

CA. Balasubramaniam Udayraj Nadar
Member of the Institute

# The Chartered Accountant's Smartphone: A New Dimension of the Professional Workspace

The smartphone has become an unavoidable tool for any profession, and Chartered Accountants are no exception. The uses of a smartphone for a Chartered Accountant are not just limited to making calls and sending texts. Critical tasks like engagement finalisations, receiving client documents and one-time passwords (OTPs) for generating UDINs are also performed through a smartphone. This results in unintentional accumulation of client data on the device. Now, the issue here is that a single smartphone is often used for both personal and professional tasks. Further, if, in the unfortunate event of a smartphone getting compromised, lost or stolen, there arises a question of how professional responsibility may be prudently understood and managed in such circumstances.

## Introduction

The office dynamics of a Chartered Accountant were completely different before the widespread use of technology. The physical office was the central location for executing all the professional tasks, interacting with clients and storing physical documents. Then, with the advent of technology such as the telephone, fax, email and the computer, these dynamics have changed drastically. Communication happened much faster, documents were shared electronically, and client documents were stored on office premises and computers.

As the technology has progressed further, all such professional tasks which were once executed in the office can now be performed by a smartphone. Chartered Accountants routinely use their smartphones for delivering their professional services. It has also increased work efficiency by enabling them to execute tasks even while travelling, which was not feasible in a traditional office environment. Such a convenience has made the device an integral professional tool, often functioning as an extension of the office itself.

This increasing reliance is not merely anecdotal. As per the Telecom Regulatory Authority of India, India has over 1,266 million wireless subscribers, of which approximately 1,006 million are wireless broadband subscribers as of January 2026. These figures demonstrate that smartphones account for over 96% of handsets in use. They are deeply embedded in everyday communication and data exchange, reflecting a broader structural shift in how both personal and professional activities are conducted.

In practice, a Chartered Accountant carries a single device for both personal and professional use. As a result, it is often difficult to categorise the device as an exclusive office system. Also, using a smartphone on a day-to-day basis accumulates client data on the device, which may be completely unintentional. Like any other technology-based tool, smartphones are not entirely immune to risk. In circumstances where client data stored is accidentally exposed due to theft or the device being compromised, questions arise as to how professional accountability should be assessed.

## The Smartphone as a De Facto Virtual Office

A typical day of a Chartered Accountant consists of many professional activities like providing consultancy, attending meetings, analysis of accounts and filing returns. Before the introduction of smartphones, all such activities were restricted to physical offices. Now, with their increased use, many such activities can be completely done through smartphones. Attending video conferences, providing on-call consultancy, receiving documents like bank statements through emails for accounting and obtaining confirmation for filing returns are a few of the many activities that can be executed.

Many Chartered Accountants only use a single smartphone for professional and non-professional use. It is often considered a personal device, as controls that are implemented on the office system are never applied on the smartphone. The office server is highly controlled as it contains sensitive information about the client. Its access is often restricted, and after office hours, no one is provided access to it. But a smartphone is always on, and even

> "As per the Telecom Regulatory Authority of India, India has over 1,266 million wireless subscribers, of which approximately 1,006 million are wireless broadband subscribers as of January 2026."

after office hours, a smartphone user has access to the information stored in it. While professional activities have migrated to these handy devices, the governance and control frameworks applicable to office systems have not changed.

## Nature of Data Accumulated on a CA's Smartphone

Multiple categories of client-related data get accumulated on a Chartered Accountant's smartphone, often unintentionally, as a consequence of using the device for execution of professional activities. Personal data such as the name, address, gender, age, occupation, education, email address and mobile number are often required for registration at various compliance portals like income tax, GST or MCA. Financial data such as draft financials, authentication credentials like one-time passwords (OTPs), and professional communications are routinely shared for execution of various compliance and assessment-related activities.



Documents containing personally identifiable data like PAN and Aadhaar, draft financials and OTPs are often forwarded through instant messaging applications or email, which are then accessed using smartphones. Many sensitive professional communications are also often accessed using these devices. Also, metadata like call logs and chat history are all stored in it. Automatic backups of chats, call logs, files and application settings are stored in the cloud. As a result of automatic backups, such data is also stored with cloud service providers in addition to the smartphone, extending the data footprint beyond the Chartered Accountant's direct governance and control.

