Points to consider

Inspection and assessment teams can use log-on details when on site using a provider's computer system. They should not access a provider's systems on their laptops or when off site. This is an approach we are developing.

- We are aware that you need to meet your own data governance requirements, particularly around preventing accidental changes or loss of data. Read-only access to records means you can be confident that you can prevent accidental data changes or loss.
- If you have guest log-in details for the system, you should provide these where you and the inspection team member are confident that they can independently access the records they need to see. Where available, this should be read-only access. You should not use the log-in details (including smart cards) of anyone who is not present.
- If read-only access is not available or the inspection team member needs support to use the system, you should help them to access the records they ask to see. For example, you could have a staff member available.
- Generally, where an inspection team member can access the digital records they need, they will not ask for paper copies. However, there are circumstances where you should provide hard copies, for example if waiting for a member of staff to assist would prevent them from carrying out their inspection activity. We may request specific formats where it is necessary for regulatory decision making or taking enforcement action. We will explain this request clearly.