A share menu looks like a shortcut. Tap an icon, choose a person or service, and send. In a busy clinical day, that can feel safer and faster than opening an app and starting from scratch. But share menus also make it easy to send information to the wrong destination—especially when suggested contacts, recent services and personal accounts appear beside work options.

The problem is not simply that someone is careless. Share menus are designed to predict what you might want to do next. They may surface a recent contact, a frequently used app or an account that was active earlier. Those suggestions can change, and the same-looking icon can lead to different accounts or recipients. A quick tap can bypass the checks you would normally make when composing a message inside an approved work system.

For clinicians and teams, preventing a share sheet risk starts before the first tap: follow the employer's BYOD and device policy, use approved systems for patient and organisational data, keep clinical work separate from entertainment, and check what appears on the lock screen. These are practical controls, not guarantees. The goal is to make the safe route easy and the wrong route less likely.



What Is a Share Sheet, and Why Is It Risky?

A share sheet is the menu that appears when you select "Share" in an app or on a device. It may offer messaging apps, email, cloud storage, nearby devices, printing or other services. Depending on the device and its settings, it may also show people or destinations you have used recently.

That convenience creates several kinds of risk:

- **The destination may be personal.** A personal email account or consumer cloud service can appear alongside an approved work service.
- **A suggested recipient may be out of date.** A person you contacted recently may not be the right person for this information.
- **The wrong account may be active.** An app can be signed in to a personal account even when its icon looks familiar.
- **The file may contain more than expected.** A screenshot, document or image can include names, identifiers, notifications or other information in the background.

- **There may be no clear pause for review.** A tap on a suggested destination can open a draft—or, in some workflows, send or upload content with little additional friction.

Share menus vary by device, operating system and app. Do not assume that a colleague's screen will look exactly like yours, or that a particular suggestion will always appear in the same place.

Start With Your Employer's BYOD and Device Policy

Before changing settings or choosing a workaround, check your employer's policy for bring your own device (BYOD), mobile device management and remote access. The policy should explain whether personal devices may be used for work, what information can be accessed, which apps and services are approved, and what to do if a device is lost or information is sent to the wrong place.

Some organisations allow work access only through managed apps or a managed work profile. Others require an organisation-owned device for particular tasks. A device that can open a work email account is not automatically approved for every kind of patient or organisational information.

Ask your IT, information governance or clinical governance team if the policy is unclear. Useful questions include:

- Is my personal device authorised for this work, and for this type of data?
- Which apps, file stores and communication channels are approved?
- Does the organisation manage the work account or work profile on my device?
- Are there restrictions on downloading, copying, printing or sharing files?
- Who should I contact if I cannot use the approved route or make a mistaken disclosure?

Do not treat a folder labelled "Work" as a security control by itself. A separate folder may help you organise material, but it does not necessarily separate accounts, prevent copying or protect data from other apps. Follow the controls your employer has approved.

Use Approved Systems for Patient and Organisational Data

For patient information and other organisational data, use only the systems your employer has approved for that purpose. That may include a clinical record system, secure messaging platform, managed email account or approved document store. The right destination depends on local policy and the task.

A personal email account, consumer messaging app or personal cloud drive may feel convenient, but convenience does not make it an authorised route. Avoid sending work material to your personal account so you can "finish it later." Do not move information into an unapproved service to get around a technical problem. If an approved system is unavailable, use the escalation or downtime process set by your organisation.

