Community Connect
IT System Access Request

HOUSTON Methodist LEADING MEDICINE

Important:

- *This form must be signed by your sponsoring Community Connect physician.*
- *All fields below are required. Incomplete forms will not be accepted.*
- *Please include a signed HM Confidentiality and Information Security Agreement (page 2).*
- *This form is not for providers.*

Select the appropriate boxes.

Community Connect role:

- ☐ Office Staff
- ☐ Clinical Staff
  Type _____ (e.g., RN)
- ☐ Billing
- ☐ Office Manager

Anticipated start date: _____

This request is for:

- ☐ New user access
- ☐ Current HM network ID (if any): _____
- ☐ Legacy 365 SharePoint remittance files (**Service Desk** – please route this request type to the IT SharePoint Team)
- ☐ SharePoint access for Billing extract files (**Service Desk** – please route this request type to the IT SharePoint Team)

Complete the following information. All fields are required.

First Name _____ Middle Initial____ Last Name _____

Title _____ Mobile Number _____

Email address (required) _____

For future communications, the best way to contact me is via my:

- ☐ Mobile phone
- ☐ Email address

Practice Name _____ Customer ID _____

Office Address _____ Suite # _____

City _____ Zip _____

Office Phone _____ Office Manager _____

_____ _____
Your signature Date

_____ _____
Printed name and signature of sponsoring physician Date

HOUSTON Methodist LEADING MEDICINE

Confidentiality & Information Security Agreement

I understand that through my work or association with Houston Methodist (HM), I have an ethical and legal responsibility to protect the privacy of all patients and employees and to safeguard the confidentiality of their health and other sensitive information. This protection also extends to members of HM's health plans. In addition, I understand that HM information systems and all HM confidential and proprietary information are to be regarded as valuable resources. I will provide all necessary safeguards for the information to be kept secure from theft, misuse and unauthorized reproduction, modification or destruction. I understand that the Houston Methodist Information Technology Division conducts information system security checks and that certain activities, such as unsuccessful log-in attempts, email usage or Internet usage may be monitored.

I understand that failure to comply with this agreement may result in the termination of my employment or association with HM and/or civil or criminal legal penalties.

I AGREE THAT I WILL:

1. Not disclose confidential or proprietary information to any individuals who aren't authorized to receive the information or to those who don't have a legitimate need to know, in order to provide patient care or to carry out their duties with HM.
2. Protect the privacy and confidentiality of our patients, employees and members of our group health plans.
3. Not disclose or share any confidential information, even if I'm no longer associated with HM.
4. Not access, change or destroy confidential or proprietary information except as required to perform my job or service.
5. Know that my use of HM information systems to access confidential information may be audited and that HM may take away my access at any time.
6. Dispose of documents or other media when no longer needed, in a way that protects confidentiality (shredding, etc.). I will follow the correct department procedure, where applicable.
7. Access only levels or components of the information system as assigned to perform my job or service.
8. Keep my password(s) secret and not share it (them) with anyone. If I suspect that my password is known, I will immediately change it so as not to compromise computer security.
9. Protect the integrity of the electronic health record (EHR) and will:
    - Not modify or correct my own personal medical record in any way.
    - Not create any test/fake patients in a system that's already live.
    - Not create a test/fake visit on an existing patient.
10. Not install, transmit or download from the Internet onto any HM information system, any unauthorized or unlicensed software or material protected by copyright.
11. Not make unauthorized copies of HM software.
12. Log off or secure my workstation, when unattended, according to departmental policy, where applicable.
13. Not transmit or display abusive, discriminatory, harassing, inflammatory, profane, pornographic or offensive language or other such materials over or on any HM information systems.
14. Report log-on or other system problems to the Information Technology Division Service Desk.
15. Use HM information systems wisely to conserve costly space on the server.
16. Abide by the provisions of this agreement if granted remote access to any HM information system.
17. Use HM information systems equipment for the sole purpose of performing my job or services except on occasion for minimum personal use.
18. Immediately report any violations of these provisions to a manager or business practices officer.
19. Participate in ongoing information security training as directed.
20. Review the HM Information Security Agreement for renewal periodically as directed.
21. Comply with Houston Methodist Policy IM01 – Acceptable Use of Computing Resources.

I have read and understand the above and hereby agree to these provisions as a condition of my employment, contract, service, association or work with Houston Methodist and these procedures will be enforced through monitoring mechanisms and random auditing. Violations of any guidelines may result in disciplinary action up to and including termination of Houston Methodist's relationship with the violator.

Signature _____ Date _____

Printed name _____ Community Connect practice _____

Department _____ Location _____