A phone can be encrypted, password-protected, and approved for work—and still reveal patient or organizational information on its lock screen. A message preview, calendar alert, or missed-call notification may be visible to anyone who picks up the device or glances across a desk.

The Information Commissioner's Office (ICO) does not provide one universal notification setting for every workplace. Its UK GDPR security guidance and advice on working from home securely point organizations toward appropriate technical and organizational measures. In practice, that means following your employer's device policy, using approved systems, and configuring notifications to reduce unnecessary disclosure.

This is practical guidance, not a substitute for your organization's policy or advice from its information governance, data protection, or IT team. A setting that is suitable for one service may not be appropriate for another. The goal is to understand the risk, use the approved configuration, and check what other people can actually see.

Start With Your Employer's BYOD and Device Policy

Before changing settings, find out whether you are allowed to use a personal device for work at all. "Bring your own device" (BYOD) arrangements are not automatic permission to handle work information on a personal phone. Your employer may require a managed work profile, a specific app, device encryption, a minimum operating-system version, or approval from a manager or IT team.

Policies can also distinguish between types of information. For example, an organization may allow access to routine work email but prohibit storing patient information in personal photos, notes, or messaging apps. It may require staff to use a managed application that can remove work data without deleting personal content. A folder labeled "Work" does not, by itself, create that separation or provide security.

Check the current policy for clear answers to these questions:

- Is personal-device use permitted, and does it require registration or approval?
- Which apps and services are approved for patient and organizational data?
- Are there required passcode, biometric, encryption, or automatic-lock settings?
- What does the policy say about lock screen notifications, screenshots, backups, and voice assistants?
- Who should you contact if a device is lost, a notification exposes information, or you are unsure whether an app is approved?

If the policy is unclear, ask your manager, information governance lead, data protection officer, or IT service desk. Do not treat a colleague's personal workaround as authorization. In a clinical environment, the most convenient setting is not necessarily the approved configuration.

Use Approved Systems for Patient and Organizational Data

"Working securely" is not just about hiding a message preview. It also means controlling where work information https://obgynkey.com/keeping-work-and-personal-phone-use-separate-practical-habits-for-healthcare-professionals/ is created, sent, stored, and accessed. Use the systems your employer has approved for the task. That may include a clinical record system, managed email, an approved collaboration tool, or a specific work app.

A notification is often only one small part of a wider information flow. A message could appear in an app preview, be copied into a personal notes app, sync to a personal cloud account, or show up on a linked watch or tablet.

Choosing the approved system helps your organization apply access controls, retention rules, audit logging, and support arrangements. An ordinary text message or personal email account may not have those safeguards.

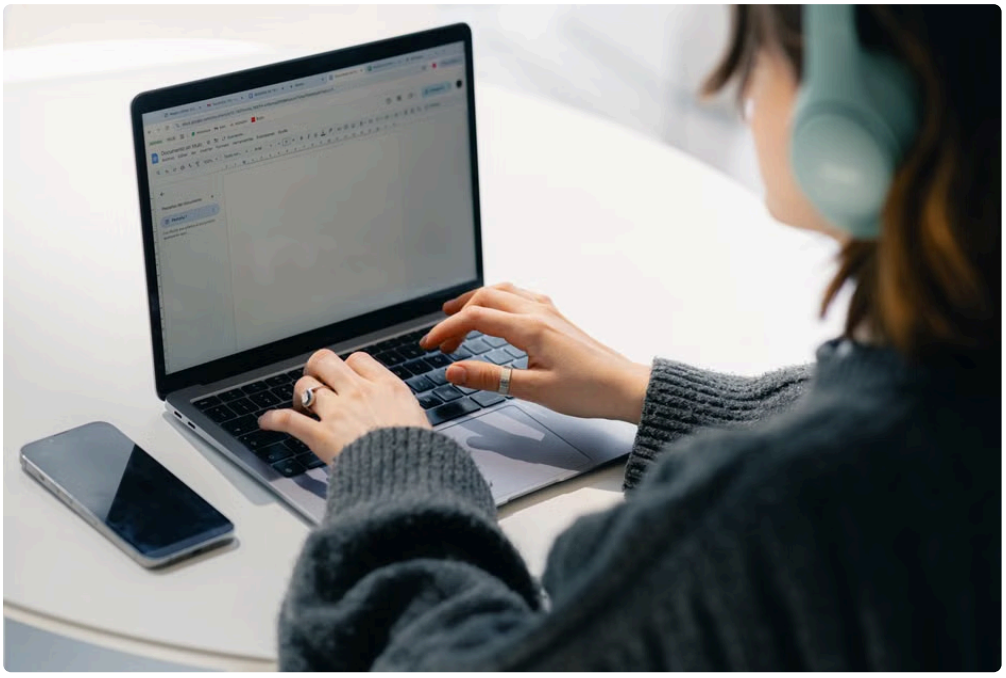
Do not move patient or organizational information to an unapproved service just because it is quicker, a work app is unavailable, or a notification is easier to manage there. Do not forward work messages to personal email as a workaround. If an approved system is not working, use your employer's support or downtime process. If urgent clinical communication is involved, follow the local escalation procedure.

