FDA U.S. Department of Health and Human Services
Food and Drug Administration

ORA
OFFICE OF REGULATORY AFFAIRS

Mi-Forms Compliance with FDA Part 11, HIPAA

Mi-Forms incorporates many features for compliance with these rigorous standards. The following issues are relevant to FDA Part 11 (and some also apply to HIPAA):

- DBMS-level audit trails: who, what, when, and why for all changes to session data and system-level data
- Data integrity: SSL transmissions from client to server use MD5 digest algorithm to ensure data integrity
- Encryption: data sent from client to server and from server to Web client is encrypted using SSL's 128-bit RC4 encryption
- Electronic signatures (not to be confused with digital signatures) can be required by the server administrator
- Single-line strikethrough: corrections can be made on paper forms with a single-line strikethrough, so that the original value is not obscured
- Data export: all data can be exported via the Web interface into simple, easy-to-parse CSV files
- Audit trail export: audit trails can be exported via the Web interface into simple, easy-to-parse CSV files
- Easy identification of records with audit information: the Web interface flags all session data which has been modified so that an analyst can find them quickly; in addition, a search mechanism allows for filtering on this criterion
- Unique and permanent electronic signatures: user IDs are never reassigned or destroyed in Mi-Forms. Even if a user account is closed, the user's information remains in the system so that auditing information remains intact
- Password aging: the administrator can control the lifespan of passwords for his users
- Password secrecy: passwords are stored in encrypted fashion and are not available in plaintext to any user, including the administrator
- Intrusion detection: logfile analysis sends alerts to the administrator when suspicious activity is detected
- Configuration change tracking: as forms in the system are updated and distributed to client software, a record of all revisions is maintained

The following issues are germane to HIPAA:

- Control user access to software code: forms stored on the client are encrypted with 128-bit RSA encryption to prevent tampering. If such a file is altered, it will be unreadable by the system. Client and server applications themselves are compiled code, which would be extremely difficult to alter in a meaningful fashion. Access to the server is strictly controlled.
- Uniform distribution of updates to clients: an automatic version control system built into Mi-Forms makes sure that clients have the latest versions of forms. Timed form releases allow for synchronized updates, even in environments where clients are not 100% connected.

Mi-Co