Make the destination check deliberate

When you need to share something, open the approved work app first where possible, then select the recipient or location within that app. This creates a useful pause to confirm the account and destination. If you start from a device share menu, stop before selecting a suggested service and check the following:

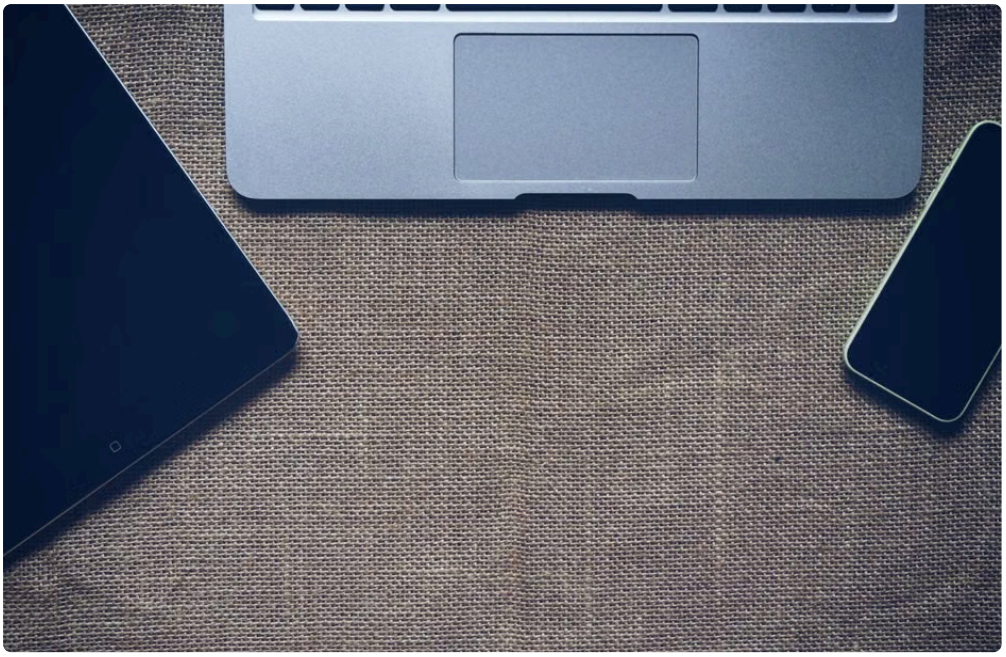
1. Is this the approved app or system for the information?
2. Is the correct work account active?
3. Is the recipient the intended person, team or shared mailbox?
4. Is the file or message appropriate to send, and does it contain only what is needed?

5. Does the final screen show the expected destination before you confirm?

If any answer is uncertain, cancel and use the route described in local guidance. A few seconds of verification are preferable to trying to retrieve information after it has been sent.

Recent Services Suggestions: Helpful, Until They Aren't

Many share menus display recent services suggestions or contact suggestions. These can reduce steps, but they are not a reliable record of where information should go. The menu may prioritise what you used last rather than what is correct for this task. It might also display a personal service that you use frequently outside work.



Do not choose a destination solely because it is at the top of the list, looks familiar or has the right person's name. Check the service name, account and recipient. If the interface does not make those details clear, back out and open the approved service directly.

Some devices let you adjust suggestions or disable certain share-menu features. Settings differ, and changing one option may not remove every suggestion or prevent sharing. If your employer recommends a setting, follow their instructions and confirm the result on your own device. Do not assume a setting is active just because you changed it.

Account Verification Is More Than Recognising an Icon

Account verification means confirming that the account you are about to use is the intended work account—not merely noticing that the app itself is familiar. This matters on shared devices, personal devices with multiple accounts, and apps that allow quick switching between work and personal profiles.

Before sending or uploading, look for the account name, email address, organisation label or work-profile indicator shown by the app. Check the recipient and, where relevant, the destination folder or channel. If the account indicator is hidden, open the app's account or profile menu rather than guessing.

For a first-time setup, follow your organisation's account enrolment and sign-in process. Do not add a work account to a personal service or connect services together unless your employer has explicitly approved that setup. When a device is shared or handed over, sign out or lock it as local policy requires.

Separate Entertainment From Clinical Work

Keeping clinical work separate from entertainment reduces the chance that personal apps, accounts or notifications will be mixed into a work task. Use an organisation-managed work profile or approved work device if your employer provides one. If your organisation permits work on a personal device, use the separation features and restrictions it specifies.

