The quickest reliable check is to look in three places: your work app's linked-device or active-session list, your phone's notification and device-pairing settings, and any computer or wearable that might be showing alerts. There usually isn't one screen that lists every device receiving every work notification.

Before changing anything, check your employer's BYOD and device policy. It should say which devices and apps are approved for work, including patient and organisational information. If you find an obgynkey.com unfamiliar device, or work notifications are reaching a personal device that your organisation does not permit, contact your IT or information-governance team using the approved route.

This is a practical check, not a substitute for your organisation's security process. The Information Commissioner's Office (ICO) provides guidance on working securely and working from home securely. Follow your employer's rules and local incident-reporting procedure if you think information may have been exposed.

Start with your employer's device policy

Take a minute to confirm what your organisation allows. A phone may be technically able to receive a work alert without being an approved device for work. Equally, your employer may provide a managed app that separates work content from personal content.

Check the policy or ask your manager, IT service desk or information-governance lead about:

- Which phones, tablets, computers and smartwatches may be used for work.
- Which apps and communication channels are approved for patient or organisational information.
- Whether personal devices must be enrolled in device management, protected by a passcode or configured in another way.
- What to do if you lose a device, see an unfamiliar session or notice a notification on the wrong screen.

Do not use personal email, an unapproved messaging app or a consumer cloud service as a workaround. A notification that contains a patient name, appointment detail or other work information is still information to protect, even if it appears only briefly.

The fastest check: work through these three places

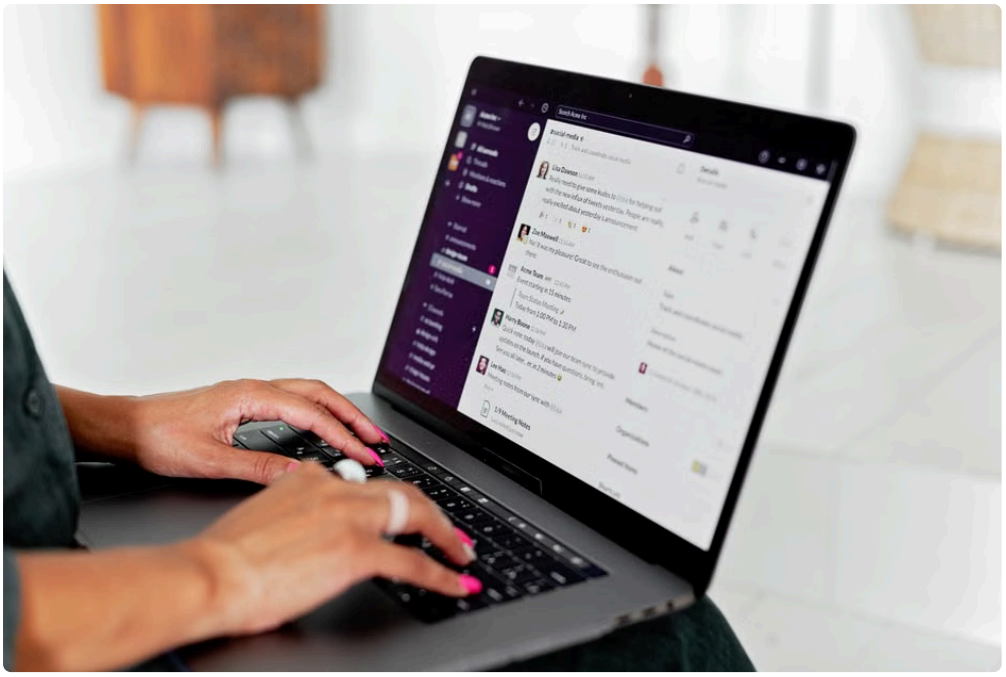
1. **Check the work app.** Open the app's account, security or device settings. Look for *Linked devices*, *Devices*, *Active sessions* or *Where you're signed in*.
2. **Check the phone's connections and notification settings.** Review paired computers, connected watches, notification sharing, and which apps can show alerts on the lock screen.
3. **Check the other screens.** Look at the computer and smartwatch themselves. Confirm whether work alerts appear there, including when the phone is locked.

Menu names vary between operating systems, app versions and employer-managed devices. Use your device's Settings search if a menu is hard to find. If a work profile or management app controls a setting, do not try to bypass it; ask your IT team.

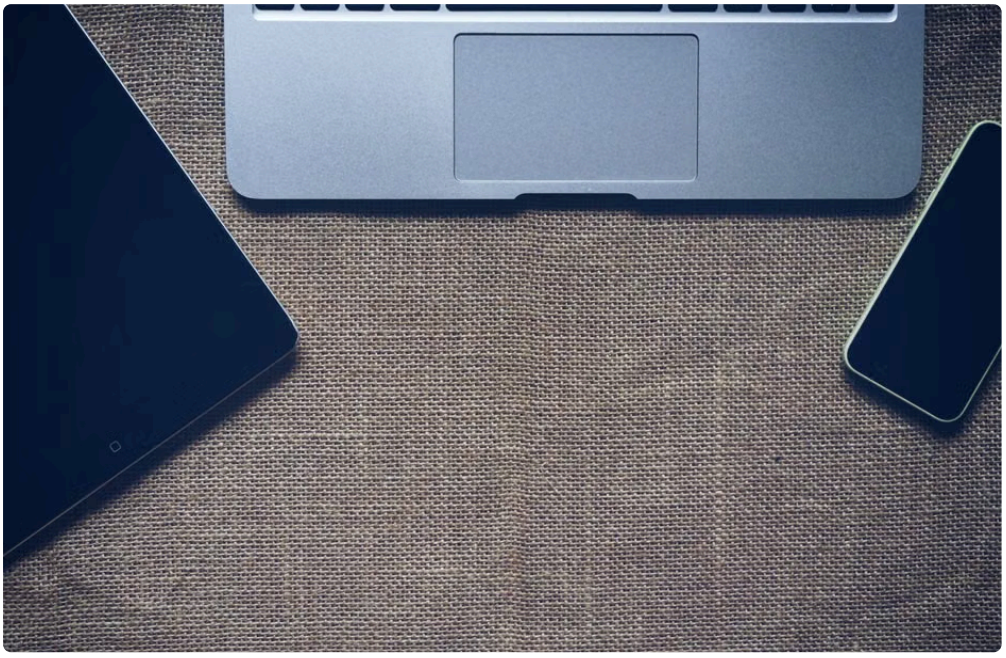
1. Review the linked devices list in each work app

