FACILITATOR SITE GUIDANCE ON THE MANAGEMENT OF THE HEART MANUAL DIGITAL LOGINS

Background

Digital usernames and passwords (logins) are created and issued to Heart Manual (HM) user sites to issue to patients who have agreed to use the digital version of the HM as part of their cardiac rehabilitation programme.

This document offers guidance to user sites on how to safely and efficiently manage this process.

Scope

This document applies to sites using the digital versions of the Post-MI and Revascularisation Heart Manuals and will be referred to collectively as D-HM versions.

Responsibilities

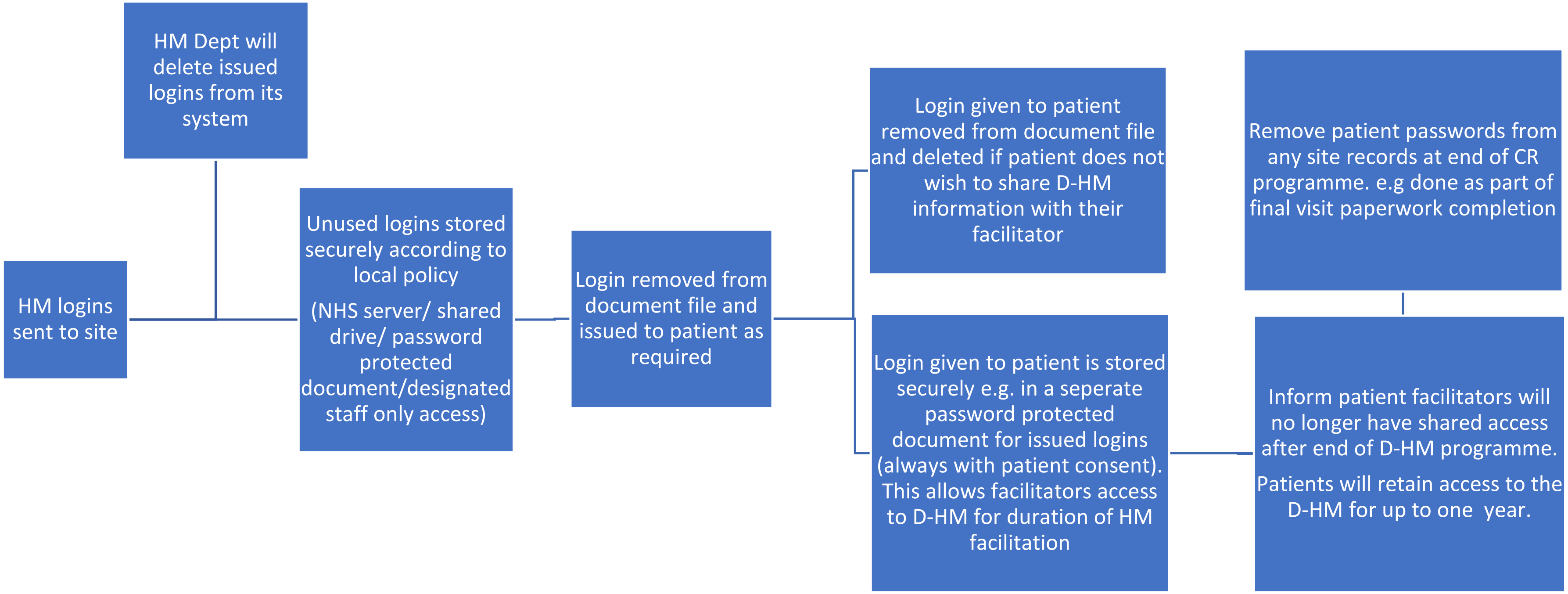
1. It is the responsibility of the HM Dept to:
    a. provide logins to user sites according to the purchase requests.
    b. delete login details once sent to site (HM Dept will not retain login details after confirmation of receipt (or after 3 months of issue to site)
    c. keep track the of number of logins issued to each site for any active orders
2. It is the responsibility of the user site to:
    a. acknowledge receipt of logins including confirmation of correct order number
    b. store logins issued by the HM Dept securely in accordance with their local IT security policies.
    c. ensure they have a process in place to track logins that have been issued to patients and those still available for allocation
    d. identify staff who have authority to access and issue logins
    e. have a process in place to securely store active patient logins where the patient has agreed to allow the CR clinical team to access their D-HM during their contact time with the site.
    f. ensure they delete user login details at the end of the D-HM programme, unless specifically agreed by the patient.

FACILITATOR SITE GUIDANCE ON THE MANAGEMENT OF THE HEART MANUAL DIGITAL LOGINS

Procedure

D-HM login will be sent electronically to a designated person. On receipt the logins must be stored securely, use of logins should be managed and all relevant staff should be aware of the process. The HM Dept will not retain login information for more than 3 months from issue to a site, therefore sites must have a robust storage process in place.

An example of a possible D-HM login storage and management process for user sites is detailed below. Sites should identify a working model for storage that meets their requirements and adheres to their local and national information governance and IT policies.



HM logins sent to site

HM Dept will delete issued logins from its system

Unused logins stored securely according to local policy

(NHS server/ shared drive/ password protected document/designated staff only access)

Login removed from document file and issued to patient as required

Login given to patient removed from document file and deleted if patient does not wish to share D-HM information with their facilitator

Login given to patient is stored securely e.g. in a seperate password protected document for issued logins (always with patient consent). This allows facilitators access to D-HM for duration of HM facilitation

Remove patient passwords from any site records at end of CR programme. e.g done as part of final visit paperwork completion

Inform patient facilitators will no longer have shared access after end of D-HM programme.

Patients will retain access to the D-HM for up to one year.

If you require any further information please contact the HM Dept.