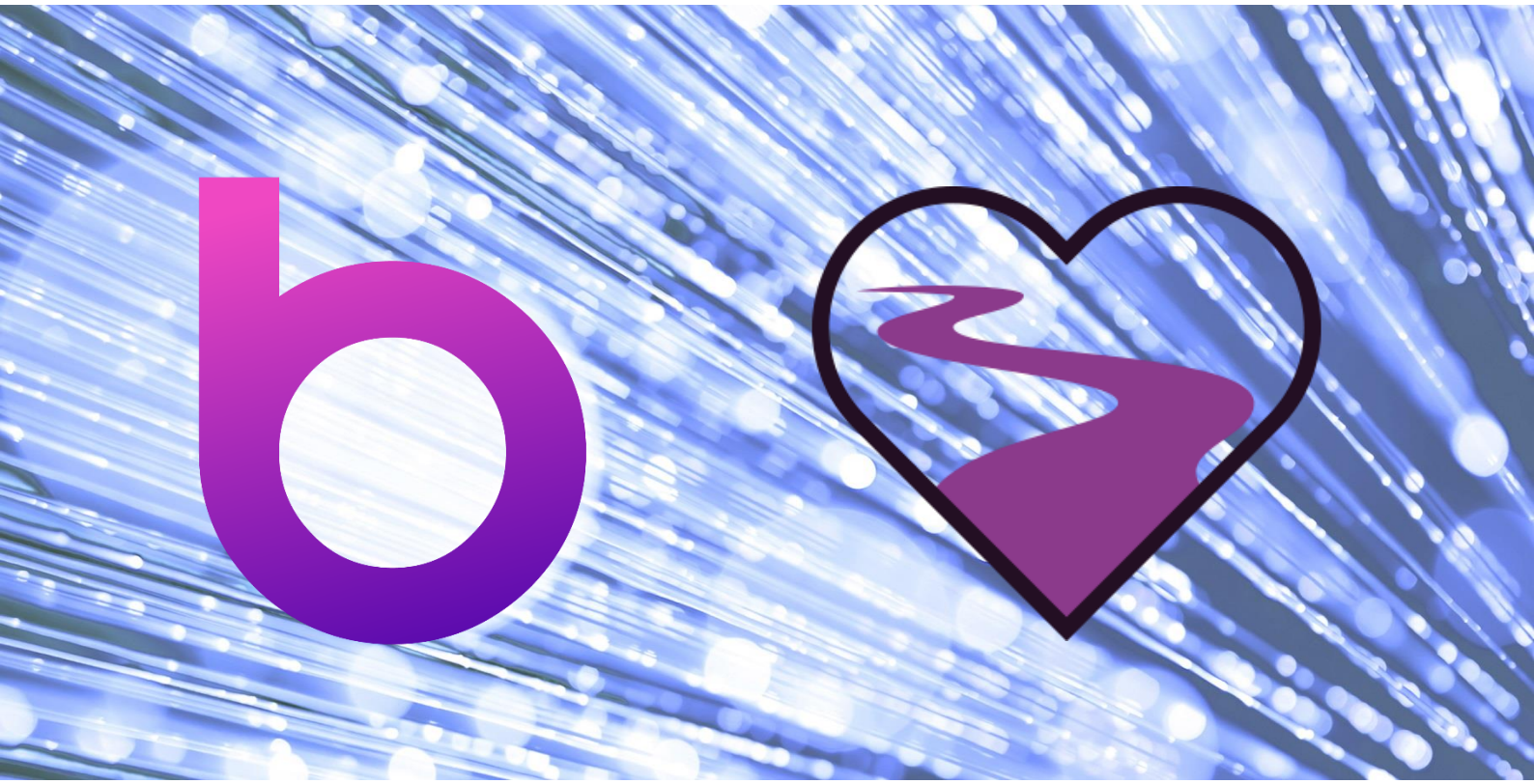
Data Handling

Upstream Outcomes Policy

(Supporting Bridgit Care & Upstream Health Business Units)

Author: D Crombie
Date: 04/04/2022
Version: 2.0



Information and technology
for better health and care

Contents

1 Background

This policy is based on NHS Digitals example policy and aligns to the recommendations and approach adopted by NHS Digital. This is based on the NHS Digital template dated 23rd May 2017.

