

Memo of Meeting

Date: July 12, 2002

Representing IntraLinks, Inc.:
1372 Broadway, N.Y., N.Y. 10018

Edward Martin, Vice President, Product Management
Richard Jenkins, General Manager, Life Sciences
Mylers T. Trachtenberg, Chief Technology Officer

Representing SEC Associates, Inc.
3900 Paramount Parkway, Suite 150 South
Morrisville, NC 27560

Ms. Lisa Olson, Principal Compliance Consultant

Representing FDA:

Charles Snipes, Compliance Officer, Center For Drug Evaluation and Research
Jeff K. Smith, Team Leader/Project Manager; Center For Biologics Evaluation
and Research
Tom Chin, Consumer Safety Officer, Office of Enforcement
Paul J. Motise, Consumer Safety Officer, Office of Enforcement

The meeting was held at the request of the IntraLinks representatives, to discuss their digital workspace services offered to FDA regulated industries (in particular establishments performing clinical trials) in the context of 21 CFR Part 11. At the start of the meeting we explained that FDA does not formally review, approve or disapprove of products or services that enable people to comply with FDA regulations. We advised that the meeting would be an information exchange and that our comments should not be taken as formal FDA positions.

The IntraLinks representatives described themselves as an application service provider to life science and financial industries. Less than half of their customers are regulated by FDA. The firm provides a third party web based platform for sharing confidential information. They host clinical trial electronic records on the firm's servers. However, clinical investigators retain copies of those electronic records locally.

The IntraLinks representatives explained the general configuration of their service as hub based in which access to various records and system resources can be restricted according to pre-defined user roles. Users can post any binary

attachments to the digital workspace. The system works in conjunction with Oracle database software. Transmissions are encrypted via the secure sockets layer protocol.

Operators are identified by electronic signatures based on identification codes in combination with passwords. During the meeting we discussed password security controls. The system requires that operators use passwords having a minimum of 8 case sensitive characters, with no character repeated more than three times and with at least one number and one letter required in the password string. Passwords expire after 90 days and cannot be recycled for 12 months. The system disconnects a user upon three consecutive log on failures.

Electronic signatures in electronic records are manifest in their human readable forms by display of the signer's printed name, date/time of signing and what the signature means.

During the meeting we discussed the system's audit trailing features. The system's audit trail records who (by operator's printed name) posted (wrote), modified or deleted what electronic records and the date and time (Eastern, U.S. time zone) of those actions. The system retains copies of electronic records that operators delete. The audit trail is retained in the digital workspace on the firm's server and cannot be altered by operators. The system also records who accessed system records.

For backup purposes the firm maintains off site tape storage at two geographically dispersed facilities.

During the meeting we discussed the firm's validation efforts. The representatives said they would welcome, and have undergone, customer audits of their software development activities.

The meeting lasted about two hours.

cc:
FDA Attendees
HFA-224
Part 11 Guidance Dockets

Doc ID IntraLinksMemoOfMeeting071202.doc
P. Motise 08/14/02