Integrated Patient Management System (iPMS)

User Access Control Policy

Saolta University Health Care Group

Community Healthcare Organisation (CH CDLMS)

Community Healthcare West (CHO 2)

This policy may be updated at any time (without notice) to ensure changes to the HSE's organisation structure and/or business practices are properly reflected in the policy.

Document Information

Title:	**Integrated Patient Management System User Access Control Policy – Saolta University Healthcare Group, CH CDLMS and CHO 2**
Purpose:	To define the correct assignment and management of user access controls applied for those being granted access to the iPMS across the Saolta University Health Care Group, Community Healthcare Group (CH CDLMS and Community Healthcare West (CHO2).
Authors:	Jointly developed in consultation with key stakeholders across the Saolta University Health Care Group, Community Healthcare Organisation 1 (CH CDLMS) and Community Healthcare West (CHO2). • Ross Cullen, ICT and Digital Health Manager (Community Healthcare West) • Anne Keary, Digital Health Lead (Community Healthcare West) • Fiona McHugh, Interim Group PAS Business Implementation Lead, Saolta University Health Care Group • Marie Doorly, Saolta iPMS Training Manager. • Martin Murphy, Technology Manager, Galway University Hospital • Gabriel T. Gormley, IT Manager (Sligo University Hospital) • Trevor Carlin, IT and Applications (Letterkenny University Hospital) • Mark Boland, iPMS Project Manager / Executive iPMS Application Lead for CHO and Saolta • Sinead Molloy, Digital Health Manager CH CDLMS • Niamh Mackin, CHO 2 iPMS Implementation team, (Portfolio Management Office, Community Healthcare West) • Dawn Fletcher, Project Officer, Ballinasloe Ambulatory care Hub, Community Healthcare West
Publication date:	27/01/2023
Target audience:	All iPMS users across Saolta University Health Care Group, Community Healthcare Organisation (CH CDLMS) and Community Healthcare West (CHO 2)
Related documents:	HSE Access Control Policy (2013)
Review date (due):	27/01/2025
Contact details:	Mark Boland, iPMS Project Manager / Executive iPMS Application Lead for CHO and Saolta

Document History/Changelog

Version	Author	Change Details	Date
0.1	A Keary	Initial template and partial draft in line with HSE Access Control (2013) policy	12/08/2022
0.2	A Keary	Insertion of Table of Contents and several changes made to each section, including Appendices	16/08/2022
0.3	A Keary	Minor changes	26/08/2022

Document History (continued)

Version	Author	Change Details	Date
0.4	A Keary	• Purpose - Insertion link for HSE Access Control (2013) policy • Font type, font size, and 1.5 line spacing applied • 4.7: Monitoring and Review - Comments inserted for discussion with iPMS teams • 6.0 Enforcement - Comments inserted for discussion with iPMS teams • Updated User Access Form • Reviewed definitions and updated Table of Contents	05/09/2022
0.5	A Keary	• Addition of CH CDLMS ECC hubs into iPMS (Group PAS) User Access Form (Appendix C) • Minor changes throughout document • Information updated appropriately from sections 4.3.2 to 4.6, including insertion of web links • Link inserted in section 5.2 • Updated Table of Contents	06/09/2022
1.0	A Keary	Initial Version with tracked changes for review	06/09/2022
1.1	R Cullen	Minor Changes	12/09/2022
1.2	A Keary	• Committed tracked changes • Combined Change Log and Description tables • Updated Appendix C	21/09/2022
1.2	A. Keary	Minor amendments	28/09/2022
1.3	A. Keary	Minor Changes	29/09/2022
1.4	R. Cullen	Minor Changes and formatting	29/09/2022
1.5	A. Keary	Minor changes	05/10/2022
1.6	A. Keary	Minor changes	07/11/2022
1.7	A. Keary	Minor changes following feedback from group members	14/12/2022
1.8	A. Keary	Minor changes following iPMS DPIA feedback from Deputy Data Protection	09/01/2023
1.9	A. Keary	Minor changes to reflect Deputy Data Protection feedback	13/01/2023
1.10	A. Keary	Minor changes throughout document	17/01/2023
1.11	S. Molloy	Minor changes to reflect CH CDLMS	17/01/2023
1.12	iPMS Group	Group included: F. McHugh, S. Molloy, M. Murphy, M. Boland, D. Fletcher, R. Cullen and A. Keary. Reviewed full policy and made amendments as required. For final circulation.	17/01/2023

