A work app can be approved for clinical or organisational use and still not be allowed to display alerts on your lock screen. The app's approval and its notification settings are separate questions. An alert might reveal a patient's name, appointment, message preview or other confidential information to someone looking at your phone.

Start with your employer's bring-your-own-device (BYOD) or mobile-device policy. Then check whether the app and the data it handles are approved, and find out what your organisation requires for lock screen notifications. If the policy is unclear, ask your manager, IT service desk, information governance team or data protection officer before enabling previews.

This is a practical guide, not a substitute for your organisation's policy. UK data protection obligations depend on the circumstances, the information involved and the controls in place.



Start with your employer's device policy

Your employer should tell you whether you may use a personal device for work, what security controls are required and which systems are approved. Do not assume that a familiar app is permitted just because it is available in an app store or because a colleague uses it.

Look for the current BYOD, mobile-device, remote-working or information security policy. Check for instructions about:

- Which devices and operating systems may access work services.
- Whether a device must be enrolled in mobile-device management (MDM) or use a separate work profile.
- Required screen-lock, encryption, update and authentication settings.
- Approved apps for email, messaging, clinical records, rota information and file sharing.
- Whether notifications may appear on a locked screen, and whether message or sender details may be shown.
- What to do if a device is lost, shared, compromised or no longer supported.

If the policy says work devices are managed by your organisation, do not try to work around its controls. A setting may be locked or changed automatically because your employer has made a security decision. Ask the service desk what is allowed rather than trying another account, app or device to get around it.

Check that the app and information are approved

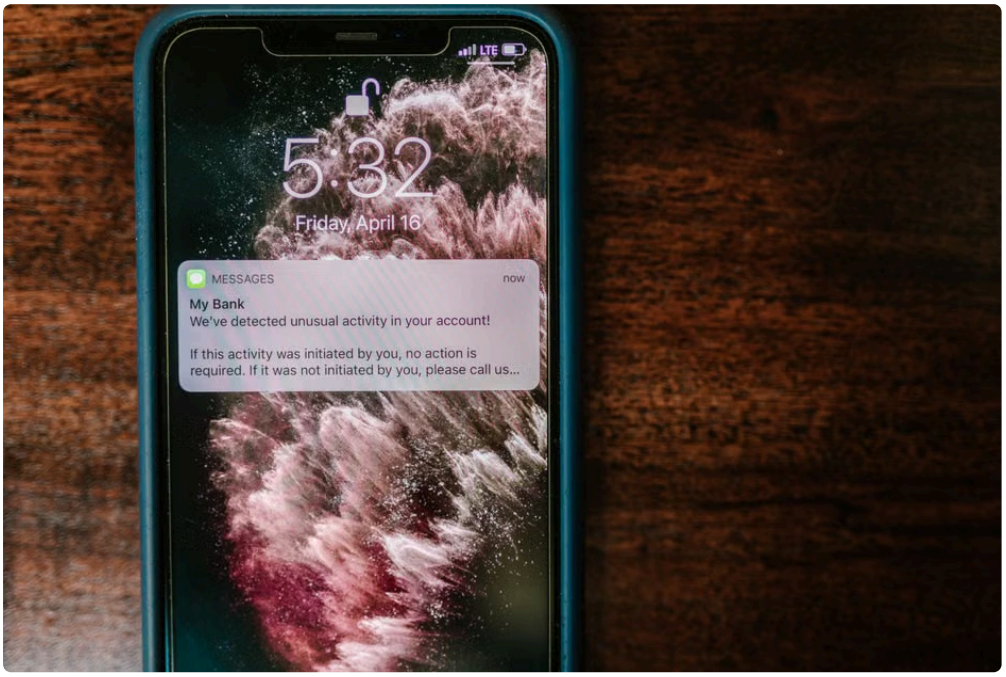
Use only systems your organisation has approved for the type of information involved. This matters for patient data and for other organisational information, such as staff details, incident reports, operational plans and internal messages. A personal messaging app, personal email account or consumer cloud service is not an acceptable workaround unless your organisation has explicitly approved it for that purpose.

Approval is not always all-or-nothing. An organisation may permit an app for general work alerts but not for patient-identifiable information. It may allow access through a managed work profile but prohibit access through the same app installed as a personal app. It may also approve an app while restricting which data can be downloaded or displayed.

Before enabling notifications, confirm:

- The app is on your organisation's approved list or has been specifically authorised for your role.
- You are signed in to the correct work account and using the approved version or managed container.
- The information sent through the app is permitted for that system.
- Your device meets your employer's security requirements.
- The notification content and visibility match your organisation's rules.

Do not treat a folder, a second home screen or a renamed app as a security boundary. A work profile or managed app can provide meaningful separation when configured by your organisation; simply placing work and entertainment apps in different folders does not.



Why lock screen notifications need a closer look

Notifications can be useful. They may help you respond to an urgent operational message or notice a change to a work schedule. But a locked phone can still show information to people nearby, depending on your settings. A colleague, visitor, family member or passer-by may see an alert without unlocking the device.

