Client Briefing November 2022

MS Teams – Some Considerations

Background

The Covid-19 pandemic has brought about many changes in the way Organisations work. One of the key developments has been the widespread use of platforms such as MS Teams for communication and file sharing purposes.

MS Teams was rolled out at pace as organisations balanced the need to remain functional whilst complying with social distancing requirements. MS Teams is now used widely in NHS organisations.

In this short briefing paper we note several good governance related issues which we think NHS organisations need to be aware of. In many cases these issues may already be covered in your own guidelines to staff on the use of MS Teams. However, we would recommend that guidelines do cover the following issues and are being complied with in practice.

Prompt Removal of attendees in Teams/regularly used Teams and Chats

Attendees to recurring meetings organised as Teams and Chats can stay as attendees indefinitely unless the attendee chooses to leave, or an administrator removes the attendee. This is often not a problem. However, it can mean that one-time attendees to a regular meeting may be able to access subsequent information and files posted to the Chat or Teams that they shouldn't have access to. It is therefore important that access lists are regularly reviewed by the Teams or Chat organiser to ensure the participant list is always current. The individual user can also be encouraged to leave the group themselves using the 'leave' facility in Teams Chats or the 'Leave Team' facility for Teams groups.

MS Teams governance

It is important that all NHS organisations set down their operational governance arrangements around the use of MS Teams. We would recommend this should supplement more general IT protocols and be specifically about the use of MS Teams. In particular, setting clear rules on the following are helpful:

- Ownership & Responsibilities
- The type of data which can/cannot be shared on the platform (including very clear and well communicated rules on sharing sensitive data)
- Content rules
- Creation, Structure, Hierarchy and Naming rules
- Access Management
- Retention & Archiving
- Rules on recording of meetings on Teams and how the recordings are restricted and retained.
- Apps Management

Screen Sharing

One of the real key functional treats of MS Teams is the ability to take a document from your own pc and share it live on screen with other members of the Team. This of course has some obvious pitfalls – particularly the likelihood that documentation other than that intended is selected and shared. This is a common issue and often is just an embarrassment to the presenter. But it can mean that private and confidential information that shouldn't be shared is shared amongst a wide number of people unintentionally. NHS organisations are encouraged to think about introducing protocols to reduce this risk. Organisations should think very carefully about tactics which reduce the risk of patient details being shared unintentionally – working with clinical and nursing staff. In particular there is a need to close all programs and windows down prior to any Teams meeting where you might be asked to share content from your pc.

Use of Personal Devices

Most users will use NHS kit to connect to MS Teams. However extra safeguards may need to be put in place where users access MS Teams through their own devices such as mobile phones. Each organisation needs to put in place and communicate clear policies on this. There may be technical options to strengthen the controls over this type of access e.g. by using two factor authentication controls such as passcode protection.

Set out clear well communicated rules when MS Teams Fails

MS Teams is a resilient and effective tool. However, it sometimes fails. The internet goes down, the connection is bad, the person speaking has audio that is breaking up and doesn't know (particularly if they are presenting a screenshare and not viewing the virtual audience). It is very important that there is a backup plan and that the backup plan is communicated to all attendees before the MS Teams meeting starts. Some common considerations might be:

- What happens if the technology fails completely?
- What happens if a key person (perhaps the Chair of a Meeting) has technical issues?
- How will we allow people back into meetings when their primary connection has failed? (This could involve checking that the person now accessing the meeting on their mobile phone is indeed the person having technical problems with their pc)

Think about Subject Access Requests/Freedom of Information Requests

Any data contained in Microsoft Teams is likely to be releasable under Subject Access Requests and under Freedom of Information Requests. Therefore, the same level of care needs to be taken with MS Teams content as all other content. Organisations need to think about how they will ensure (i.e. check) all MS Teams content complies with information governance policies and procedures.

Do you need Training?

As noted in the introduction – many NHS staff adopted MS Teams in March 2020 on a bit of 'sink or swim' basis – with little formal instruction or training. Perhaps now, in 2022, it is time to consider whether more structured staff training on MS Teams would be helpful in perhaps correcting any 'bad habits' and emphasising some of the key issues noted in this document.

Some useful Links

https://transform.england.nhs.uk/information-governance/faqs-on-recording-ms-teams-meetings/

https://support.nhs.net/knowledge-base/viewing-patient-records-in-microsoft-teams/

https://support.nhs.net/knowledge-base/end-to-end-encryption-e2ee-for-one-to-one-microsoft-teams-calls/