



SAFLINK HELPS LIFE SCIENCES COMPANIES WITH FDA COMPLIANCE

SAFLINK's biometrics-based authentication solution delivers a one-two punch: it streamlines regulatory compliance with FDA regulations and increases manufacturing efficiency.

INTRODUCTION

Pharmaceutical and other life sciences companies find themselves in an increasingly difficult IT environment. Not only do they face the same business challenges found in any large enterprise, from newer federal regulatory initiatives such as the Sarbanes-Oxley Act of 2002 to more general concerns of network security, infrastructure efficiency, and protecting intellectual property – they also face specific oversight by the U.S. Food and Drug Administration. In particular, FDA's 21 CFR Part 11 requires that life sciences companies must have specific controls in place to ensure the authenticity, integrity and confidentiality of electronic records and software, preventing their unauthorized modification or destruction. Non-compliance can result in heavy fines and even the possible delay or removal of products from the market.

According to IDC, a leading market research firm, the life sciences industry will spend upwards of \$6 billion per year on regulatory requirements related to Part 11 compliance. The key aspect of these requirements relates to security. Specifically, Part 11 compliance ensures that systems and records are protected from unauthorized access and that individual users are authenticated before system access or modification is allowed. This security goes beyond simple access control to provide a methodology to identify and track over time exactly what changes were made and what individuals were allowed access.

STRONG PASSWORDS ARE BAD MEDICINE

As part of its compliance guidelines, 21 CFR Part 11 specifically identifies biometrics as the preferred means for ensuring authentication and confidentiality. A study by industry research firm The Meta Group notes that most companies with over \$500 million in revenue have upwards of 75 different applications in place. Typically, each user accesses an average of six of these applications on a regular basis and each application requires a unique password to ensure security. Most users have difficulty remembering one strong password (a password that is at least eight characters long and appears to be a random mix of letters, numbers and symbols), much less six. As a result, security and productivity suffers. Users frequently resort to writing passwords on Post-It® Notes or other unsecured locations, and spend more than 44 hours a year logging on to applications¹.

From an IT administration standpoint, things are even worse: users must routinely call their corporate help desk to identify new or lost passwords; passwords must be regularly changed in order to maintain security; password security must be portable across partnerships and third parties; and, when employees leave an organization, their historical password data must be strictly maintained for audit purposes. The result is a significant administrative overhead cost related purely to the maintenance of password information.

As a result, a growing number of life sciences companies are turning to the FDA's other recommendation for Part 11 compliance: biometrics.

BIOMETRICS FOR LIFE SCIENCES

Biometrics rely on unique physical identifiers, such as fingerprints or iris scans, to identify and authenticate each user. Inexpensive scanners are located at each data check-point and computer workstation, allowing rapid user access based on biometric data. This technology, at the core of biometric security solutions, provides a number of impressive business benefits:

Increased efficiency and output. Moreover, companies can actually find that productivity is improved. For instance, workers on a manufacturing floor might each need to perform 300-500 transactions requiring log-in/log-out per shift. Using biometrics, each of these transactions is authenticated in half the time associated with a typical password log-in/log-out sequence, resulting in a significant increase in efficiency. This efficiency translates into less manufacturing and development time to market for new drugs, providing an immediate return on investment for pharmaceutical firms.

Compliance with regulations and legislation. FDA regulations dictate that individuals who are researching, testing, or manufacturing a pharmaceutical product must record their identity through a digital signature for any specific action. On the manufacturing floor, employees have to authenticate as many as 300-500 times a shift! Not only is this a hassle, but it takes time. Biometrics shorten the time required for each signature or sign-on – by as much as 50%.

Protection of intellectual property. According to an ASIS study, Trends in Proprietary Information Loss, the average manufacturing company loses \$28 million in intellectual property due to computer security breaches. With biometrics, you can lock out vulnerabilities exposed by traditional text-based passwords.

Reliable audit capabilities. Biometrics provide the ability to track individual logins, documents, and application use. Our software integrates thoroughly with popular applications like Microsoft® Active Directory™ and Novell® NMAST™, integrating biometric audit logs with your existing audit functionality. The use of biometrics eliminates passwords, and absolutely authenticates each individual user before granting network access, eliminating password sharing or unauthorized access.

Lower IT costs. At the corporate level, the benefits are far more substantial. From an administrative standpoint, biometrics eliminates the costly overhead associated with managing and maintaining an extensive set of passwords, along with the help desk support associated with forgotten log-in information.

Insurance against liability. There is a host of new business legislation which has resulted in serious fines and jail time for executives who fail to secure customer data. Companies are legally required to disclose any breaches in security where customer data might have been compromised – a PR nightmare. Biometrics is an inexpensive insurance against this liability, because it keeps unauthorized users from stealing or hacking passwords, and can irrefutably prove who was accessing which data at what time.

SAFLINK AND LIFE SCIENCES: REAL WORLD EXPERIENCE

SAFLINK, one of the leading providers of biometric technology, is working with a number of pharmaceutical and other life sciences companies to install Part 11 compliant security solutions, from office environments to plant floors.

For example, SAFLINK is currently working with one of the world's largest pharmaceutical developers to deploy a biometric system on the manufacturing floor for a billion-dollar drug. In this particular installation, the manufacturer is updating its non-password-protected on-floor workstations to biometrics in order to ensure Part 11 compliance. Floor operators walk up to the workstation and log in using a quick iris or fingerprint scan. Once the operator is done and leaves the machine, he or she is automatically logged out and a special "read only" mode is entered, enabling alarms and other events without granting full application access.

This particular manufacturer is so pleased with the installation that it is not only looking to expand to other plants and departments, but it is even talking with SAFLINK about potentially extending biometrics to their Laboratory Information Management Systems (LIMS), replacing the current paper logs for laboratory equipment usage with a complete biometric system.

A critical reason for selecting SAFLINK, according to this pharmaceutical company, was SAFLINK's support of more than 40 biometric technologies and devices – which in turn ensures that the company is not locked into a single solution for every installation. On the plant floor, for instance, iris scans are often preferable to fingerprint technology; the scans work through safety glasses or even clean room hoods versus fingerprints which aren't recognizable through the gloves the operators wear during shifts.

As the FDA steps up compliance requirements for 21 CFR Part 11, the IT challenges for life sciences companies such as this pharmaceutical manufacturer are steadily increasing. Biometric technology provided by companies like SAFLINK is recognized by the government as one way to get ahead of that curve, providing the data authenticity, integrity and confidentiality necessary to achieve compliance.

(Footnotes)

1 Based on a 1996 study by the Network Applications Consortium

WWW.SAFLINK.COM
(800) 762-9595
SALES@SAFLINK.COM

