External Practice or Agency Request for Office level Access

## Practice Information

**IDENTITY AND ACCESS MANAGER (IAM) Console access.**

CircleHealth utilizes an electronic centrally managed console (IAM) to administrate access to hospital systems. A limited number of applications are available to affiliated practices and agencies doing clinical or financial business with the hospital system. Each external office or agency may be granted a console to request, change or terminate staff access for their practice / entity to the hospital systems. Please provide the below requested information, and sign the attached confidentiality and information security agreement. (All Fields are required)

| | | | | | |
|---|---|---|---|---|---|
| Practice Name | | | | | |
| Primary Address | | | | Phone | |
| Address Line2 | | | | Fax | |
| City | | State | | Zip Code | |

| | | | |
|---|---|---|---|
| Primary Contact (Full Name) | | Primary Contact Title | |
| Primary Contact Email | | | |

| | | | |
|---|---|---|---|
| Physician or Office Manager(may be different than primary Conact) Full name | | | |
| Physician or Office Manager Signature | | Date: | |

* This is a ☐ New or ☐ Change Request.

Once the above form and the following security agreements are completed and signed, submit the request by calling our helpdesk at 978 937 6445 and submitting the form, or, sending the form by fax to 978 446 2964

External Practice or Agency Request for Office level Access

INFORMATION SECURITY PRACTICE LEVEL

Information Services runs regular and real time audit reports at the application level to monitor user activity to identify possible "curiosity" security breaches with users accessing patient information. The report will check for users accessing patient records.

After verifying that the user did not need access to this patient information, the following protocol will be followed:

- *First offence:* the Information Services System Auditor will forward a letter to the user's Office Manager indicating the breach in security. The Office Manager will counsel his/her employee regarding the violation and review the hospital policy. The user will b e required to re-sign the confidentiality statement which will then be returned to Information Services. If the signed confidentiality form is not returned within 30 days, the user's access will be inactivated. Access will not be reactivated until the signed confidentiality form has been received.
- *Second offence:* the Information Services System Auditor will forward a letter to the user's Office Manager indicating the breach in security. The violation will be reviewed with the Physician Head of Practice and both shall counsel their employee regarding the violation and review the hospital policy. The user will be required to re-sign the confidentiality form. The Physician Head of Practice will also sign the statement attesting that employee has been counseled and return it to Information Services. If signed confidentiality form is not returned within 30 days, the user's access will be inactivated. Access will not be reactivated until the Chief Information Officer has spoken with the Physician Head of Practice and the appropriate paperwork has been received by Information Services.
- *Third offence:* the Information Services System Auditor will notify the Chief Information Officer, who will speak directly to the Physician Head of Practice and decide on course of action at that time.

The Information Security Officer will submit a quarterly report to the Lowell General Hospital Corporate Compliance Committee. The quarterly report will include statistics for the previous quarter's audit violations.

*By signing this document I understand and agree to the following:* I have read the above procedure and agree to comply with all its terms.

| | | | |
|---|---|---|---|
| Physician / office Manager Signature | | Date | |
| Print Name | | | |

External Practice or Agency Request for Office level Access

## Information Security Individual Access

**In addition to the practice level agreement, each time an individual user accesses our systems remotely they must electronically acknowledge the below policies to proceed. The text of the electronic agreement is included below. Each user created for the practice must have a signed agreement on file. Fax this signed page for each user created to 978-446-2964**

I understand that Lowell General Hospital has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information. Additionally, Lowell General Hospital must assure the confidentiality of its human resources, clinical, payroll, fiscal, computer systems, and management information (collectively, "Confidential Information"). In the course of my employment/assignment/affiliation at Lowell General Hospital, I understand that I may come into the possession of Confidential Information.

I further understand that I must sign and comply with this agreement in order to get authorization for access to any of Lowell General Hospital's Confidential Information.

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. In addition, I understand that my personal access code, user ID(s), and password(s) used to access computer systems are also an integral aspect of this Confidential Information.

2. I will not access or view any Confidential Information, or utilize equipment, other than what is required to do my job.

3. I will not access my own patient account/medical record/employee file. I understand I have a right as a patient/employee to view this information but must do so through the proper channels via the medical records department or my physician for the medical record, patient accounting for billing information, and human resources for HR/Payroll information.

4. I will not discuss Confidential Information where others can overhear the conversation (for example, in hallways, elevators, in the cafeteria, on public transportation, in restaurants, and at social events). It is not acceptable to discuss Confidential Information in public areas even if a patient's name is not used. Such a discussion may raise doubts among patients and visitors about our respect for their privacy.

5. I will not make inquiries about Confidential Information for other personnel who do not have proper authorization to access such Confidential Information.

6. I will not willingly inform another person of my computer password or knowingly use another person's computer password instead of my own for any reason.

7. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information in Lowell General Hospital's computer system. Such unauthorized transmissions include, but are not limited to, removing and/or transferring Confidential Information from Lowell General Hospital's computer system to unauthorized locations (for instance, home).

8. I will respect patient confidentiality when accessing information from a remote location, such as an office or home.

9. I will log off any computer or terminal prior to leaving it unattended.

10. I will comply with any security or privacy policy promulgated by Lowell General Hospital to protect the security and privacy of Confidential Information.

11. I will immediately report to my supervisor any activity, by any person, including myself, that is a violation of this Agreement or any of Lowell General Hospital's information security or privacy policy. The transgression will in turn be reported to the Chief Information Officer for review.

12. Upon termination of my employment, I will immediately return any documents or other media containing Confidential Information to Lowell General Hospital.

13. I agree that my obligations under this Agreement will continue after the termination of my employment.

14. I understand the violation of this Agreement may result in disciplinary action, up to and including termination of employment and/or suspension and loss of privileges, in accordance with the Lowell General Hospital's Confidentiality of Computerized Information Policy, as well as legal liability.

15. I further understand that all computer access activity is subject to audit.

Individual user Signature: _____ Date: _____

Print Name: _____.

Practice Name: _____.