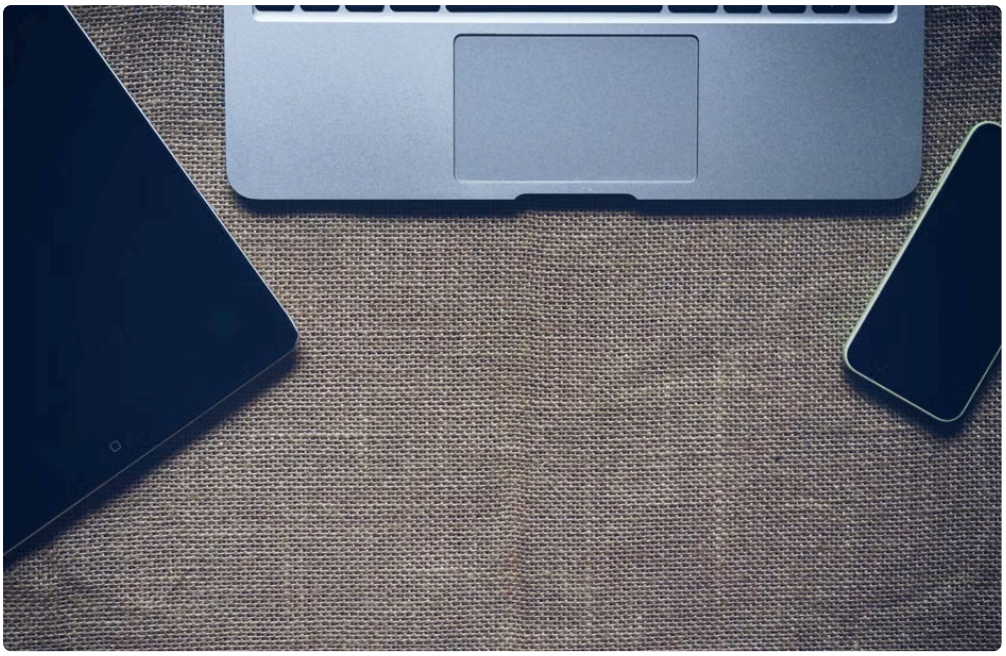
A phone lights up on a ward, in a clinic, or during a handover. A message preview appears before you can pick it up. If it contains a patient's name, a clinical detail, or a work conversation, someone nearby may see it without unlocking your device.

That is a preventable route to patient info exposure. The right fix is usually a small change to notification settings—but start with your employer's device policy, not a settings menu. Your organization may manage work notifications centrally or require you to use an approved app. Changing settings should support those controls, not work around them.



This guide explains how to improve lock screen previews and notification privacy on a work or personal device used for work. It reflects the Information Commissioner's Office (ICO) guidance on keeping information secure. It is not a substitute for your employer's policy or your local information governance advice.

Start with your employer's BYOD and device policy

BYOD means "bring your own device." If you use a personal phone or tablet for work, check your organization's BYOD policy before changing how work messages are delivered. If you have a work-issued device, check its acceptable-use and mobile-device guidance. These policies should tell you which devices, apps, and ways of accessing work information are permitted.

Look for instructions about:

- Whether personal devices can be used for work at all.
- Which approved apps and systems you must use for email, messaging, documents, and patient information.
- Whether your organization manages the device, a separate work profile, or notification settings.
- What to do if you lose a device, see information displayed to the wrong person, or suspect an account has been accessed.
- Whether you may use a smartwatch, car display, or other connected device with work notifications.

If a policy is unclear, ask your manager, IT service desk, or information governance team before adding a work account to a personal app. Don't use personal email, consumer messaging, or an unapproved notes app as a workaround. A hidden preview does not make an unapproved system suitable for patient or organizational data.

Use approved systems for patient and organizational data

Use only the communication and record systems your employer has approved for the information involved. This matters whether a message contains a patient's name, a staff rota, an incident detail, or an internal document. The fact that a familiar app is convenient does not mean it is approved for work.

The ICO's UK GDPR security guidance describes the need for appropriate technical and organizational measures to protect personal data. Its guidance on working securely, including when working from home, is a useful reminder that information needs protection outside the workplace too. For practical advice, see the ICO security guidance and the ICO's working from home securely guidance. Your organization should translate relevant requirements into local procedures and approved tools.

Notification settings are one layer of protection, not the whole security plan. They can reduce what appears on a display, but they do not change where a message is stored, who can access the account, or whether the app is suitable for clinical information.

Separate entertainment from clinical work

On a personal phone, it is easy for work and personal notifications to arrive on the same screen. Keep work use within the boundaries your employer has approved. If your device supports a managed work profile or a separate work app, follow your organization's setup instructions. Do not create your own split by forwarding work messages into personal accounts.

Consider these practical boundaries:

- Use approved work apps for work conversations and records.
- Keep personal entertainment apps and accounts separate from work accounts where your policy allows.
- Do not copy patient or organizational information into personal messages, screenshots, cloud notes, or social media.
- Review whether work notifications are mirrored to a watch, tablet, vehicle display, or computer. Follow policy before connecting another device.
- Use the approved method to sign out of or remove work access when your role, device, or employment changes.