2 Approval / update history

Version ID	Description	SIRO Approval
1.0	Initial version for release	08/10/2018 : Darren Crombie
2.0	Updated version following 2022 review	05/04/2022 : Darren Crombie

Terminology

Term	Meaning/Application
SHALL	*This term is used to state a **Mandatory** requirement of this policy*
SHOULD	*This term is used to state a **Recommended** requirement of this policy*
MAY	*This term is used to state an **Optional** requirement*

Policy

General

- *When handling data, all users **shall** do so in accordance with and be responsible for adherence to the Data Handling Policy and the Upstream Outcomes Physical Security Policy. Periodic auditing of adherence to this policy **shall** be the responsibility of the Upstream Outcomes Information Governance Team <or equivalent organisation>.*
- *Users **shall** ensure that information is appropriately marked in accordance with Government Security Classification Scheme (GSCS) and any bespoke requirements as required by the wider NHS.*
- *An approved level of protection **shall** be used in the transfer of data in relation to its level of security classification and privacy requirement.*
- *Users **shall** ensure data is transferred only to named individuals and those who need to know and that data **shall** be kept to the minimum required.*
- *Any mishandling of data in transfer or at rest **shall** be reported as an incident.*
- *Users **shall** have authority (in writing) from the Information Asset Owner (IAO) to undertake the transfer.*
- *A Data Access Agreement (DAA) or Data Sharing Agreement (DSA) **should** be produced, agreed and signed by all parties prior to any NHS data containing Personally Identifiable Information (PII) or OFFICIAL-SENSITIVE data/information being passed or shared with any non-government or non-public authority body.*
- *The Upstream Outcomes Security Team **should** be approached where there is difficulty identifying a suitable method of transfer.*

Safe Havens

The term 'Safe Haven' is used within the NHS to denote either a secure physical location or the agreed set of administrative arrangements that are in place to ensure security classified, personal or other sensitive information is communicated safely and securely.

*Safe Havens **should** be established, where:*

- *Information can be securely received and transferred.*
- *Paper-based information is stored securely in approved containers, as soon as practical.*
- *IT is not on view or accessible to unauthorised persons.*

- *All waste potentially containing security classified, personal or other sensitive information is securely retained until it can be securely disposed of or destroyed.*
- *Conversations discussing security classified, personal or other sensitive information can be held where they cannot be overhead by unauthorised persons.*

Digital/Internet Data Transfers

*In addition to the general principles above, digital transfers **shall** adhere to the following:*

- *Only approved transfer methods **shall** be used and in accordance with the Security Classification of data.*
- *Data up to and including OFFICIAL – SENSITIVE **may** be sent within the PSN and the N3/HSCN without a need for encryption.*
- *An approved method of encryption **shall** be used for the transfer of OFFICIAL – SENSITIVE data that is sent outside the secure network.*
- *An approved method of encryption **should** be used for the transfer of OFFICIAL data that is sent outside the secure network.*

Physical Data Transfers

*Physical transfers include paper and portable physical media (USB, hard disks, CDs, DVDs, etc.) In addition to the general principles above at 5.1, physical transfers **shall** adhere to the following,*

- *A Upstream Outcomes management approved method of transfer **shall** be determined for the type of data being transferred.*
- *A record of custody of transfers **shall** be kept.*
- *All data (with the exception of hard copy transfers) **shall** be stored encrypted (using a Upstream Outcomes approved method) for transfer regardless of classification.*
- *An approved method of transfer **shall** be determined for the type of data being transferred.*
- *Portable media **shall** only be authorised when there is a valid business requirement.*
- *Only official Upstream Outcomes approved removable media **shall** be used.*
- *Where information is transferred via mail the outer envelope/package **shall** not be marked with its Security Classification.*

Data Disposal

- *Information held on ICT systems **shall** be securely erased in accordance with HMG mandated requirements and the Upstream Outcomes Sanitisation, Reuse, Disposal and Destruction Policy.*
- *Information held in paper form **shall** be securely destroyed in accordance with the NHS Records Management Policy.*

Other Data Handling

- *Where there are occasions when new pieces of work require one time only data transfers or data storage, Upstream Outcomes staff **should** request guidance from a member of the Upstream Outcomes Information Security Team*

3 Key Words

Data, Destruction, Disposal, Email, Encryption, IAO, Information, IT Systems, Personal, Physical Security, Safe Haven, Security Classification, Sensitive