1.13	N. Mackin	All tracked changes accepted, and feedback from iPMS CHW team applied	18/01/2023
1.14	M. Boland A. Keary S. Molloy	Minor amendments to Appendix C	26/01/2023
1.15	A. Keary	Minor amendments to Appendix C Minor amendments to Appendix B	27/01/2023
1.16	M. Boland	Minor amendments to Appendix B and C	30/01/2023
1.17	A. Keary	Minor amendments to Appendix C	31/01/2023
1.18	A. Keary	Minor amendments to Appendix C and insertion of Appendix D	20/02/2023
1.18	A. Keary	Feedback from Saolta iPMS Trainer (M. Doorly)	10/03/2023
1.19	A. Keary	Amendments to User Access Form	10/03/2023
1.20	A. Keary/D. Fletcher	New revised iPMS user Access form based on Cork University Hospital template and also includes option for access removal. Updated 4.2, 4.3, and 4.5 accordingly to reflect granting access and removal of access.	17/04/2023
1.21	M. Boland	Appendices B and C updated and tracked changes committed.	18/04/2023
2.0 Final	A. Keary	Final version of policy	18/04/2023

Table of Contents

1.0 Purpose

The Health Service Executive (HSE) is legally required under the Irish Data Protection Act 2018 and the General Data Protection Regulation (GDPR) (EU) 2016/679 to ensure the security and confidentiality of information it processes on behalf of its service users, patients and employees. In line with the HSE Data protection Policy (Link), the *HSE Access Control Policy (2013)* and the *Sláintecare Implementation Strategy and Action Plan 2021-2023 Strategy* (Link) the Saolta University Health Care Group, CHO Area 1(CH CDLMS) and CHO Area 2 have jointly developed the Integrated Patient Management System (iPMS) User Access Policy to demonstrate their commitment to the correct use and management of access controls being applied to iPMS across the Saolta University Health Care Group, CH CDLMS and CHO 2 services. This policy outlines the specific supplementary aspects required around the access and usage of iPMS and at the same time, our requirement to comply with the mandatory *HSE Access Control Policy (2013)* (Link). Insufficient access controls or unmanaged access to iPMS information could lead to the unauthorised disclosure or theft of this information, fraud and possible litigation.

The purpose of this policy is to define the correct use and management of user access controls assigned to users requiring access to the integrated Patient Management System (iPMS) and keeping in line with the *HSE Access Control Policy (2013).* This policy is mandatory and by accessing iPMS, users are agreeing to abide by the terms of this policy.

2.0 Scope

All facilities across the Saolta University Health Care Group, CHO Area 1(CH CDLMS) and Community Healthcare West (CHO Area 2) who have implemented iPMS Patient Administration System (PAS) as part of their digital operations for managing service user care delivery are required to adhere to this policy.

This policy represents the HSE West and North West regional positions and applies to all iPMS users across the following areas:

All HSE staff across Saolta University Health Care Group;
All HSE staff across Community Healthcare Organisation 1 (CH CDLMS);
All HSE staff across Community Healthcare West (CHW) (CHO2);

This policy also applies to all connections to (locally and remotely) HSE network domains (LAN/WAN/Wi-Fi) for the purpose of accessing iPMS.

3.0 Definitions

List of terms used throughout this policy are defined in *appendix A*.

4.0 Policy

4.1 Principles of Access Control

In line with the HSE Access Policy (2013), the following principles apply:

iPMS system is always password protected;
iPMS must have a designated system administrator(s) who is responsible for managing and controlling access to iPMS.
Designated system administrator(s) are responsible for the day-to-day administration of iPMS, including the creation and management of system access accounts for authorised users. Refer to *appendix B* for a list of designated system administrators. There is a requirement that any new or existing system administrator(s) are included within appendix B and a copy of this policy be held within each department.

The ICT Directorate is the designated owner of all HSE network domains. Each HSE network domain must have a designated network administrator(s) who is responsible for the day-to-day administration of the network domain, including the creation and management of network domain access accounts for authorised users.

Access to iPMS must be strictly controlled by a formal written user access authorisation request form and equally comply with the de-registration process.
Access to iPMS and networks must be strictly controlled by a formal written registration and de-registration process and will be outlined within this policy.
Access to iPMS must by controlled by the use of individual user access accounts. The use of generic or group access accounts to access iPMS is strictly prohibited.