## Why Smartphones Fall Outside Traditional Office Controls

Smartphones are generally considered to be personal devices as they are protected by a user PIN or biometrics. The user of a smartphone has exclusive access to all the content stored on the device irrespective of whether such content relates to the user's own personal data or unintentionally accumulated professional data. Unlike office systems, access to which is often restricted after official hours, smartphones are typically kept active at all times. This gives unrestricted access to professional data even after official hours. Further, since smartphones are used simultaneously for personal and professional purposes and are highly mobile, professional data travels wherever the user carries the device. This highlights the limitations of traditional office governance frameworks when applied to smartphones.

Smartphones are vulnerable to theft due to their high monetary and usage value. They are also susceptible to loss due to carelessness. In such circumstances, the risk of unauthorised access or exposure extends not only to the personal data of the user but also to the sensitive professional and client-related information. This raises



significant ethical and legal questions regarding the extent of professional responsibility and accountability of Chartered Accountants for client data stored on personal smartphones.

Using a single smartphone for both personal and professional work is a recognised enterprise security problem. The Mobile Security Index Report 2025 shows that 70% of mobile devices impacted by an attack are personal, and not corporate-issued devices.

## Professional, Ethical and Legal Implications

The following discussion is indicative in nature and seeks to highlight general professional considerations. It does not purport to interpret statutory provisions or impose additional obligations beyond those prescribed under applicable laws and professional standards.

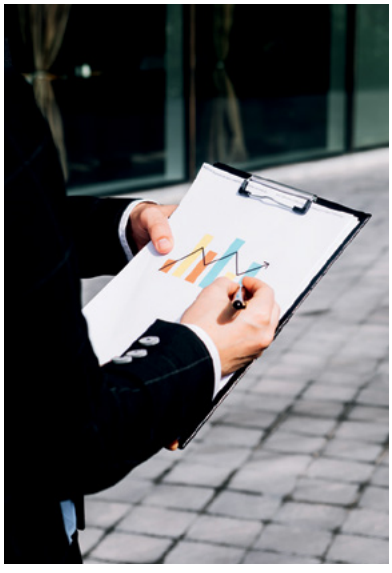
As per the Code of Ethics, Chartered Accountants are ethically bound to safeguard client confidentiality and shall be alert to the possibility of inadvertent disclosure. The obligation of client confidentiality is technology neutral and applies irrespective of whether client data is stored in physical files, office systems or a personal device like a smartphone. The Information Technology Act, 2000 requires implementing and maintaining reasonable security measures and procedures to safeguard the personal information of clients in a computer resource. A smartphone has all the functionality of a computer resource,

like emails, instant messaging and cloud backups. Further, Chartered Accountants are data fiduciaries under the Digital Personal Data Protection Act, 2023, which underscores the importance of appropriate safeguards, even where personal devices are used for professional purposes.

Reasonable security measures are contextual, risk-based and not absolute, and must be assessed in light of the manner in which the smartphone is actually used. The reasonableness of security measures for office systems may differ from what is reasonable for a personal device. Nature, volume and duration of professional data may determine the reasonableness of security measures. Smartphones are always active at all times, portable, and used for personal and professional activities. So, traditional office governance and control practices are impractical to apply. But without reasonable security measures, there is a risk of data exposure, such as the loss of a device. Smartphones increase efficiency, but convenience cannot override ethical and legal duties.

## Common Risk Scenarios in Practice

Risks associated with smartphones are not hypothetical and may arise from routine professional use, often without conscious intent or

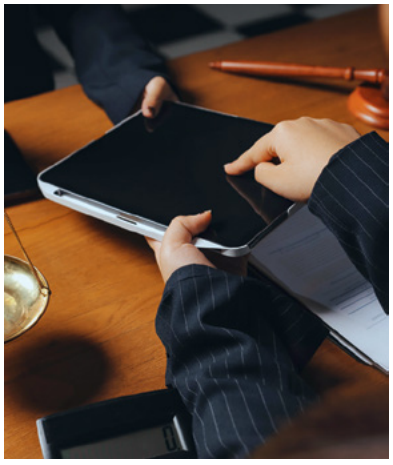


> **"As per the Code of Ethics, Chartered Accountants are ethically bound to safeguard client confidentiality and shall be alert to the possibility of inadvertent disclosure. The obligation of client confidentiality is technology neutral and applies irrespective of whether client data is stored in physical files, office systems or a personal device like a smartphone."**

negligence. Smartphones typically contain emails, chat history, one-time passwords (OTPs) and client documents containing personally identifiable information. Such devices are vulnerable to loss or theft, particularly in public places or during travel. In such situations, there is a risk of unauthorized access, especially where adequate security controls are not implemented, such as protecting the device with a strong password.

