

Seclore for the Pharma Industry

How Pharmaceutical companies can secure their confidential data - with no overheads and side effects

The Pharma sector spends more on research than any other industry, according to a KPMG report. The industry has been on the defensive for the past decade - with rising costs resulting from pricing pressures, higher litigation exposure, complex regulatory environments, and generic competition.

Loss-making business units are being sold off and all non-core functions are being outsourced. And all this massive outsourcing is accompanied by the equally massive exchange of information across borders – both organizational and national. Years' worth of research and hard work is being shared on a platter with zero security and systemic safeguards

With so much money being spent on R&D in a world of rising costs, it becomes critical for Pharma firms to ensure the security and safety of their IP. Your traditional IT security infrastructure is unable to secure your data once it crosses your network boundary. To secure such data, you need a data-centric security solution, something that remains effective even after data crosses your firewall. This means you can secure information wherever it goes in your supply chain and global networks

Seclore's Enterprise Rights Management (ERM) is being used by numerous pharmaceutical companies to persistently secure their sensitive information. A few customer success stories where Seclore has offered unique advantages are described below.

Customer Drug Formulation and Manufacturing Data:

API (Active Pharmaceutical Ingredient) manufacturers receive highly confidential details regarding drug formulation and manufacturing from customers. These documents are then freely circulated amongst various internal teams: Technology, R&D, QA, Production etc. This information is highly critical and API manufacturers would incur heavy penalties and legal liabilities – not to mention reputational damage and loss of competitive advantage - if it is compromised

Using Seclore's ERM solution, files are protected as soon as they are received from the customer. Predefined permissions are defined for each user within the organization that wishes to access the information. Thus, using Seclore's ERM solution, API manufactures are able to successfully ensure that customer data remains safe and secure throughout the entire lifecycle – and also monitor all activities being performed on the documents.

R&D Guidelines for Manufacturing:

Major Pharmaceutical companies regularly send confidential R&D guidelines to manufacturing units, which combine this information with the BOM (Bill of Material) and share them with the Quality Assurance, R&D, and PRC (Product Registration Cell; a part of Regulatory Affairs) teams. Since so many different

employees possess this information, chances of data leakage are extremely high. This information is key IP critical to the manufacturing process and could seriously erode competitive advantage if leaked.

Seclore can protect this information right at the source – before it is sent to the Manufacturing units. User access permissions on the documents can be easily mapped with information flow across different teams. This ensures that the additional security does not interfere with normal business workflows and user experience.

Trade Schemes:

Marketing teams create quarterly sales forecast data on the basis of market trends, new product launches, and other similar information. To meet these numbers, the Trade Marketing Manager develops various schemes for retailers and distributors, which contain specialized incentive plans for field agents. The schemes are vetted by Marketing, Finance, and the senior management for budgetary approvals and subsequently shared with the field teams. They go through numerous iterations with several departments before they are finally launched to distributors and retailers. This highly sensitive data can be leaked at any stage by any employee – since the file sharing and access is completely insecure and unmonitored.

With Seclore, the organization is able to ensure that only authorized employees get access to the documents, and that

all access is fully monitored by the information owners as well as IT.

Marketing Information:

Marketing teams of API manufacturers generate large amounts of sensitive information, which they regularly share with senior members of internal departments such as Production, R&D, Regulatory, Finance as well as the senior management. Much of this information directly influences or is related to company strategy. For example, the sales forecast for a particular product is shared with the Product Brand Managers, R&D, Production, and Finance. Contract agreements are shared with the Legal and Regulatory departments.

With Seclore, all this information is protected by the Marketing team – by simply dragging and dropping the respective files into special designated folders based on the recipient department. Files get automatically – and permanently – protected with predetermined policies as soon as they are dropped into the folders. This ensures that information cannot be misused – and also ensures that unnecessary user overheads are negligible.

USA – West Coast

691 S. Milpitas
Blvd.#217
Milpitas CA 95035
1-844-473-2567

USA – East Coast

420 Lexington Avenue
Suite 300,
Graybar Building
New York City
NY 10170

India

Excom House Second Floor
Plot No. 7 & 8,
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072

+91 22 6130 4200
+91 22 6143 4800

Gurugram

+91 124 475 0600

Singapore

Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton
Way
Level 34-01
Singapore – 068811

+65 8292 1930
+65 9180 2700

Europe

Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 151 1918 5673

UAE

Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

Saudi Arabia

5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