Practical steps may include:

- Use the managed work profile or approved work apps for work activity.
- Avoid saving patient or organisational files into personal photo libraries, downloads folders or personal cloud storage.
- Do not copy work information into personal notes, chat apps or social platforms.
- Keep personal entertainment apps out of the work workflow; do not use them to open, edit or transfer work files.
- Ask IT for help if work and personal accounts are difficult to distinguish.

Separation is a way to reduce accidental mixing, not a substitute for approved systems or sound access controls. A file in a work-labelled folder can still be exposed if it is shared through an unapproved app.

Lock Screen Previews and Notification Privacy

Share-menu mistakes are not the only way information can appear in the wrong place. Lock-screen previews may show message text, sender details, appointment information or other sensitive content to anyone who can see the device. Notifications may also appear while screen-sharing, presenting or using a device in Click here to find out more a public area.

Set notification previews in line with your employer's policy and the privacy needs of your role. Options may include hiding message content while locked, showing no previews, or limiting previews to approved apps. Avoid relying on a generic setting name: devices can behave differently depending on the app, unlock state and notification type.

Test the setting on the actual lock screen. Lock your device, send a test notification from an appropriate non-sensitive source, and check what is visible without unlocking. If you use a managed work profile, check its notifications separately. Repeat the test after major operating-system updates or when changing notification settings.

This test is important because a setting that appears privacy-protective in a menu may still reveal sender names, message snippets or app details in another context. If you are unsure what is displayed, ask IT for device-specific guidance.

A Simple Safe-Sharing Routine

A short routine can help during a busy shift without turning every share into a lengthy task.

1. **Pause.** Ask whether sharing is necessary and whether the information is appropriate to share.
2. **Choose the approved route.** Open the work system directly when practical instead of relying on a suggested destination.
3. **Verify the account.** Confirm that the work account or managed profile is active.

4. **Verify the recipient and content.** Check names, addresses, group membership, attachments and the information visible in the file.
5. **Review before confirming.** Read the final screen carefully, especially if the device has pre-filled a recipient or location.
6. **Stop if it looks wrong.** Cancel and restart through the approved service; do not try to repair an uncertain send by forwarding it elsewhere.

Situation Safer action A personal service appears in the share menu Do not select it for work data. Open the approved work system instead. A recent contact is suggested Verify the full recipient and whether they are authorised to receive the information. You cannot tell which account is active Cancel, check the app's account details, and follow your organisation's sign-in guidance. A lock-screen preview may expose work details Adjust settings according to policy and test the actual locked screen. The approved service is unavailable Use the local downtime or escalation process; do not switch to a personal workaround.

What to Do if You Share to the Wrong Destination

If you realise that information has gone to the wrong person, account or service, act promptly. Follow your organisation's incident-reporting process and contact the designated information governance, privacy, security or clinical governance team. Give a clear account of what was shared, when, through which service, and who may have received it. Preserve relevant details and follow instructions about containment or deletion.

Do not assume that deleting a message or file from your device removes every copy. The recipient may have received a notification, downloaded a file or synced it elsewhere. Do not try to conceal the mistake or contact the recipient outside the approved process unless your organisation tells you to do so.

Use ICO Guidance Alongside Local Policy

The UK Information Commissioner's Office (ICO) provides guidance on protecting personal information, including advice on working securely and working from home securely. This guidance can help organisations and staff think about secure working practices, devices and information handling. It does not replace your employer's policies, local procedures or advice from your information governance and IT teams.

The most useful mindset is simple: a share menu is a convenience feature, not a decision-maker. Start with your employer's BYOD rules, use only approved systems for patient and organisational data, keep work distinct from personal activity, verify the account and recipient, and check what the locked screen reveals. Those small, repeatable checks make a wrong-destination mistake less likely—and make it easier to spot when a screen is asking you to slow down.