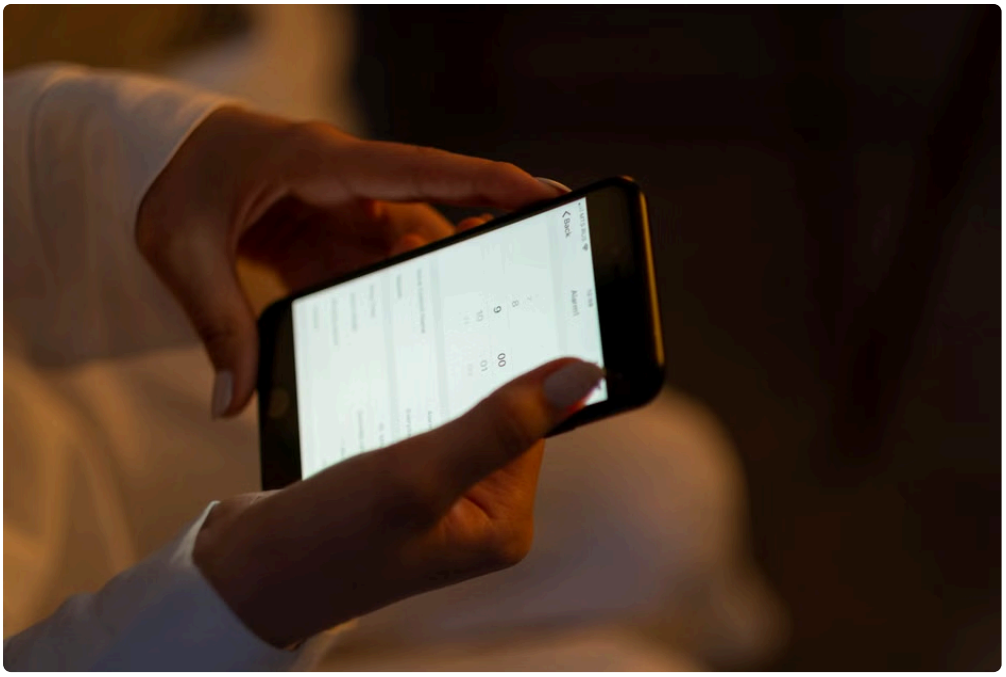
Separate entertainment from clinical work

Where your organization permits a personal device, keep work and personal use separate as far as the approved tools allow. A managed work profile or dedicated work app may help isolate work data from personal apps. Use the approved method rather than assuming that separate folders, home-screen pages, or contact lists provide a security boundary.

Keep patient information out of entertainment and consumer services. For example, do not paste work content into a personal messaging app, use a public social platform to coordinate care, or ask a consumer assistant to read out a clinical message. Be alert to features that cross between devices: notifications can appear on a smartwatch, a car display, a tablet, or a desktop even when the phone itself is locked.

Separation also reduces easy mistakes. When choosing a share option, pause to check the recipient, destination app, and account before sending. The wrong share-menu tap can disclose a document or image to a personal account. If an app offers both work and personal profiles, confirm which one is active before attaching or sharing anything.





Why Lock Screen Exposure Matters

Lock screen exposure occurs when a person can learn information from a device without opening it or signing in. A preview might show a name, message text, appointment, subject line, caller, or part of a clinical update. Even if the screen does not display a diagnosis or full record, a combination of details may reveal more than intended.

Consider a phone left on a shared desk, a device visible at a reception point, or a notification appearing while you are speaking with a patient. The person who sees it may be a coworker without a need to know, a visitor, a family member, or a member of the public. The risk is not limited to theft or hacking; ordinary, brief visibility can also expose information.