Access to HSE network domains will generally be controlled by the use of individual user access accounts.

4.2 Account Privileges

In line with the HSE Access Control Policy (2013) the following outlines iPMS account privileges:

Access rights and privileges applied to iPMS users and network domains must be allocated based on the specific requirement of a user's HSE role / function rather than on their status. The patient / service user journey throughout the service / intervention being provided should also be integral to access rights and privileges being applied to a user account.
The criteria used for granting access privileges must be based on the principle of "least privilege" whereby authorised users will only be granted access to iPMS which are necessary for them to carry out the responsibilities of their HSE role or function as defined by their line manager.
Care must be taken to ensure that access privileges granted to iPMS users do not unknowingly or unnecessarily undermine essential segregation of duties.
Care must be taken to ensure that access privileges granted to iPMS users do not unknowingly or unnecessarily prevent access to key clinical data throughout a patient's journey of the service/intervention being provided.
The creation of iPMS user access accounts with special privileges such as system administrators must be rigorously controlled and restricted to only those users who are responsible for the management or

maintenance of iPMS. Each system administrator must have a specific admin level account, which is only used for system administrative purposes, and is kept separate from their iPMS standard user access account.

4.3 Account Registration

In line with the HSE Access Control Policy (2013) the following section outlines requirements around account registration processes.

4.3.1 iPMS Access Accounts

In line with the HSE Access Control Policy (2013) the following outlines iPMS Access Accounts:

Access to iPMS will be controlled by the use of individual user access accounts. The use of generic / group access accounts is not permitted under any circumstances on iPMS.
All new requests for access to iPMS must be made in writing using the iPMS (Group PAS) User Access Request Form. Refer to *appendix C*.
Only staff with a HSE email can be authorised access to iPMS. Line managers must ensure that where a staff member does not yet have a HSE email that this is set up in advance of submitting a completed iPMS (Group PAS) User Access Request Form. Refer to *appendix C*..
Line managers must complete the request on behalf of any HSE staff who require access to iPMS and issue to the designated system administrator(s) or Ivanti as outlined in appendix C. The request must be clearly marked 'New Access'.
System administrators must only create new iPMS user accounts when they have received a fully authorised iPMS User Access Request Form from the line manager. Where additional access is required for other acute or community locations, page 2 of the iPMS User Access Request Form must also be completed. Refer to a*ppendix C*.

4.4 Account Management

In line with the HSE Access Control Policy (2013) the following outlines account management:

Requests from users for password resets must only be performed once the user's identity has been verified by the designated system administrator (for example: a user's identity may be verified by providing their email address and unique identifier).
Existing iPMS users who require additional access privileges on iPMS must obtain the written authorisation from the line manager. The request must be clearly marked 'Amend Current Access' to avoid the creation of multiple accounts for the same user.
The access accounts of users taking career breaks, going on maternity leave or those on long term sick leave must be suspended until such a time as they return to work. Requests for account suspensions must be made in writing by the user's line manager using the HSE Suspend / Remove Access Request Form (Link) and forwarded to the appropriate system administrator(s).The request should be clearly marked 'Suspend User Account'.
The access accounts of users who are about to change roles or transfer to another HSE directorate or service area, must be reviewed to ensure access account privileges that are no longer required by the user in their new role are removed. In such circumstances, the user's existing line manager must request the

removal of the unnecessary account privileges. Unnecessary account privileges can be removed by completing page 3 of the User Access Form, and forwarded to the appropriate system administrator before the user changes role or transfers. The request should be clearly marked 'Delete user account privileges'.

4.5 Account De-Registration

As soon as a user leaves the employment of the HSE all his/her information systems, including iPMS and network access accounts must be revoked immediately.
Line managers must request the deletion of a user's iPMS accounts as soon as they have been informed by the user that they are leaving the employment of the HSE. The requests must be made in writing using the page 3 of the iPMS User Access Form (refer to appendix C) and forwarded to the relevant system administrator(s). The request should be clearly marked 'Delete User Account' and made in advance of the user's last day.
iPMS System administrators must revoke iPMS user accounts at the requested date and time after the receipt of a properly completed form.

