Title	**TELEPHONE RECORDING**			Number	**IT05**
Effective From:	02.01.11	Duration:	No end date	Review:	01.09.25
Author:	Andrew Savage			Version:	1.5
Other Ref:					
Contacts:	Simeon Hemming, Konrad Kobic,				

Version Control

(Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

DATE	***CHANGE***	***CHANGED BY***
26.03.19	Reviewed, no change	AS
24.04.21	Reviewed, no change	TP
04.10.23	Reviewed, Updated Contacts, Citations and practices.	KK

Introduction

It is good practice where demand for telephone triage outstrips demand for face-to-face consultations advanced or extended access can be offered by carrying out telephone triage. The telephone has also become an important tool enabling practices to achieve targets such as the Quality and Outcomes framework (QOF) or the GMS (nGMS).

It is good practice to use telephone recording equipment to be able to monitor and review details of any clinical consultations or complaints about staff attitude or behaviour.

Legally a business or other organisation can record or monitor phone calls but only in a limited set of circumstances relevant for that business which have been defined by the LBP Regulations. The main ones are:

- to provide evidence of a business transaction
- to ensure that a business complies with regulatory procedures.
- to see that quality standards or targets are being met in the interests of national security.
- to prevent or detect crime to investigate the unauthorised use of a telecom system.
- to secure the effective operation of the telecom system.

In addition, businesses can monitor, but not record, phone calls or e-mails that have been received to see whether they are relevant to the business (ie open an employee's voicemail or mailbox systems while they are away to see if there are any business communications stored there). For further information see the DTI website where the LBP Regulations are posted.

However, any interception of employees' communications must be proportionate and in accordance with Data Protection principles. The Information Commissioner has published a Data Protection Code on "Monitoring at Work" available on its website here. The Code is designed to help employers comply with the legal requirements of UK General Data Protection

Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) Any enforcement action would be based on a failure to meet the requirements of the act - however relevant parts of the Code are likely to be cited in connection with any enforcement action relating to the processing of personal information in the employment context. Accordingly, this Code of Practice and the Data Protection Act must also be considered by any business before it intercepts employees' communications.

The business does not have to inform its clients that recording is being done as long as the recording or monitoring is done for one of the above purposes the only obligation on businesses is to inform their own employees. If the business wants to record for any other purpose, such as market research, they will have to obtain your consent.

Good Practice

The recorded message that patients or callers to the business hear should include a statement that messages are being recorded.

Access to the call recording information must be secure and controlled by the system manager and all staff with access will be allocated a personal username and password.

Levels of access must be agreed and authorised by the Head of department.

The call recorder system is in the cloud and is maintained and backed up by Our suppliers at Mitel.

Access to the back-up facility must be controlled by the system administrator or Head of Department.

The call recording equipment must be able to identify the callers Calling Line Identity (CLI) and the telephone extension within the business that has received the call, along with the time and date that the call was received.

All recordings must be used for the purpose of the business and must not be transmitted electronically on unsecure email networks or stored on unsecure media.