VOL. 13 NO. 3 PAGES 208 www.expresspharmaonline.acom

EXPRESS PHARMA

INDIA'S FOREMOST PHARMA & BIOTECH MAGAZINE
1-15 DECEMBER 2017, ₹40

CPhI P-mec INDIA SPECIAL

OPTEL PRESENTS Pharma CXO Summit 9-10 NOVEMBER, 2017 | GOA
LEVERAGING GLOBAL TRACEABILITY FOR SUSTAINABLE BUSINESS AND GROWTH
EXCLUSIVE COVERAGE INSIDE


CIPLA


RUSAN PHARMA


SHANTHA BIOTECH


ZIM LABS


INDOCO REMEDIES


EISAI, INDIA


GLENMARK

KUDOS FOR EXPORT EXCELLENCE

Express Pharma Export Excellence Awards 2017 celebrates the success of Indian exporters at Pharma CXO Summit attended by leaders and veterans of India Pharma Inc

Save time and protect data integrity with fingerprint authentication

Aditya Marfatia, Director, Electrolab and **Dr Neelam Sayed**, Application Scientist, Electrolab give an insight about how Electrolab with a technological collaboration has introduced a convenient 21 CFR part 11 compliant operating system, integrOS

Dr Neelam Sayed

Aditya Marfatia

EACH CONSUMER expects the drugs they consume to be safe and effective. To ensure safety, efficacy and quality of drugs, regulatory bodies such as US FDA, UK MHRA and Indian FDA have set regulatory standards, typically referred to as Good Manufacturing Practices (GMP). GMP assures proper design, monitoring and control of manufacturing processes and facilities for various systems. This is supported by underlying data records to trace manufacturing processes, which can prove evidence that the drugs have been manufactured as per agreed protocols.

Data integrity affirms that complete, consistent and accurate data records are attributable, legible, contemporaneously recorded, original or a true copy and accurate (ALCOA). It refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle, including the usage of any system which stores, processes, or retrieves data. Ensuring data integrity means protecting original data from accidental or intentional modification, falsification, malicious intent (fraud), or even deletion (data loss). Considering that raw data acts as an evidence that drugs are safe, efficacious and manufactured as per appropriate quality standards required, violation of data integrity is considered to be grave by