The ICO's security approach is risk-based. Organizations should choose measures appropriate to the information and circumstances, while staff should follow the controls their employer has put in place. For a clinician, that means balancing the need to notice a time-critical work alert with the need to avoid displaying sensitive content unnecessarily. It does not mean every notification must be switched off, nor that hiding previews alone makes a device secure.

Set Notification Privacy Deliberately

Use your employer's approved configuration if one is provided. If you are permitted to manage the setting yourself, review both the device's lock screen controls and the notification settings inside each work app. Menu names vary across phone models and software versions, so verify the actual result rather than relying on a setting label.

1. **Check the policy first.** Confirm whether your organization requires a particular setting or centrally manages notifications.
2. **Choose what appears while locked.** Options may include showing all content, hiding sensitive content, or showing no notification details. Use the choice required by policy; when permitted, avoid displaying message content on a locked screen.
3. **Review work apps individually.** Check email, messaging, calendar, clinical, and authentication apps. A general lock screen setting may not control every app in the same way.

4. **Check other connected devices.** Review notification mirroring to watches, tablets, car systems, and computer desktops, following your organization's rules.
5. **Test while the phone is locked.** Send a test notification from an approved source or ask IT how to test safely. Look at the screen as someone nearby would. Confirm whether the sender, subject, message text, or appointment details are visible.
6. **Recheck after changes.** An operating-system update, app update, new device, or restored backup may change behavior. Test again after significant changes.

Testing the real lock screen is important. A setting may say that previews are hidden but still show a sender's name, app label, or part of a notification. Another setting may hide content only when the phone is locked and reveal it after facial recognition. That behavior can be acceptable under a particular policy, but do not assume it without checking.

Setting or situation What to check Practical aim Lock screen previews Can a passerby read message or calendar content? Show no sensitive content unless policy explicitly approves another setting. App-specific notifications Does the app override the phone's general preview setting? Apply the approved configuration to each relevant app. Wearables and vehicle displays Are work alerts mirrored to another screen? Use only permitted devices and review what they display. Shared or public settings Could someone nearby see or hear an alert? Position the screen discreetly and avoid reading sensitive alerts aloud.

Balance Privacy With Safe Clinical Communication

Turning off every alert may prevent useful or urgent communication from reaching you. Changing notification settings can also affect on-call arrangements, escalation workflows, or response expectations. Do not make changes that could interfere with a clinical duty without checking the relevant local process.

If you need alerts to respond safely, ask your manager or IT team whether there is an approved way to receive them with content hidden—for example, a notification that identifies the app but does not reveal the message. Confirm how urgent communications are delivered and what you are expected to monitor. A privacy setting should fit the service's communication arrangements, not quietly replace them.

When a message is not urgent, open the approved app after unlocking the device and sign in as required. Avoid reading sensitive content over a shoulder or in a crowded space. If you need to discuss information, use an appropriate private setting and follow the organization's confidentiality procedures.

What to Do if Information Is Exposed

If a lock screen, wearable, or other notification displays information to the wrong person, do not assume that the event is too minor to report. Follow your organization's incident-reporting process promptly. Include what was visible, which device or app was involved, who may have seen it, and what steps you took. Report a lost device or suspected account compromise immediately through the designated route.

Do not try to conceal an incident by deleting messages or changing settings without documenting what happened. Your employer's information governance team can assess the situation and advise on any further action. Prompt reporting helps the organization respond and identify whether a configuration, training, or process change is needed.

A Practical "Working Securely" Check

Before using a personal or work mobile device for work, make these checks part of your routine:

- You have permission to use the device and know the applicable BYOD policy.
- Patient and organizational data stay in approved systems.
- Work and personal activity are separated using the organization's approved tools, not just folders.
- Lock screen previews and app-specific notifications match the approved configuration.
- You have checked connected screens such as watches, tablets, and car displays.
- You have tested the actual locked screen to see what another person could read.
- You know how to report an exposure, lost device, or technical problem.

In short, ICO guidance is not a single "hide previews" rule. It supports a broader approach: follow your employer's policy, use approved systems, protect work information wherever it appears, and choose notification settings that fit both privacy and clinical needs. A quick real-world lock screen test is a useful final check—but it does not replace the organization's approved configuration or its wider security controls.