There are two different privacy questions:

QuestionWhat to check Can the app send notifications?The app's notification permission and any organisation-managed restrictions. What appears while the phone is locked?Whether alerts are hidden, shown without details,

or displayed with previews and sender information. Where do alerts appear?Lock screen, notification centre, banners, watch, car display or other connected devices.

Turning off previews may reduce what is exposed, but it does not necessarily stop every alert or prevent information appearing on a paired watch or another linked device. Conversely, disabling notifications entirely may affect a work process. Follow your organisation's instructions and check the complete set of devices and displays you use.

Choose the least revealing setting your policy permits

When notifications are allowed, a sensible privacy setting is often to show that an alert exists without showing its contents until you unlock the phone. Depending on your device and app, options may include hiding previews, showing previews only when unlocked, or turning off lock screen notifications for that app.

Do not rely on a setting name alone. The wording and behaviour differ between operating systems, device models and app versions. Your organisation may also manage settings centrally, so the option you see may not be the final control.

Use this sequence:

1. Read the relevant BYOD or mobile-device instructions.
2. Confirm the app and account are approved for the information you handle.
3. Check the organisation's specific rule for lock screen alerts and previews.
4. Open the device's notification settings and review the work app's permissions. If a work profile or managed device is used, check the managed settings or ask IT.
5. Set the lock screen to hide sensitive details if your policy permits notifications but does not allow previews.
6. Test the result on the actual locked screen, not just in the settings menu. Send a test alert or use an approved non-sensitive notification, lock the phone and check what is visible.
7. Repeat the check for a paired watch, car display or other linked device if work alerts can appear there.

Testing on the actual lock screen matters because a setting can behave differently from what you expect. Check whether the app name, sender, message text, subject line or appointment details are visible. Do not use real patient information to test. If you cannot safely test without exposing confidential data, ask IT for help.

Keep entertainment and clinical work separate

Many people use one device for both work and personal life. That does not remove the need to keep work information within approved systems. Avoid copying patient or organisational information into entertainment apps, personal notes, personal email, consumer file storage or social media. Do not use a screenshot or a messaging shortcut to move information between work and personal spaces.

Where your employer provides a managed work profile or container, use it as instructed. It may separate work apps and data from personal apps, and may let your organisation apply specific security controls. It is not a reason to assume every notification is private: lock screen alerts can still be visible outside the work profile, depending on the device configuration.

For shared or family-use devices, follow the policy rather than relying on people to avoid looking at alerts. If a device is not approved for work access, do not sign in to work services on it. If your organisation permits personal-device use, protect the device with a strong passcode or other approved screen lock, keep its software updated and do not let other people use it while you are signed in to work systems.

What UK GDPR and ICO guidance mean in practice

The UK GDPR requires organisations to use appropriate technical and organisational measures to protect personal data. The precise measures depend on the risk and context; there is not one universal rule that every work app must have all lock screen notifications disabled. Your employer is responsible for setting and communicating appropriate controls, and staff should follow those controls and report problems.

The Information Commissioner's Office (ICO) provides guidance on keeping information secure, including practical advice relevant to working away from the workplace and working from home. Its guidance supports basic habits such as protecting devices, preventing unauthorised access and handling personal information securely. It does not replace your organisation's own policy or approve a particular app for your workplace.

Use the ICO's current guidance as background, then apply your employer's instructions to your device and role:

- ICO: Security under the UK GDPR
- ICO: Working from home securely

ICO pages and their structure can change, so search the ICO website for "working securely" or "working from home securely" if a link has moved. The key point is that notification choices form part of a wider security arrangement: approved systems, device protection, access controls and staff practice all matter.

If the policy is unclear or the setting is unavailable

Do not guess, and do not switch on previews simply to see whether they work. Ask your manager or IT service desk a specific question, such as: "Is this app approved on my device, and may it show sender names or message previews while the screen is locked?" If the app handles patient information, include that context without sending patient details in an unsecured message.

Contact the information governance team or data protection officer if you need help on call notification settings interpreting a rule about personal data. Contact IT if the device is managed, the option is unavailable, or notifications behave differently from the policy. If a work alert unexpectedly displays confidential details, follow your organisation's incident-reporting process promptly.

A quick decision check

- **Policy:** Does your employer allow work access on this device?
- **Approval:** Is this app approved for the information you will receive?
- **Permissions:** Are notification permissions allowed by the app and organisation settings?
- **Privacy:** Does the locked screen reveal message content, names or other sensitive details?
- **Testing:** Have you checked the actual lock screen and any connected displays?
- **Uncertainty:** Have you asked the right team rather than using an unapproved workaround?

If you cannot answer those questions confidently, leave previews off where possible and get advice before using the app for work. The safest setting is not always "no notifications"; it is the setting your organisation has approved, configured and tested for the information you handle.