4.6 Security

Access to all information systems, including iPMS must be controlled via strong password authentication schemes.
User access accounts must be created in such a way that the identity of each iPMS user can be established at all times during their usage. Each user access account must be unique and consist of at least a username and password set. All passwords created must be in line with the requirement of the HSE Password Standards Policy (2013) (link).
Where possible all HSE information systems, including iPMS must be configured to:
Force users to change their password at their first logon. Where this is not possible, users must be instructed to manually change their password the first time they logon to iPMS.
Automatically 'lock' a user account after a number of consecutive failed login attempts.
Automatically 'lock' or log out user accounts after 30 minutes of inactivity. Where this is not possible, users must be instructed to manually log off or 'lock' their HSE computer device (using Ctrl+Alt+Delete keys) when they have to leave it unattended for any period of time and at the end of the each working day.
Audit logging and reporting must be enabled on all information systems.

4.7 Monitoring and Review

Information owners or their nominees must continually monitor access to iPMS. They must perform quarterly reviews of the systems they are responsible for to ensure:
That each user access account and the privileges assigned to that account are appropriate and relevant to that user's current role or function;
That iPMS and the information processed by the system is only accessed and used by authorised users for legitimate reasons.
System administrators must conduct a system review at least once every quarter. iPMS User access accounts which have been inactive for 60 consecutive days or more must be suspended unless instructed otherwise by the user's line manager.
Suspended user accounts which have not been reactivated within a 12 month period should be marked for deletion, unless instructed otherwise by the user's line manager.

5.0 Roles and Responsibilities

5.1 System Administrator(s)

In line with the HSE Access Control Policy (2013), each system administrator is responsible for:

Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation;
All system administrators must attend dedicated iPMS training/induction prior to working as a system administrator or user. This training must incorporate Data Quality Training.
User accounts will only be set up and activated once a user has attended iPMS training/induction.
All system administrators must adhere to completing the mandatory GDPR training module available on HSELanD.
Taking appropriate and prompt action on receipt of requests for iPMS user registration, change of privileges, password resets and de-registration of users in accordance with this policy and the procedures for iPMS;
Taking appropriate and prompt action on receipt of requests for the suspension of an iPMS user account in accordance with this policy and the procedures for iPMS;
Ensuring all passwords generated for new user accounts and password resets meet the requirements of the HSE Password Standards Policy (2013) (link).
Notifying iPMS users of their system account details in a secure and confidential manner;
Ensuring that appropriate records of iPMS system activity, including all authorised iPMS user registrations, change of privileges and de- registration requests are maintained and made available for review to the appropriate personnel;
Conducting periodic review of iPMS in which they are responsible for in accordance with this policy;
Notifying the site IT manager if they suspect an iPMS user is responsible for misusing iPMS or is in breach of this policy;
Informing their site IT manager immediately in the event of a security incident involving iPMS;
Complying with instructions issued by the ICT Directorate on behalf of the HSE.

5.2 ICT Directorate

The ICT Directorate is responsible for:

The management, control, ownership, security and integrity of all HSE network domain (LAN/WAN) on behalf of the HSE;
The implementation of the HSE Access Control Policy (2013) and all other relevant policies within the ICT Directorate;
Ensuring adequate procedures are in place to ensure compliance with the HSE Access Control Policy (2013) all other relevant policies;
Designating a network administrator(s) for each HSE network domain;

5.3 Line Managers

In line with the HSE Access Control Policy (2013), each Line Manager is responsible for:

The implementation of this policy and all other relevant HSE policies within the business areas for which they are responsible;
Ensuring that all members of staff who report to them are made aware of and are instructed to comply with this policy and all other relevant HSE policies;
Ensure that staff requiring access to iPMS have a HSE email set up as per local policy prior to submitting a completed iPMS User Access Form;
Ensuring complete and timely iPMS user access requests, for both permanent and temporary staff, are forwarded to the designated system administrator allowing sufficient time for the creation of the required iPMS user account prior to the user's start date;
Ensuring that each user that requests access fulfils all the criteria (principle of "least privilege") for being granted access to iPMS;
Ensuring they make timely requests for the suspension of all iPMS user accounts belonging to members of their staff who are taking a career break, going on maternity leave or leave or those on long term sick leave;
Ensuring they make timely requests for the deletion of all iPMS user accounts belonging to members of their staff who are leaving the employment of the HSE;
Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.4 Users

In line with the HSE Access Control Policy (2013) each iPMS user is responsible for:

Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation;
All users must attend dedicated iPMS training/induction prior to gaining access to iPMS. This training must incorporate Data Quality Training.
User accounts will only be activated once a user has attended the required iPMS training/induction.
All system administrators must adhere to completing the mandatory GDPR training module available on HSELanD.
Respecting and protecting the privacy and confidentiality of iPMS they access, and the information processed by iPMS;
Ensuring that they only uses iPMS user access accounts and passwords which have been assigned to them;
Ensuring all passwords assigned to them are kept confidential at all times and not shared with others including their co-workers or third parties;
Changing their passwords at least every 90 days or when instructed to do so by designated system administrator(s);
Users to log out/lock their device when unattended so that others cannot access iPMS to carry out transactions either intentionally or inadvertently.
Reporting all misuse and breaches of this policy to their line manager.

6.0 Enforcement

The HSE reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. HSE staff, who breach this policy may be subject to disciplinary action, including suspension and dismissal as provided for in the HSE disciplinary procedure.

The HSE will refer any use of its I.T. resources for illegal activities to the Gardaí.

7.0 Review and Update

This policy will be reviewed and updated two yearly or more frequently if necessary to ensure any changes to the HSE's organisation structure and business practices are properly reflected in this policy.

Appendix A: Definitions

Access: All local or remote access to the Integrated Patient Management System (iPMS).

Authorisation / Authorised: Official HSE approval and permission to perform a particular task.

Backup: The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure or loss/theft etc.

CH CDLMS (CHO Area 1: Community Healthcare Organisation 1 – all community services across counties Cavan, Donegal, Leitrim, Monaghan and Sligo

CHO Area 2: Community Healthcare Organisation 2 – all community services across counties Galway, Mayo and Roscommon

CHW: Community Healthcare West (otherwise known as CHO Area 2 or CHO 2 for short)

Confidential information: (As defined by the *HSE Information Classification and Handling Policy*) Information which is protected by Irish and/or E.U. legislation or regulations, HSE policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact the HSE, its patients, its staff and its business partners. Some examples of confidential information pertaining to iPMS include: Patient / client / staff personal data (Except that which is restricted)

Patient /client / staff medical records (Except that which is restricted)

Staff personal records

Draft reports

Audit reports

Vendor contracts / Commercially sensitive data

Data covered by Non-Disclosure Agreements

Passwords / cryptographic private keys

Data collected as part of criminal/HR investigations

Incident Reports

Dedalus: Software vendor for the iPMS system. iPMS was previously owned by DXC and iSoft**.**

GUH: Galway University Hospitals

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the HSE.

Information System: A computerized system or software application used to access, record, store, gather and process information.

iPMS: Integrated patient Management System

Line manager: The individual an iPMS user reports directly to.

LUH: Letterkenny University Hospital

PUH: Portiuncula University Hospital Privacy

Privacy: The right of individual or group to exclude themselves or information about themselves from being made public.

Process / processed / processing: Performing any manual or automated operation or set of operations on information including:

Obtaining, recording or keeping the information;

Collecting, organising, storing, altering or adapting the information;

Retrieving, consulting or using the information;

Disclosing the information or data by transmitting, disseminating or otherwise making it available;

Aligning, combining, blocking, erasing or destroying the information.

Remote Access: Any Connection to the HSE network(s) or information systems that originates from a computer or device located outside of the HSE network.

Restricted Information: (As defined by the *HSE Information Classification and Handling Policy*) Highly sensitive confidential information**.** The unauthorised or accidental disclosure of this information would seriously and adversely impact the HSE, its patients, its staff and its business partners. Some examples of restricted information include:

Patient / client / staff sensitive restricted information (i.e. mental health status, HIV status, STD/STI status etc.)

Childcare / Adoption information

Social Work information

Addiction Services information

Disability Services information

Unpublished financial reports

Strategic corporate plans

Sensitive medical research

RUH: Roscommon University Hospital

Saolta University Health Care Group: Includes the following acute hospitals: Galway University Hospitals, Portiuncula University Hospital, Roscommon University Hospital, Mayo University Hospital, Sligo University Hospital and Letterkenny University Hospital.

SUH: Sligo University Hospital

System Administrator: The individual(s) charged by the designated system owner with the day to day management of HSE information systems. Also includes the HSE personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the HSE to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the HSE.

Users: Any authorized individual using any of the HSE's IT resources.

