Division of Population Health - Process for running a shared voice recorder pool

Approved at IG Committee Meeting 2024-07-22

Background

The sharing of voice recorders between users comes with inherent information governance risks, and so is generally discouraged. However, in some cases it may be pragmatic for certain devices to be shared between people. In such cases, a pool of shared devices may be set up and maintained at department-/section-/group-level. Voice recorders can be used to store or access risk-bearing data, and there are associated information governance risks, so care must be taken to ensure that individuals understand their responsibilities, and that the management of the devices is reviewed for any potential IG issues. The pool should be kept as small as possible to keep it manageable and to reduce the risks, and where the same person repeatedly requires access to a device, consideration should be given to purchasing a device specifically for that person.

Purpose

To outline a process describing how groups can set up a device pool to allow voice recorders to be shared between individuals in a way which minimises and mitigates any IG risks.

Scope

Within the Division of Population Health, any shared pool of voice recorders should be managed in line with the procedure outlined below.

Procedure

For any group within the Division of Population Health wishing to establish a pool of voice recorders for sharing, an individual or individuals should be assigned responsibility for ensuring the following steps are taken:

1. Checking in and out devices.
2. Document devices included in pool (see ‘Maintaining a device list’ section)
3. Appropriately set up devices to be loaned out (see ‘Setting up devices for loan’ section)
4. Establish loan terms and terms of use (privacy policy, etc.) if necessary
5. Include guidance (e.g. a “dos and don’ts” checklist) with device
6. Establish a system to log:
    - Which device
    - Person to whom it was loaned
    - When it was loaned
    - When it was due to be returned
    - When it was returned
    - How it is processed and secured prior to being re-loaned
7. Log any potential incidents with IG committee

Maintaining a device list

Any devices to be included within the pool should be assigned an identifying name and logged (e.g. in a spreadsheet).

Setting up devices for loan

- Devices must be reformatted
- Devices must be encrypted with a new encryption key
- Devices must be protected with a new PIN

Suggested guidance to include with loaned-out devices

The advice may vary depending on the circumstances of the loan, but the same basic principles apply as for any device used for data storage:

1. look after the device:
    a. take care not to lose it or leave it unattended when in public
    b. ensure that it is suitably secured (e.g. behind a locked door) when you do not have it with you
2. use only for the agreed, specific, work-related reasons
3. erase all recordings before returning the device
4. return the device by the agreed date

Version	Effective Date	Summary of changes
1	22nd July 2024	n/a first version