Colorectal Peritoneal Metastases (CPM) CLINICAL DATABASE PRIVACY POLICY

This policy explains what information this clinical database is collecting, how we will use it, and how we keep it secure. It only applies to information we collect when you interact with this database. No information about any individual is saved outside the database. We may change this policy from time to time so please check occasionally to ensure that you're happy with any changes. By using this clinical database, you're agreeing to be bound by this policy.

This database is gathering the data for patients that undergo surgery for peritoneal metastases, commonly Colorectal Peritoneal Metastases (CPM).

Colorectal clinicians will use the database: write to the database system administrators and ask to register with and include their patients in the CPM clinical database. The system administrator then registers the lead clinician and hospital securely through the database which generates their ID, hospital code and password login details, and act as the local Hospital Administrator responsible for the registry. Each hospital has a Hospital Administrator and this person can securely provide access to local Users who are located at the same hospital, with their own ID and password. The local users consist of other members of the clinical and research teams who also agree to follow Good Clinical Practice (GCP) and data protection regulations.

The hospital administrators' place of work and email address will be securely stored by the system but all are well known to each other outside this database. The hospital administrators' contact details will not be shared with any external party, unless the hospital administrator grants permission to do so.

Hospital Administrators can access and download the data for their hospital but do not have access to data from any other hospital. Users can only enter data for their hospital. The system administrators responsible for managing the registry have access to all the pseudo-anonymised data from all centres.

The database generates a unique identifier for each patient which provides anonymity when the data is downloaded.

The database collects the following information for each patient from the clinical team:

- Details about each patient – hospital where treated, initials, sex and date of birth.
- Pre-operative information, including previous treatments and tumour staging (CT & MRI results)
- Technical details about the operation
- Post-operative details including complications and readmissions
- Histopathology results and oncological outcomes
- Any late problems, consequent recurrence, readmissions and death

Security:

- The database is held on PAM Internet's own secure server behind a firewall and protected by anti-virus software
- Patient and hospital data that could identify a person is encrypted using Microsoft Rijndael keys and encryption libraries
- All transmissions across the internet are encrypted using https protocols through an authenticated security certificate
- Only patients assigned to the hospital of the logged-in user may be accessed

- Each user is assigned role(s) determining the information they are allowed to access

How the information will be used

The aim of the clinical database is to gather information and data on short, medium and long term outcomes after CPM treatment and compare the treatment options and results between centres. The data collected will include information regularly gathered as part of routine care provided to patients undergoing treatment for CPM. Steering group will agree on all analysis, projects and publications using the information stored in the CPM database.

CPM registry contact

If you have any questions regarding the above CPM clinical database privacy policy, then please contact faheez.mohamed@hhft.nhs.uk