Cloud backups are generally enabled by default on most smartphones. As a result, personal and professional data stored on the device may be automatically uploaded to third-party servers, often without clarity over data retention policies or the geographical location of stored data. This leads to the storage of client information beyond a Chartered Accountant's direct control.

In practice, smartphones may also be accessed by office staff for limited purposes or by family members during travel or emergencies. Such informal access, though unintentional, increases the risk of accidental exposure of professional data to unauthorized persons.



As per the 2024 Global Mobile Threat Report, 82% of phishing sites specifically targeted mobile devices, of which 76% of phishing sites use HTTPS, giving victims a false sense of security. This is highly relevant for Chartered Accountants because OTPs, tax credentials, client attachments, and approval links are often handled on smartphones.

Further, smartphones are frequently used for downloading applications intended for personal convenience. Some applications may contain malware or spyware, potentially compromising the device and the data stored on it. The mixed use of smartphones for both personal and professional activities also makes segregation, monitoring and timely deletion of professional data difficult.

These risks arise from ordinary professional use of smartphones and not from exceptional uses. Therefore, the appropriate response should be implementing reasonable safeguards rather than avoiding smartphones altogether.

## Indicative Safeguards and Reasonable Controls

The safeguards discussed are illustrative and may be adopted based on firm size, nature of practice, and risk assessment.

At the firm level, it should be recognized that smartphones are complex technological tools with



the capacity to store and process multiple categories of sensitive professional data. Accordingly, firms should acknowledge smartphones as an extension of the professional workspace rather than merely personal devices.

Firms may articulate clear internal guidance to partners and staff that professional communication and document sharing through smartphones should be avoided wherever practicable, particularly for sensitive or high-risk information. Such policies need not be extensive or technical in nature but should clearly define acceptable use, boundaries and individual responsibilities.

Where smartphones are used for both personal and professional activities, conscious effort should be made to distinguish between the two. Basic security controls such as strong passwords, biometric authentication and automatic locking should be treated as minimum safeguards. Features enabling remote locking or wiping of data in the event of loss or theft provide an additional layer of reasonable protection.

Further, periodic removal of data accumulated during professional activities such as documents, chat histories and authentication information reduces prolonged exposure and limits the impact of accidental or unauthorized access.

Such safeguards are also aligned with internationally recognized guidance. The National Institute of Standards and Technology (NIST) has issued guidelines on managing the security of both organization-provided and personally owned mobile devices, recommending defined mobile device security policies. Similarly, the National Cyber Security Centre (NCSC) highlights the importance of controls such as device encryption, updates, access restrictions and remote wiping capabilities.

Equally important is client awareness. Clients should be sensitized to the risks of sharing sensitive documents and information through informal smartphone-based communication. Encouraging structured communication channels such as email reinforces data discipline without significantly impacting convenience.

Ultimately, risks associated with smartphone usage arise not from the technology itself but from human behaviour surrounding its use. When governed consciously and proportionately, smartphones can significantly enhance professional efficiency without compromising ethical and legal responsibilities.

## Conclusion

Smartphones have become an unavoidable companion in the professional workflow of Chartered Accountants, capable of executing activities traditionally confined to the physical office. However, they often operate outside conventional office governance structures and controls. Ethical and legal responsibilities cannot be avoided merely because professional data resides on a personal device.

At the same time, expecting absolute control or complete elimination of risk in the use of smartphones is neither practical nor reasonable. Identifying inherent risks and implementing proportionate safeguards enables the profession to engage with this complex technology more consciously. The objective should not be to resist technological adoption, but to embrace it responsibly while upholding professional accountability. The smartphone is not merely a device; it is a mobile office that requires conscious governance. Such an approach enables the profession to adapt to technological realities while remaining aligned with its long-standing ethical foundations.

> **"As per the 2024 Global Mobile Threat Report, 82% of phishing sites specifically targeted mobile devices, of which 76% of phishing sites use HTTPS, giving victims a false sense of security."**

## References


- *https://trai.gov.in/sites/default/files/2026-03/PR_No.39of2026.pdf*
- *https://www.verizon.com/business/resources/T41c/reports/2025-mobile-security-index.pdf*
- *https://zimperium.com/resources/surge-in-mobile-phishing-attacks-key-trends-and-threats-uncovered*


Author may be reached at eboard@icai.in