Appendix B: List of iPMS system administrators / super users across Saolta University Health Care Group, Community Healthcare organisation 1 (CH CDLMS) and Community Healthcare West (CHW) (CHO 2)

Location	Name of designated system administrator(s)
Saolta / CHO	Mark Boland
Galway University Hospital	Siobhan Trowell Christina Eifert Nora Ann Cosgrove
Portiuncula University Hospital	Siobhan Moloney Lisa Creaven
Roscommon University Hospital	Paul O Dowd Pauline Conroy
Mayo University Hospital	Mary Casey Louise Rawson Tim Ganley
Sligo University Hospital	Gary McCormack Imelda Mchale Farnan Golden Grainne Wyer
Letterkenny University Hospital	Geraldine O'Donnell Malachy McKinney Frank Haugh
CHO 2 (Project team for Mental Health and Older Persons)	Donna Corcoran Niamh Mackin
CHO 2	Dawn Fletcher Marie Philbin Tom Haddock Kate Gaffney
CH CDLMS (CHO 1)	TBC

(The above list of system administrators is likely to change regularly. Note this list is accurate as per March 2023).

Appendix C: iPMS (Group Patient Administration System) User Access Request Form

Saolta

Cúram Sláinte Phobail, Iarthar
Community Healthcare West

CÚRAM SLÁINTE POBAIL
COMMUNITY HEALTHCARE

iPMS System Access Request Form

New Access: ☐ Amend Current Access: ☐ (if yes, supply Citrix Logon)

Username\email address: _____

This form is used to grant, amend and remove access to the HSE Patient Administration System, iPMS. The form must be completed (Block Capitals or typed) by a user and signed by their line manager. Completed forms should be forwarded to **iPMS System Administrator, IT Department (refer to page 3). Please note that incomplete or illegible forms will be returned to sender.**

Section 1 is for system access within your own current location. Section 2 is for External Hospital/Facility system access. Section 3 is for Removal of Rights.

Section 1:

User Details		
First Name:	Job Title:	HSE Personnel Number:
Last Name:	Department:	Mobile/landline/Ext No./Bleep:
Medical Council/NMBI/CORU Number:	Please state the name of your Hospital/Facility:	
HSE Email Address Required:		
Laptop/PC Asset Tag Number Required:		

iPMS Access	Please tick if required (✓)
Patient Details	
Create\Update Patient Demographics	
View Only Patient Demographics	
Appointments	
Make OPD Appointments	
View Only Appointments	
Clinic Diary Manager (Add Slots\ Clinics on hold etc.)	
Waiting Lists	
Create\Edit Waiting List Entry	
View Only Waiting List Entry	
PDT Chart Tracking	
Create a new patient document type	
View Chart Tracking	
Patient record Enquiry (General Overview)	
Patient Record Enquiry	
Other (please specify in detail):	

iPMS Access	Please tick if Required (✓)
Emergency Department	
Create ED Attendances	
View only ED Attendances	
Alerts	
Create Alerts	
Edit Alerts	
View only Alerts	
Inpatients	
Admit\Transfer\Discharge Patients	
Ward View Only	
Theatre	
Theatre View	
Theatre Booking Rights	
Billing & Finance	
Billing View	
Edit Billing	

User Declaration		
I have read and understood the Health Service Executive policies governing the user of its IT resources, and I agree to be bound by the terms therein. I acknowledge that the access to personal information is subject to (a) that I will only access data relevant to a specific patient contact and (b) that I will adhere to my duty of confidentiality to the individual involved. I understand that I may be subject to the HSE's disciplinary procedures should I fail to comply with these obligations. I agree that I will also adhere to the iPMS User Access Policy.		
Name:	**Signature:**	**Date:**

Line Manager declaration and authorisation – unsigned forms will be returned	
Declaration: I certify that I know this staff member and requires access to iPMS.	
Operational Lead/Clinical Manager Name:	**Operational Lead/Clinical Manager Signature:**
Direct Tel No:	**Date:**

Section 2:

Please note, Section 2 is ONLY to be completed if requesting access to another hospital/facility besides your main base. Please specify full reasons as to why this access is required – access will only be granted in valid/exceptional circumstances.

User Details		
First Name:	Job Title:	HSE Personnel Number:
Last Name:	Department:	Mobile/landline/Ext No./Bleep:
Medical Council/NMBI/CORU Number:	Please state the name of your Hospital/Facility:	
HSE Email Address Required:		
Laptop/PC Asset Tag Number Required:		
External Hospital/Facility that Access is Required for:		

iPMS Access	Please tick if required (✓)
Patient Details	
Create\Update Patient Demographics	
View Only Patient Demographics	
Appointments	
Make OPD Appointments	
View Only Appointments	
Clinic Diary Manager (Add Slots\ Clinics on hold etc.)	
Waiting Lists	
Create\Edit Waiting List Entry	
View Only Waiting List Entry	
PDT Chart Tracking	
Create a new patient document type	
View Chart Tracking	
Patient record Enquiry (General Overview)	
Patient Record Enquiry	
Other (please specify in detail):	

iPMS Access	Please tick if Required (✓)
Emergency Department	
Create ED Attendances	
View only ED Attendances	
Alerts	
Create Alerts	
Edit Alerts	
View only Alerts	
Inpatients	
Admit\Transfer\Discharge Patients	
Ward View Only	
Theatre	
Theatre View	
Theatre Booking Rights	
Billing & Finance	
Billing View	
Edit Billing	

You must provide below detailed reason(s) for External Facility access

User Declaration

I have read and understood the Health Service Executive policies governing the user of its IT resources, and I agree to be bound by the terms therein. I acknowledge that the access to personal information is subject to (a) that I will only access data relevant to a specific patient contact and (b) that I will adhere to my duty of confidentiality to the individual involved. I understand that I may be subject to the HSE's disciplinary procedures should I fail to comply with these obligations. I agree that I will also adhere to the iPMS User Access Policy.

Name:	Signature:	Date:

Line Manager declaration and authorisation – unsigned forms will be returned

Declaration: I certify that I know this staff member and requires access to iPMS.

Operational Lead/Clinical Manager Name:	Operational Lead/Clinical Manager Signature:
Direct Tel No:	Date:

Section 3:

Please note, Section 3 is to be completed if requesting removal of access rights from a user account in line with requirements for job role.

User Details		
First Name:	Job Title:	HSE Personnel Number:
Last Name:	Department:	Mobile/landline/Ext No./Bleep:
Medical Council/NMBI/CORU Number:	Please state the name of your Hospital/Facility:	
HSE Email Address Required:		
Laptop/PC Asset Tag Number Required:		

iPMS Access	Please tick if to be removed (✓)	iPMS Access	Please tick if to be removed (✓)
Patient Details		**Emergency Department**	
Create\Update Patient Demographics		Create ED Attendances	
View Only Patient Demographics		View only ED Attendances	
Appointments		**Alerts**	
Make OPD Appointments		Create Alerts	
View Only Appointments		Edit Alerts	
Clinic Diary Manager (Add Slots\ Clinics on hold etc.)		View only Alerts	
Waiting Lists		**Inpatients**	
Create\Edit Waiting List Entry		Admit\Transfer\Discharge Patients	
View Only Waiting List Entry		Ward View Only	
PDT Chart Tracking		**Theatre**	
Create a new patient document type		Theatre View	
View Chart Tracking		Theatre Booking Rights	
Patient record Enquiry (General Overview)		**Billing & Finance**	
Patient Record Enquiry		**Billing View**	
Other (please specify in detail):		**Edit Billing**	
External Hospital that Access is Required for:			

User Declaration		
I am declaring that I no longer require access to the above iPMS modules.		
Name:	**Signature:**	**Date:**
Operational Lead/Clinical Manager Name:	**Operational Lead/Clinical Manager Signature:**	
Direct Tel No:	Date:	

RETURN COMPLETED FORMS TO:

Location	Contact Details
Galway University Hospitals requests	IPMSGUH.Support@mailn.hse.ie
Roscommon University Hospital requests	Roscommon.ipmssupport@hse.ie
Portiuncula University Hospital requests	Ipms.portiuncula@hse.ie
Mayo University Hospital requests	MUH.InformationServices@hse.ie
Sligo University Hospital requests	applicationsupport.suh@hse.ie
Letterkenny University Hospital requests	Log a ticket to Ivanti and attach completed form or systemsluh@hse.ie
CHO 2 (CHW) – Older Persons & Mental Health requests	CHWiPMS.SupportTeam@hse.ie
CHO 2 (CHW) – ECC related requests	ipmssupport.chw@hse.ie
CHO 1 (CH CDLMS) requests	Coming soon