Standard Operating Procedure (SOP)

APPROVAL AND MANAGEMENT OF DATA SHARING AGREEMENTS

SETTING	Trustwide
FOR STAFF	For staff involved in any project requiring the sharing of data and the production and management of legal documentation to facilitate this.
ISSUE	This procedure describes the steps that must be followed to approve and manage data sharing agreements involving identifiable personal data.

Standard Operating Procedure (SOP)

Overview

Where a third party has requested that the Trust enters into a data sharing agreement or an initiative is contemplated which may require the sharing of Trust identifiable personal data, a Data Protection Impact Assessment should be conducted. Subject to that any requests for, or proposals which may require, a data sharing agreement should be referred to: InformationGovernance@UHBW.nhs.uk.

Note: This SOP does not apply to DSAs done in the context of research and studies which follow Health Research Authority procedures and protocols.

Background

A DSA is required where patient identifiable data is being shared:
a) For non-care purposes and;
b) For care related purposes where one of the recipients cannot independently demonstrate assurance (e.g. by having completed a satisfactory Data Protection and Security Toolkit assessment)

In the latter case the Agreement will commit the party to appropriate standards and safeguards.

A DSA is not-required for other care related purposes (but may optionally be used) nor for mandated disclosures for secondary purposes e.g. by the Trust to NHS England/NHS Digital.

For further information see Confidential Patient Data Sharing Policy.

Template data sharing and data processing agreements are available from InformationGovernance@UHBW.nhs.uk.

Step 1 – A. Trust is leading on a DSA involving Trust Data

The requester should complete a draft DSA as fully as possible using and adapting the Trust template. When completed the documents should be submitted to Information Governance (IG) for a compliance check. IG may consult Legal Services in any case where there is uncertainty about the validity of the proposal or the safeguards required. IG will (with a response target of five days) then either:

(a) Return the documents to the requester for further development or clarification, or;

(b) Submit the proposal to the authorised signatory with a recommendation.

Step 1 – B. Trust has received a request from another party

The requester should assess the desired protocol to ensure it accurately portrays the data sharing required for the project. When complete the draft DSA and any other supporting documents to IG for a compliance check. The DPO may consult Legal Services in any case where there is uncertainty about the validity of the proposal or the safeguards required. The DPO will then (with a response target of five days) either:

(a) Return the documents to the requester for further development or clarification from the originator, or;
(b) Submit the proposal to the authorised signatory with a recommendation.

Step 2. Consideration by Authorised Signatory

The authorised signatory for each data sharing agreement depends on the type of data shared as follows:

- Patient data – Medical Director as Caldicott Guardian
- Staff data – Director of People
- Data that does not fall within these categories – Director of Finance & Information as Senior Information Risk Owner

The authorised signatory will review the proposed agreement and either:

(a) Return the documents to IG for further development or clarification from the originator, or;
(b) Approve and sign the agreement, and return a signed copy to IG

If necessary the authorised signatory may ask a review panel to discuss the appropriateness of the request and proposed DSA. The review panel should consist of subject matter leads and two of the following:

- Data Protection Officer;
- Head of Information;
- Director of Corporate Governance

The authorised signatory and available review panel members should liaise as required, either by email, telephone, or face-to-face. After deliberation the authorised signatory makes a judgement and decisions on the appropriateness of the request.

IG will add any approved agreements to the register of agreements and make a note of the timing of the next review.

Step 3. Review

All agreements should provide a primary contact within the Trust for their operation and be reviewed after an appropriate time. Review shall be the responsibility of the information asset owner and/or primary contact. IG will remind the information asset owner at least three months before the review date provided within the agreement.

Table A

REFERENCES	https://ico.org.uk/for-organisations/data-sharing-information-hub/

RELATED DOCUMENTS AND PAGES	Information Governance Policy Confidential Patient Data Sharing Policy
AUTHORISING BODY	Information Risk Management Group
SAFETY	None
QUERIES AND CONTACT	InformationGovernance@UHBW.nhs.uk 0117 34 **23701/23794**