

Regulatory Compliance for India

Companies doing business in India must be aware of important compliance regulations that impact how business information is governed, secured, and archived. Some of these important regulations that you need to comply with are listed below.

Retain Unified Archiving at a Glance:

- + **Unified archiving:** Email, social, and mobile communication archiving in one central location
- + **Built-in eDiscovery:** Retain Unified Archiving includes powerful eDiscovery tools, at no additional cost.
- + **Compliant archive:** Retain Unified Archiving meets regulatory standards for archiving, including; WORM storage, granular retention policies, eDiscovery, exporting, full auditing and logging capabilities, archive access control, and encryption.
- + **Archive search:** Retain Unified Archiving features a "Google" like search tool for quick and easy searches.



Regulations and Guidelines for Governmental Agencies

2011 INDIAN PRIVACY LAW

On April 11, 2011, India's Ministry of Communications and Information Technology notified the Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 under the Information Technology Act, 2000. India now has a privacy law, brought into force with immediate effect with wide ramifications on the way companies will do business in India. This client advisory provides a description and review of the new law.

In 2008, the IT Act was amended to introduce the following:

1. A new civil provision prescribes damages for an entity that is negligent in using "reasonable security practices and procedures" while handling "sensitive

personal data or information" resulting in wrongful loss or wrongful gain to any person.

2. Criminal punishment for a person if (a) he or she discloses sensitive personal information; (b) does so without the consent of the person or in breach of the relevant contract; and (c) with an intention of, or knowing that the disclosure would cause wrongful loss or gain.

For more information, please visit this link:

www.outsourcing-law.com/2011/07/2011-indian-privacy-law/

THE PUBLIC RECORDS ACT, 1993

This act regulates the management, administration and preservation of public records of the Central Government, Union Territory Administrations, public sector undertakings, statutory bodies and corporations,

commissions and committees constituted by the Central Government or a Union Territory Administration and matters connected therewith or incidental thereto. This act also states that the Central Government shall have the power to coordinate, regulate and supervise the operations connected with the administration, management, preservation, selection, disposal and retirement of public records under this Act can be. The Public Records Act can apply to government correspondence via email, social media, and mobile communication data, since this communication can be part of the public record.

http://nationalarchives.nic.in/writereaddata/html_en_files/html/public_records93.html

THE FREEDOM OF INFORMATION ACT KNOWN AS “RIGHT TO INFORMATION ACT” IN INDIA

An Act to provide for setting out the practical regime of right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability in the working of every public authority, the constitution of a Central Information Commission and State Information Commissions and for matters connected therewith or incidental thereto.

<http://rti.gov.in/webactrti.htm>

RETENTION AND DISPOSAL OF PUBLIC RECORDS INDIA

This regulation details the requirements for preserving records. It states that certain records and correspondence be kept for 5 to 35 years, depending on the nature of the record. This regulation can apply to correspondence in the form of email, social media, and mobile communication data.

www.mca.gov.in/Ministry_hn/actsbills/rules/DoRitOotRoCR2003.pdf

ELECTRONIC TRANSACTIONS ACT IS A PART OF INDIAN IT ACT 2000

Chapter 7 of Section 1: Retention of electronic records

Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if—

- a. The information contained therein remains accessible so as to be usable for a subsequent reference;
- b. The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
- c. The details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

- 1. Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

<http://meity.gov.in/content/view-it-act-2000>

COMPANIES ACT 1956, AMENDED IN 2013

Sec 260(point 2): without prejudice to the provisions of sub-section (1), the company

administrator may cause to be prepared with respect to the company—

- a. a complete inventory of—
 - i. all assets and liabilities of whatever nature;
 - ii. all books of account, registers, maps, plans, records, documents of title and all other documents of whatever nature;

Whoever violates the provisions of this Chapter or any scheme, or any order, of the Tribunal or the Appellate Tribunal or makes a false statement or gives false evidence before the Tribunal or the Appellate Tribunal or attempts to tamper with the records of reference or appeal filed under this Act, he shall be punishable with imprisonment for a term which may extend to seven years and with fine which may extend to ten lakh rupees.

Sec 402: All the provisions of the Information Technology Act, 2000 relating to the electronic records, including the manner and format in which the electronic records shall be filed, in so far as they are not inconsistent with this Act, shall apply in relation to the records in electronic form specified under section 398.

www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

“We were looking for a solution that archives in accordance with current retention laws—Retain fulfills all our internal and the external compliance regulations!”

STEFAN VETTER
Tax Counsellor & Partner
Rieker - Alber - Thoni

**INDIAN MEDICAL COUNCIL
(PROFESSIONAL CONDUCT, ETIQUETTE
AND ETHICS) REGULATIONS, 2002
(CODE OF ETHICS REGULATIONS, 2002)**

The Medical Council of India (MCI) Code of Ethics Regulations sets the professional standards for medical practice.

Security

- **Confidentiality:** Physicians are obliged to protect the confidentiality of patients including their personal and domestic lives, unless the law requires their revelation, or if there is a serious and identified risk to a specific person and / or community or notifiable disease.
- **Digitization of records:** Efforts should be made to computerize medical records for quick retrieval.

Disclosure

- **Disclosure of prognosis:** A contradictory clause requires physicians to ensure that the patient, his relatives or his responsible friends are aware of the patient's prognosis while serving the best interests of the patient and the family.
- Disclosure of a patient's prognosis should rest with the patient and not the medical attendant.

Purpose Limitation

- **Data Retention:** Physicians must maintain the medical records of their patients for a period of three years. Failure to maintain medical records for three years and/ or refusal to provide medical records within 72 hours of the request constitutes professional misconduct rendering the Physician liable for disciplinary action.

Access and Correction

- **Access to records:** Patients, authorized attendants or legal authorities can request for medical records, which have to be issued within 72 hours.

<http://cis-india.org/internet-governance/health-privacy.pdf>

India Is Still a Country Deprived of Strong HIPAA Compliance

HOW DOES RETAIN UNIFIED ARCHIVING ADDRESS REGULATORY CONCERNS?

Multi-Platform Unified Archiving: All messaging data, including email, social media, and mobile, is archived into one unified data archive. This gives you the ability to search, publish, and perform eDiscovery from one central location.

Policy-based Archiving: Retain™ Unified Archiving provides fully configurable policies that allow you to define the Exchange email messaging data you want to archive. These policies allow you to define what is archived based on mailbox type, message source, item type, message status, the age of the message, and attachments.

Compliance and Control: The standard archiving functionality of email systems lack critical capabilities that can put your organization at risk for data loss and compliance violations. Retain Unified Archiving solves this problem by disabling auto-purge, supporting SmartPurge, allowing for archive policy control, supporting export to PDF, allowing archived messages to be restored to the inbox, allowing for redaction on exported messages and prohibiting message alteration or deletion. These features help ensure your data archive is complete and compliant.

Social Media Archiving and Oversight:

Micro Focus® Retain Social provides archiving and, monitoring of Facebook, Twitter, LinkedIn, Instagram, Flickr, Pinterest, Google, YouTube and Vimeo.

Mobile Communication Management:

Retain Mobile delivers secure, encrypted messaging and archiving for iOS, Android and BlackBerry devices. This solution is for organizations that utilize personal employee and corporate devices to generate and consume business data, while meeting regulatory and compliance requirements. Retain Mobile archives SMS/MMS, BBM Protected and phone call logs for Android, and BBM, BBM Protected, PIN, SMS/MMS and phone call logs for BlackBerry. Additionally, Retain Mobile archives all encrypted SMS/Text messages and dedicated business phone number data for iOS and Android, via the secure communications server, as well as BBM Protected.

Web Access Archive Viewer: Only Retain Unified Archiving offers an easy-to-use browser-based interface with powerful search tools that let you quickly access, search, and perform eDiscovery on the archive.

Complete Export Functionality: Export the data easily into either PST, PDF or stand-alone archive viewer formats. The exported file is fully indexed, searchable, and includes a table of contents for quick browsing.

Redaction Control: Exported data can be redacted, ensuring that personal information, or other redacted items do not become part of the open records request.

Retain Unified Archiving helps you stay compliant with the regulations that affect your organization, but it does more. Retain Unified Archiving also helps you manage data, increase email system performance, and maintain oversight of communication data.

www.microfocus.com

Litigation Hold: To protect email that may potentially be involved in future litigation, Retain Unified Archiving can flag an archived item to protect it from deletion or actions until the hold is removed.

Audit Trail: Retain Unified Archiving creates a searchable audit trail of all administrators and users who have permission to search the archive, enabling you to have a record of all activity.

Message Tagging: Administrators and end users can create custom and confidential tags for messages within the archive. These tags are searchable for easier eDiscovery.

Intelligent Archiving: Retain Unified Archiving offers intelligent, granular archiving by taking advantage of the Microsoft Recoverable Items Folder, or by using EWS impersonation, archiving is not limited to journaling. Retain Unified Archiving can also archive via journaling, if required.

Configurable Permissions: Grant users, administrators, or others access to the features and functionality of the Retain Unified Archiving system based on the roles you set.

Mailbox Management: Easily search and restore data with the Retain Web Access Archive Viewer. Give end users the ability to search, forward, print, restore, access, and view messages in their original context without administrator support.

Fast and Easy Retrieval: Retain Unified Archiving contains a built-in Lucene indexing engine or the Retain High Performance Indexing Engine (for larger deployments).

Secure Storage: Retain Unified Archiving archives messaging data with multiple layers of security. Retain Unified Archiving supports multiple databases, including MS SQL, MySQL, Postgres and Oracle. In addition to secure storage, with messages being archived using AES encryption, EMC Centera, or NetApp Snaplock storage, optional Windows server or Linux server encrypted partitions can be used. Retain Unified Archiving features native support for iCAS technology and support for WORM storage, further securing your archived data.



Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com