Folders and app placement can make a device easier to use, but they are not security controls. Putting work apps in a folder does not prevent previews, syncing, or access by someone who can unlock the phone.

Choose the notification privacy level you need

You can usually choose whether the lock screen shows full message content, a limited description, or no notification details. The labels vary by phone, operating system version, and management settings. The safest option for a shared or public setting is generally to hide sensitive content until the device is unlocked—or to prevent the relevant app from appearing on the lock screen, if your policy permits it.

Setting choice What someone nearby may see When to consider it Show full previews Message text, sender, or other notification details Only if permitted and appropriate for your setting; it creates the greatest exposure risk. Show when unlocked An alert may appear, but its content is hidden until the device is unlocked A practical balance when you want to know a notification arrived without displaying its contents. Hide or disable lock screen notifications Little or no detail on the lock screen, depending on the device and app Useful where the screen may be visible to patients, visitors, or colleagues.

Even a sender's name or the fact that a particular service has sent an alert can reveal information. Think about the whole notification, not just the message body.

Change settings on common phones

Menu names differ between versions and manufacturers. If your device is managed by your employer, some options may be unavailable or may reset automatically. Do not remove management software or weaken required security settings to get around a restriction. Ask IT for the approved configuration.

On an iPhone

1. Open **Settings**, then select **Notifications**.
2. Choose the work app you use, such as your approved email or messaging app.
3. Open its preview or lock-screen display options. Depending on your iOS version, look for **Show Previews** under Notifications, or a similar setting.
4. Choose an option such as **When Unlocked** or **Never**, if available and permitted by policy.
5. Check whether the app is still allowed to show alerts on the Lock Screen. Turn that display off if you do not want the app's notifications there.

Some apps have their own preview controls in the app's settings. Check both the iPhone's notification settings and the app's settings; changing one may not control every kind of alert.



On an Android phone

1. Open **Settings** and look for **Notifications** or **Lock screen notifications**.
2. Choose an option such as hiding sensitive content, showing notifications without content, or not showing lock screen notifications. The wording varies by manufacturer and Android version.
3. For more control, open the app's notification settings and review its categories or channels. Hide sensitive content or disable lock screen display for relevant categories where available.
4. If your organization uses a managed work profile, check its instructions or ask IT before changing work-app settings.

Android devices may let you control lock screen display for all apps or for individual apps and notification categories. A global change can also hide personal alerts, so check what it affects before relying on it.

Test the setting on the actual lock screen

Do not assume a setting worked because the menu changed. I test notification privacy on the actual device, with its screen locked, because settings can behave differently after an update, an app change, or a connection to another device.

1. Ask a colleague or use a non-sensitive test message. Do not put patient information into a test.
2. Lock the phone and trigger a notification from the work app.
3. Look at the screen as someone standing nearby could. Check whether the sender, message text, subject line, or other details are visible.
4. Unlock the phone and confirm you can still access the notification in the approved way.
5. Repeat the check for any work app that can send alerts, and for a watch or other connected display if one is permitted.

Check again after operating-system updates, app updates, a device replacement, or a change to your work profile. Some settings can https://obgynkey.com/keeping-work-and-personal-phone-use-separate-practical-habits-for-healthcare-professionals/ revert, and new notification categories may be added.

Check the less obvious places information can appear

Hiding previews in one place may not hide them everywhere. Before relying on your setup, review other screens and alert types:

- **Incoming calls:** A caller name or number may be visible even when message previews are hidden.
- **Email subjects:** The subject line can contain personal or clinical details even if the email body is concealed.
- **Voice assistants:** Spoken announcements can expose information to people nearby.
- **Wearables and vehicle displays:** Alerts may be mirrored from the phone to another screen or spoken aloud.
- **Notification history:** Some devices keep a record of recent alerts that may be visible after unlocking.
- **Shared spaces:** A phone on a desk can be visible to patients, visitors, or colleagues. Turn the screen away or keep the device with you when appropriate.

If patient information appears on the lock screen

If a preview displays patient information, first reduce further exposure: lock the device, move it out of view, and change the setting if you are authorized to do so. Then follow your employer's incident-reporting process. Contact your manager or information governance team promptly if the information may have been seen by someone who should not see it, or if you are unsure whether an incident needs reporting.

Do not delete evidence, forward the message to a personal account, or try to investigate beyond your role. Record the basic facts requested by your local process, such as what was displayed, when, and who may have seen it. Your organization will assess the event and advise on next steps.

A quick pre-shift check

- Is this device permitted for the work I am doing?
- Am I using the approved app or system for patient and organizational data?
- Are lock screen previews hidden or limited as required by policy?
- Have I checked the actual locked screen, not just the settings menu?
- Could a watch, car display, or voice assistant show the same alert?
- Do I know who to contact if information is exposed?

Good notification privacy is a straightforward habit: follow your employer's BYOD and device rules, keep work in approved systems, limit what appears while the phone is locked, and test the result. These steps reduce the chance of accidental patient info exposure without relying on a folder, a vague reminder, or an assumption that the setting is working.