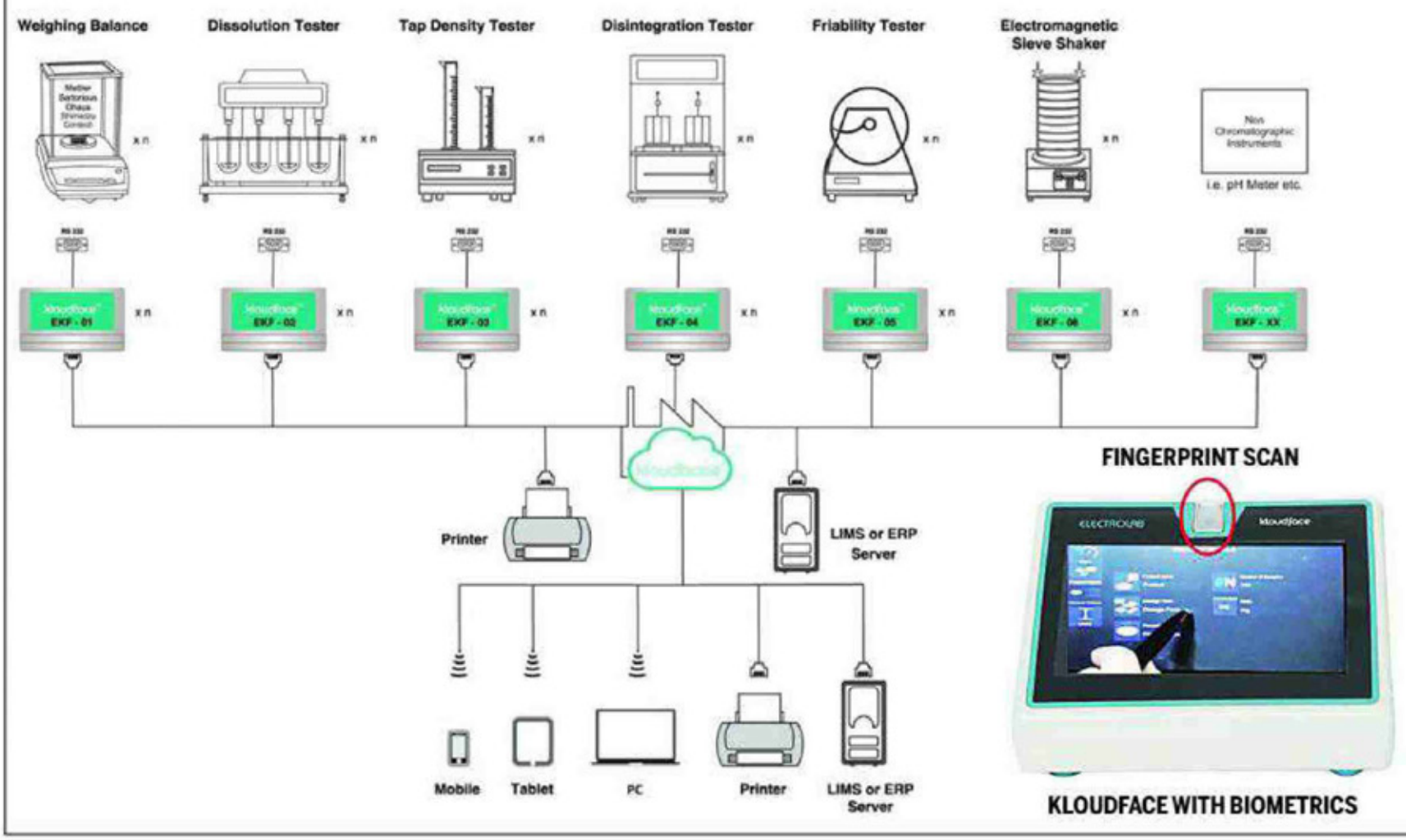
leading regulators such as the US FDA, UK MHRA, Health Canada, Therapeutic Drugs Administration (TGA) and Indian FDA, all of which mandate data integrity.

In recent years, FDA has increasingly observed CGMP violations involving data integrity during inspections. FDA inspections cite a range of serious deficiencies in how employees handle important data records and documents. FDA cites reports of records found in trash bins, data that do not match test results, unauthorised manipulation of electronic raw data, sample retesting to achieve desired results, deletion of undesirable results, practice of performing trial injections for HPLC analyses prior to running the release and stability tests etc. Some of the key root causes for these violations are lack of awareness, shortage of manpower, quantity over quality approach and ineffective training. These data integrity-related CGMP violations have led to numerous regulatory actions, including warning letters, drug recalls, import alerts and consent decrees. These regulatory actions not only impact the existing revenue stream of the company, but also affect the drug maker's ability to get approval for new drug applications. In addition, it also causes reputational damage, competitive disadvantage and lengthy remediation process that tend to consume time, money and often loss of talent. Data integrity is critical to regulatory compliance and hence the fundamental reason for formation of Code of Federal Regulations (CFR).

A company's SOP describes how processes are to be performed while manufacturing a particular drug or formulation. During implementation of these processes, the US FDA registered company needs to comply with Title 21 of CFR – Part 11, commonly known as '21 CFR 11'. 21 CFR Part 11 establishes the criteria under which electronic records and signa-

FIG.1: THE KEY PILLARS OF 21 CFR PART 11 COMPLIANCE

FIG.2: INTEGRATION OF INSTRUMENTS WITH KLOUDFACE WITH INTEGROS



FDA Warning Letter Excerpt, 2015 states "Access to production equipment used in parenteral manufacturing and solid (b)(4) dosage forms used a password shared by four or five individuals to gain access to each individual piece of equipment and access level. During our inspection, your Executive Production and QA manager confirmed that the password was shared. Neither your operators nor your supervisors had individual passwords."

