

Secure Information Sharing for Healthcare, Pharmaceutical, Life Science

Regulatory compliance and manageable data governance for the healthcare industry

Information exchange: Confidentiality is key

Healthcare providers and pharmaceutical companies have to handle an ever-increasing amount of confidential information. For healthcare providers, the main concern is the proper handling of patient information in accordance with regulations, while for pharmaceutical and life sciences companies, protection of confidential information from competitors also plays a critical role.

Regulatory compliance: HIPAA, HL7 etc.

Healthcare providers have to deal with an ever-increasing security-related regulatory burden (e.g. HIPAA, HL7) and a need to govern and audit flows and usage of sensitive data (mostly patient-related). Strong security needs to be demonstratively implemented across a highly complex, interconnected IT landscape that comprises many stakeholders, many legacy systems, and frequent system changes. Cost-effective, agile, low-risk security policy management is a critical aspect in the overall picture.

Growing IT landscapes add complexity

Healthcare providers, pharmaceuticals (and in fact most other large organizations) are currently struggling to contain the cost of their more and more complex, interconnected, and business-critical IT environments. In some cases, Service Oriented Architectures (SOAs), process-centric architectures (BPM), as well as data-centric technical IT architectures (e.g. DDS) are all being deployed alongside more traditional application integration platforms such as JavaEE, JMS, CORBA/CCM. On the business end, best practice frameworks such as COBIT and ITIL are implemented

Managing data governance and regulatory compliance in these complex business and IT environments is a challenge, and so is achieving alignment between business and technical security compliance, privacy, and confidentiality.

Information Security: A Critical Enabler

Information security is the main technical means of implementing technical security solutions to meet these challenges.

While implementing a good solution can be costly, the effort and challenges need to be seen in comparison to the much higher cost of not adopting them, resulting in loss of competitive advantage and exploding IT procurement and maintenance costs. Without the right technology in place, security policy management can be one of the main cost factors



ObjectSecurity OpenPMF lets you intuitively select business-centric security & compliance policies, which are then automatically enforced across your IT landscape (using a "model-driven security" approach). You can conveniently manage your policies at run-time, and even change your software applications and workflows without extra administration. OpenPMF reduces costs, improves security, and enables agility. Available as a packaged product and as an integrated turn-key solution.

Products & Services

- OpenPMF (packaged product & turn-key solution)
- SimulateWorld 4D synthetic environment toolkit
- SecureMiddleware: secure open source middleware
- Services: security policy management, Web 2.0 / SOA / Cloud / SaaS Security, middleware security, training workshop, tech. support, R&D
- Studies: in-depth documents about hot topics in security, e.g. model-driven security & SOA

www.objectsecurity.com