Start with the apps that send work alerts: for example, your organisation's approved email, messaging, video-meeting or clinical system. In each app, open the account or security area and look for a **linked devices list** or

active sessions. Check the device name, type and last activity against devices you recognise and are allowed to use.



Some apps let you sign out a specific session. Others require an administrator to review or revoke access. If a device looks unfamiliar, do not assume it belongs to you because the name is generic. Take a note of what the app shows and contact your service desk. Follow local guidance before taking action that might affect clinical work or remove access needed by a colleague.



A linked-device list is useful, but it is not a complete inventory of notification destinations. It may show devices signed in to that particular app, not a computer receiving mirrored phone alerts, a watch displaying previews, or an email account configured separately. Check each work app you use.

What to record

- The app or system you checked.
- The device name and last-activity time, if shown.
- Whether you recognise the device and whether it is approved.

- Any action you took or person you contacted.

Keep notes within an approved work process. Do not copy patient information into a personal note or send screenshots to a personal account to ask for help.

2. Check paired computer notifications

A phone may send alerts to a computer through a companion app, browser session, operating-system feature or notification-sync setting. That computer may be shared, left unlocked at home, or used by someone else. Check both the phone and computer rather than assuming the work app's linked-device list will show this connection.

On your phone, review Bluetooth connections and any settings or apps for connecting to a computer. On the computer, inspect connected-phone, notification-mirroring, browser and account settings. Look for names you recognise, then check whether work-app notifications are enabled. The exact route depends on the devices and software you use, so search Settings for terms such as "notifications", "phone connection", "sharing" or "paired devices".

Bluetooth pairing and notification access are not the same thing. A device can be paired for audio without receiving message previews; a companion service may also relay alerts in a different way. Confirm the result by testing the actual computer screen, not just by reading a list of paired devices.

3. Check smartwatch alerts

Smartwatch alerts can be easy to overlook because the watch may mirror the phone automatically. Check the watch app on your phone for notification settings and review which apps are allowed to alert. Then look at the watch itself, including what appears when it is worn, raised, or tapped.

Pay particular attention to **smartwatch alerts** on a shared device, a watch you no longer use, or a watch that displays message content when it is not on your wrist. If it is no longer yours or should not receive work alerts, remove it using the approved device settings or ask IT for help. Do not rely on the watch being out of sight; its screen may light up in a workplace, vehicle or public area.

4. Reduce what appears on the lock screen

Even when a device is approved, a lock screen can reveal information to someone nearby. Names, message previews, meeting titles and clinical details may appear before you unlock the device. Set notifications so that they reveal as little as your organisation's policy allows.

On each device, review lock-screen notification settings and the settings for individual work apps. Depending on the device, you may be able to hide previews until the device is unlocked, show only a generic alert, or turn off lock-screen notifications for a particular app. Review notification content on paired computers and watches too; changing the phone's setting does not always change what the companion device displays.

Then test it. Lock the phone and check the real lock screen. Trigger a harmless test notification if your organisation allows it, and check the computer and watch as well. Confirm what is visible to someone standing beside the device. This simple test catches settings that sound private in a menu but still show content in practice.

Check Where to look What you are confirming Work app sessions App account, security or device settings Only recognised, approved devices are signed in Paired computer notifications Phone connections and computer companion settings Work alerts are not appearing on an unintended computer Smartwatch alerts Watch app and

watch notification settings The watch is approved and does not expose unwanted previews Lock screen Phone, computer and watch display settings Visible content is limited when the device is locked

Keep entertainment and clinical work separate

Separate personal entertainment from clinical work as far as your employer's tools allow. Use approved work apps and work profiles for work, and avoid forwarding work alerts into personal messaging, email or cloud accounts. Don't paste work content into a personal assistant, notes app or social platform to make it easier to find later.

Separation helps prevent accidental mixing, but it is not a security guarantee by itself. A separate folder, home screen or app collection does not control who can see a lock-screen preview, which account is signed in, or whether a device is managed. Use the controls and approved systems your employer specifies.

A quick checklist before you finish

- I have checked my employer's BYOD and device policy.
- I have reviewed the linked devices list or active sessions in each work app I use.
- I have checked paired computer notifications and any phone-to-computer sharing.
- I have reviewed smartwatch alerts and removed any connection I should no longer use.
- I have set lock-screen previews appropriately on every device.
- I have tested the actual lock screen, computer and watch rather than relying on a menu label.
- I know who to contact if a device or session is unfamiliar.

If you find a device you do not recognise

Use your organisation's incident or IT reporting route promptly. Share the details the service desk needs, such as the app, device name and last activity, but don't include patient information in an unapproved channel. If you suspect that patient or organisational information has been exposed, follow your local incident-reporting process rather than trying to investigate alone.

In short: check each work app's linked devices list, then inspect paired computer notifications and smartwatch alerts, and finally test what appears on each lock screen. Start with your employer's policy, use approved systems for work information, and treat the real screen—not the settings menu—as the final check.