



www.oceanasensor.com

CROs and Data Element Security (Fortress Secure Interface®)

The Challenge

All businesses and industries have spent billions of dollars over the past two decades attempting to secure their information networks, Internet connections and valued corporate information. Most have succeeded in building very large walls around their information infrastructure but have failed in their attempt to secure all of their important data. General regulatory initiatives have presented a new set of requirements to address. HIPAA, Sarbanes-Oxley, California SB 1386 and NASD 2711 to name a few have established a more rigorous challenge to protect the information rather than just the IT platform. The new enhancements to HIPAA regulations "Federal data breach notification rules for entities covered by the Health Insurance Portability and Accountability Act (HIPAA) took effect November 30, 2009." The move significantly expands the exposure those entities face when personal health information gets loose. The new rule has a broader scope because it applies the breach notification rules to "business associates" of covered entities," (Association of Clinical Research Organizations). Clinical Research Organizations (CRO) have dealt with regulatory issues with their customers for years. Beginning with product development, formulation and manufacturing; clinical trial management (preclinical through phase IV) through clinical, medical and safety monitoring; preclinical, toxicology, and clinical laboratory, data management and biostatistics securing the data collected is extremely important and confidential.

A **data element level security** platform is a fundamental need to meet these regulatory needs. It assures compliance, enforces employee behavior to support compliance and allows security policies and procedures to be implemented within IT systems rather than protecting the exterior of these systems.

Impact of Data Element Level Security

The data element security model reduces the need for human judgment and behavior in setting security policy. Software can initiate and automate the process of making decisions at the data element level for each level of employee, customer or regulatory agency. Software decides whether a Clinical Research Analyst should see the same data as a physician or the end customer. Each user can use the same system and see the same screen with sensitive data elements blocked out based on their role or responsibility. The model captures the CROs

existing practices and anticipates situations that will arise in a fully networked collaborative environment. This innovative approach represents a breakthrough solution for on-line data security with protection of intellectual property and confidential information from internal and external attack. This powerful combination of data security and the ability to tailor applications exists today as Fortress Secure Interface®. It provides data element level security based on roles and responsibilities to the CRO in the following areas to name a few:

- Detailed CRF Design and Review
- 21 CFR Part 11-Compliant Systems
- Double-Data Entry protection
- IRB Submissions
- Electronic Data Capture
- Data Validation
- Protocol Development and Review
- Electronic Data Integration and Transfer
- Assurance of Sponsor Confidentiality

Generally, the Fortress Secure Interface® system was designed with the following attributes:

- State of the art security functionality that is easy to use and addresses the organization's need to protect key assets of intellectual property, customer information, personnel data and business process logic,
- An architecture that supports protection of dynamic and static data sources
- A secure interface between external clients and proprietary or sensitive application information, which the products protect.
- A secure application that is FIPS 140-2 certified by the federal government (NIST)
- Scalable solutions that can accommodate terabytes of data and hundreds of users
- A rapidly deployed solution that takes only days to implement
- Integrates with a wide range of applications, databases and software tools.
- Products that are hosted on networks, one or more PCs and storage hardware devices