Difficult Airway Society

DAS Difficult Airway Database and Alert card Project

Information Governance FAQs

Consent

Do patients need to give their consent before their data is added to the database?

Patient data is collected only after explicit written consent from the patient. The consent is for:

- Sharing and storing their identifiable details (**offline**) with DAS to enable the issue of the physical Airway Alert Card.
- Storage of their pseudo-anonymised details on the DAS Airway Database to ensure safer care for their next anaesthetic **(online)**
- Optional consent for sharing anonymised data for research purposes

Is there a process if a patient wishes to access their own data?

Yes, a full report can be provided in a pdf format on request.

Can a patient request to be removed from the DAS Airway Database?

A patient can request to be removed and their details will be deleted from the DAS Airway Database. There is a link on the patient information page where they can contact us with requests to be deleted from the database.

Data Transfer

Patient Identifiable Data – offline storage

After obtaining consent from the patient the online airway alert form is completed by a clinician on the DAS Website. All patient identifiers are automatically encrypted and moved to the **offline system**. The data entry to the DAS Website generates a unique access code.

The encrypted patient identifiable data is then stored on the **offline** database.

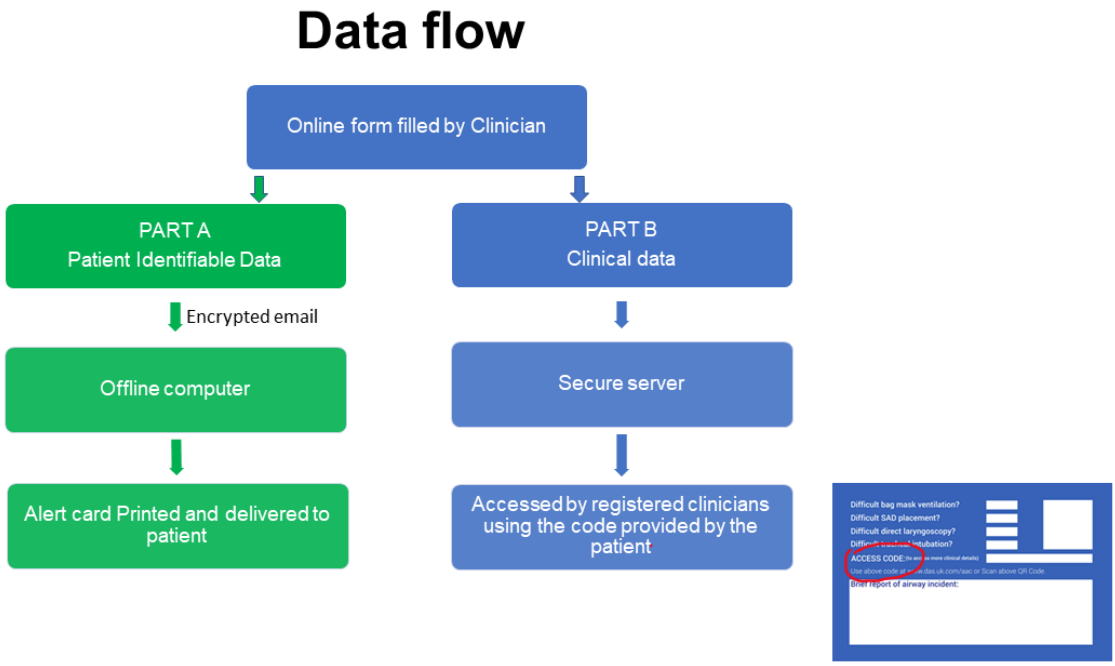
Non-identifiable data on the online system

The following information remains on the **online system:**

- Pseudonymised NHS number

- Non -patient identifiable clinical data

This data can be accessed by a clinician either with the patient's unique alphanumeric code printed on the airway alert card or using their NHS number in an emergency.



Data Storage

Are patient identifiers stored in the online DAS Airway Database?

The DAS Airway Database is a linked anonymised database which does not contain any patient identifiable information. The clinical information is matched only to:

- Age
- Gender
- A hashed version of the NHS Number – using the blowfish algorithm it is impossible to reverse this to the original NHS number

How long will the information be retained?

The DAS Airway Database contains information used for clinical purposes, this is likely to be relevant and lifesaving throughout the patient's life. An arbitrary age of 99 has been adopted as the lifetime of the data held on the DAS Airway Database – after which time the data will be automatically deleted. Patient data can be deleted if DAS is notified of a patient's death.

Difficult Airway Society

Data Access

Who will be able to access the patient details?

Only authorised users (GMC registered medical practitioners who are also registered with DAS) can access the online DAS Airway Database for clinical purposes. The Database admin team (who are information governance trained) can access the offline database for printing the alert card.

Will authorised users be able to browse through the DAS Airway Database?

Authorised users can only access details of the patient who has the Airway Alert Card, or a patient under their care against their NHS Number if their card is not available. They can also view the details of the patients that they submitted themselves. It is not possible for them to browse the rest of the DAS Airway Database.

Is access to the DAS Airway Database logged – Are these logs audited?

Each access to the DAS Airway Database is logged with details of the authorised user. The access logs are reported to the DAS Committee on a regular basis. Access generated through the use of an NHS number generates an e mail alert to the authorised user and to the DAS Administrator.

Data Security

Is the DAS Airway Database Secure?

The DAS website (which incorporates the DAS Database) uses SSL encryption technology that is used in many trusted online e-commerce websites. All secure content in the DAS website is protected by SSL and you will see the familiar green padlock symbol in your internet browser address bar when accessing secure areas on the DAS website.

Disaster and recovery process for off-line database (identifiable data)

The DAS Airway Alert Card Project computer is uniquely used for the for storing the offline data and printing the patient Airway Alert Cards. It is a Windows 10 computer operated with Bitlocker encryption. Encryption of the data is provided by PGP using public and private access keys. The offline database used is a MS Access Database which is backed up whenever a new patient is added using an encrypted portable drive. The portable drive is stored in the NHS Anaesthetic Department which is the administrative centre for the DAS Airway Alert Card Project. The password for the encrypted portable drive is known only to the project leads (currently Dr Achuthan Sajayan and Dr Fauzia Mir) and the DAS Airway Alert Card administration team.

Why was PGP chosen for encryption?

PGP is a widely used cross platform technology. It works by having paired encryption keys (x1 public and x 1 private). Messages can be encrypted using the public key – these can only be decrypted using the private key. Any data compromised would be secure as this could only be access by the public key – it could not be decrypted as the private keys are held independently.

Data Accuracy

How do you make sure the data is accurate?

The patient data is submitted by the treating clinician and they are responsible for ensuring the accuracy of the data. If they subsequently identify any inaccuracies they can contact the DAS Admin team to edit the data.