DSA Full Audit Checklist (Editable)

Name of document:

Is the purpose of the sharing clear and necessary?

☐ Yes ☐ No Comments:

Is the amount of personal data limited to what is necessary?

☐ Yes ☐ No Comments:

Is it clear whether the sharing is for direct care, secondary purposes, or both?

☐ Yes ☐ No Comments:

If both, does the document clearly separate the two?

☐ Yes ☐ No Comments:

Is the lawful basis stated (UK GDPR Article 6 and 9)?

☐ Yes ☐ No Comments:

Is the sharing supported by contract or statutory duty?

☐ Yes ☐ No Comments:

Is the sharing consistent with the lawful basis?

☐ Yes ☐ No Comments:

Is the confidentiality position clear?

☐ Yes ☐ No Comments:

Are confidentiality boundaries and purpose limits clear?

☐ Yes ☐ No Comments:

Can all organisations involved in sharing be identified?

☐ Yes ☐ No Comments:

Are data controllers/joint controllers clearly defined?

☐ Yes ☐ No Comments:

Are data processors and agreements in place?

☐ Yes ☐ No Comments:

Is it clear what personal data is being shared?

☐ Yes ☐ No Comments:

Is there a DPIA or screening completed?

☐ Yes ☐ No Comments:

Is it clear how the sharing works and data flows?

☐ Yes ☐ No Comments:

Are access roles clearly defined?

☐ Yes ☐ No Comments:

Are contact points for queries/incidents defined?

☐ Yes ☐ No Comments:

Are dates (start/review/end) recorded?

☐ Yes ☐ No Comments:

Are patient rights clearly stated?

☐ Yes ☐ No Comments:

Are retention and deletion methods defined?

☐ Yes ☐ No Comments:

Have risks and benefits been considered?

☐ Yes ☐ No Comments: