Technical Safeguards Requirements**

As stated in Volume 4 of the HIPAA Security Series

*“Technical safeguards are becoming increasingly more important due technology advancements in the health care industry. As technology improves, new security challenges emerge. Healthcare organizations are with the challenge of protecting electronic protected health information (EPHI), such as electronic health records, from various internal and external risks. To reduce risks to EPHI, covered entities must implement technical safeguards.”*

The standards guidance for these Technical Safeguards is found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). With regard to Technical Safeguards the HIPAA Security Rule outlines five areas of required compliance

1. Access Control
2. Audit Controls
3. Integrity
4. Person or Entity Authentication
5. Transmission Security

### **1 Standard § 164.312(a)(1) Access Control**

*“Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) [Information Access Management].”*

- PsychNotesEMR rides on multiple Server 2003 platforms and is accessed via over a 128 bit encrypted link. All traffic on and off the servers is encrypted and the only user access to the PsychNotes servers is via a remote terminal encrypted link. All computation is done on the server and the local computer is basically a dumb terminal.

- PsychNotes has an internal security access control system that allows each mental health to have fine control over both what each user can see and what each user can modify.

### **1.1 Standard § 164.312(a)(2)(i) Unique User Identification**

*“Assign a unique name and/or number for identifying and tracking user identity.”*

- The system administrator assigns both a user name and an initial password to each user. On first logon each users chooses their own permanent password. This password is known only to that user and it is the user’s responsibility to avoid compromise of this password. The system administrator assigns each username to a particular practice database on the MySQL Server which runs on all PsycNotesEMR Server 2003 platforms. On logon to the system the user is automatically routed to the correct mental health practice database.
- All passwords must comply with the strongest protection standards recommended for Server 2003 users. The details are that passwords much be at least 8 characters long, no full names and at least one character from 3 of the following groups: uppercase letters, lowercase letters, numbers, non-alphanumeric characters such as # or %.
- A log is maintained of all user actions within the database and this log can be used to track all user activity at virtually the keystroke level.

### **1.2 Standard § 164.312(a)(2)(ii) Emergency Access Procedure**

*“Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.”*

- All health professionals with system access could need emergency access to their own PsychNotes files. This could happen as a result of three conditions. In the first circumstance the user, for some reason, not have access to the internet and need information from the database. In the second circumstance a failure or an environmental disaster could occur which would cause the failure of the PsychNotes servers. In the third circumstance failures or an environmental disaster could occur which would cause the failure of both PsychNotes servers.
- APMS has contingency plans for all of the above circumstances. Should a server system failure occur the PsychNotes administrators can shift activity to the warm backup server. Should the warm backup server fail the administrators can use the information at the remote ftp site to restore the operation of PsychNotes.

### **1.3 Standard § 164.312(a)(2)(iii) Automatic Logoff**

*“Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.”*

- PsychNotes servers are currently set to automatically log off users after one hour of inactivity.
- The automatic logoff feature applies to both all users and all administrators.

#### **1.4 Standard § 164.312(a)(2)(iv) Encryption and Decryption (A)**

*“Implement a mechanism to encrypt and decrypt electronic protected health information.”*

- All information leaving PsychNotes is always encrypted. The data itself is protected through the complex layered structure inherent to the MySQL Server.
- All data flow is encrypted and access is protected by a strong password system.

#### **2 Standard §164.312(b) Audit Controls**

*“Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”*

- All changes to a PsychNotes database are recorded in the log file which can be read but not altered by the system users. Any user change to any record is date stamped and both the specific change and the user making the change are placed in the log file.
- Since all actions by users are recorded there is no limit to audit control of the information in the PsychNotes system.
- The audit controls as implemented allow the organization to adhere to policy and procedures developed to comply with the required implementation specification at § 164.308(a)(1)(ii)(D) for Information System Activity Review? Such policy and procedure are a matter for each individual medical practice to establish. However PsychNotes is configured to readily support any reasonable audit policy.

#### **3 Standard § 164.312(c)(1) Integrity**

*“Implement policies and procedures to protect electronic protected health information from improper alteration or destruction”*

### **3.1 Standard § 164.312(c)(2) Mechanism to Authenticate Electronic Protected Health Information (A)**

*“Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”*

- The internal security system of PsychNotes limits write access by users to only those specific records that they have write permission for. As a result it is not possible for a user to make changes which he/she is not authorized to make.
- It is not possible for a user to bypass the audit system and modify data that is held within the MySQL server since the internal data can only be accessed through PsychNotes and MySQL itself insures data integrity through its own internal consistency checks..
- The text log record insures that any changes to the database can be detected.

### **4 Standard § 164.312(d) Person or Entity Authentication**

*Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”*

- Access is limited to authorized users with passwords. Passwords must meet the strong requirements as described above.

### **5 Standard § 164.312(e) Transmission Security**

*“Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”*

#### **5.1 Standard § 164.312(e)(2)(i) Integrity Controls**

*“Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.”*

- Since all data is transmitted via encrypted links with appropriate Microsoft integrity checks in place it is highly unlikely that information between a remote user and PsychNotes could be modified in transit.
- To date analysis of PsychNotes has not detected any outstanding scenarios that could cause a problem during data transmission.

## 5.2 Standard § 164.312(e)(2)(ii) Encryption (A)

*“Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”*

- As noted above all information transmitted to remote users is 128 bit encrypted.
- With the exception of initial setup work done internally at a PsychNotes facility all information is effectively transmitted as it flows in or out of a PsychNotes database is encrypted at all time.
- Since PsychNotes is designed to support remote users encryption of data transmission is obviously essential and is applied uniformly.
- As noted above the built in Server 2003 128 bit encryption is used for all data transmission