Why is FDA concerned with the use of shared login accounts for computer systems?
US FDA in its draft guidance states "You must exercise appropriate controls to assure that only authorised personnel make changes to computerized MPCRs (master production and control records), or other records, or input laboratory data into computerised records and you must implement documentation controls that ensure actions are attributable to a specific individual. When login credentials are shared, a unique individual cannot be identified through the login and the system would thus not conform to the CGMP requirements in parts 211 and 212. FDA requires that systems controls, including documentation controls, be designed to follow CGMP to assure product quality".

tures are stored and is considered trustworthy, reliable and equivalent to paper records by the US FDA. Part 11 has a total of 19 requirements, some of them are specific to Part 11 and others are more generic requirements of some or all FDA regulations. The key pillars of 21 CFR part 11 compliance is depicted in Fig.1.

It is crucial to pay particular attention to all these requirements when addressing data integrity. Due to lack of thorough understanding of 21 CFR aspects, pharmacists and even instrument manufacturers may believe a system is 21 CFR part 11 compliant however; gaps may still exist which when highlighted by auditors can lead to detrimental effects.

Some of the commonly observed issues that lead to breaches in data integrity include no correct administrator rights for laboratory system (72 per cent users in QC department have IT administration rights), sharing of login IDs and passwords for laboratory systems (33 per cent), audit or reviews not being conducted to assess potential gaps in assurance of data integrity (33 per cent), unawareness about 21 CFR Part 11 compliance requirements (25 per cent), disabled audit trails on lab equipment (21 per cent) and no clearly documented SOP on backup and deletion of laboratory data (13 per cent) (Analysing the state of data integrity compliance in the Indian pharmaceutical industry, EY). Amongst all the above concerns, sharing of login credentials for laboratory systems is a common issue cited by FDA in its observations.

Primarily, sharing of login credentials are done to streamline remembering multiple passwords for multiple instruments and for cost saving reasons when softwares are licensed on a named user model.

In a convenience focussed world, making compliance convenient would minimise deviations from good laboratory practices. Users, especially in regulated industries need solutions that minimise the time personnel are spending on compliance activities while ensuring that they are still in compliance. To ensure complete 21 CFR part 11 compliance and to overcome all the hassles listed above while also better securing the organisation, Electrolab with a technological collaboration has introduced a convenient 21 CFR part 11 compliant operating system, integrOS. integrOS has a secure authentication method that utilises fingerprint authentication to register a user on the system. Biometrics is usually a quicker process than entering a username and password and far more secure than using login credentials. Biometric technology eliminates employee downtime due to forgotten passwords and also reduces the amount of IT support required to reset accounts. An audit trail with classification of events based on user, date, creation/modification status in integrOS aids with compliance and assures that no alterations have been made post approval. Managing paper and complying with regulatory policies can be tedious, while integrOS allows more efficient use of time in the lab or on the plant floor. kloudface is an interface which allows existing installed base of instruments to use integrOS and achieve convenient compliance, hence optimising capital investment. Instruments that can be integrated with kloudface with integrOS are depicted in Fig.2.

Data integrity software integrOS, fulfills CFR requirements in terms of multi-level security, unlimited users, user defined privileges, audit trails, accurate and complete copies of records, authority and device checks, linking of electronic signatures etc. Utilising integrOS with biometrics in the manufacturing process and laboratories can help to remain compliant, operate more efficiently and receive faster approvals.

Contact details:
Electrolab
Email: sales@electrolabgroup.com
Website: www.electrolabgroup.com
Tel: +91-22-4041 3131/ +91-22-41613122