Indiana University Health

Access Request - Lifepoint
IU HEALTH NON-EMPLOYEE FORM

The purpose of this form is to activate or inactivate Lifepoint access for IU Health Non-Employees. Please review IU Health Information Security and Confidentiality policies before requesting access.

- **Activate User** – Fill out this section if a new end user needs access to Lifepoint.
- **Inactivate User** – Fill out this section if a current end user needs their access removed in Lifepoint.

Notification of completed request will be sent to the defined manager's email.

The End User Training Agreement on pages 2-3 must be read, reviewed, and signed by both the end users and manager to complete the end user activation in Lifepoint.

The Information Security and Confidentiality form on pages 4-5 must be read, reviewed, and signed by both the end user and manager to complete the end user activation in Lifepoint.

Email completed forms to **DPLMLABINTERFACE@iuhealth.org**

Activate User

*Legal Name:	
*Date of Birth:	
*Cell Phone #:	
*Email Address:	
*Facility Name:	
*Facility Address:	
*IU Health Client Account #:	

Inactive User

*Legal Name:	
*Lifepoint Username:	
*IU Health Client Account #:	

* = Required

Indiana University Health

End User Training Agreement

Instructions:

- *Please indicate which configuration your location is currently setup for in Lifepoint, and then please watch the corresponding training videos listed below that are contained on our **How To Guide: Lifepoint** website.*

- *End User and Manager are required to sign off that each training video has been viewed by adding initials in the appropriate box below. Failure to watch these training videos and acknowledge completion will result in delayed activation of a new user or client location in our Lifepoint system.*

Results Only			
Required Audience	**Viewing Order**	**Training Video Chapter**	**Video Length**
Client	1	Results	2:37
Client	2	Patient History	1:29
Client	3	Pending Orders Reports	0:36
Client	4	IU Health Test Directory	0:57
		Total Training Time	5:39
		End User Initials	
		Manager Initials	

Orders and Results			
Required Audience	**Viewing Order**	**Training Video Chapter**	**Video Length**
Client	1	Add New Patients	1:47
Client	2	Placing Orders	4:59
Client	3	Results	2:37
Client	4	Patient History	1:29
Client	5	Pending Orders Reports	0:36
Client	6	IU Health Test Directory	0:57
		Total Training Time	12:25
		End User Initials	
		Manager Initials	

* = Required

Standing/Future Orders - Client Draws Patients Onsite			
Required Audience	Viewing Order	Training Video Chapter	Video Length
Client	1	Add New Patients	1:47
Client	2	Placing Orders	4:59
Client	3	Placing Standing Future Orders	3:43
Client	4	Cancelling Standing Orders	0:59
Client	5	Collecting Standing Orders	2:35
Client	6	Managing + Future Orders	4:01
Client	7	Results	2:37
Client	8	Patient History	1:29
Client	9	Pending Orders Reports	0:36
Client	10	IU Health Test Directory	0:57
		Total Training Time	23:43
		End User Initials	
		Manager Initials	

Standing/Future Orders - IU Health Phlebotomy Draws Patients			
Required Audience	Viewing Order	Training Video Chapter	Video Length
Client	1	Add New Patients	1:47
Client	2	Placing Orders	4:59
Client	3	Placing Standing Future Orders	3:43
Client	4	Cancelling Standing Orders	0:59
IU Health Phlebotomy	*5*	*Collecting Standing Orders*	*2:35*
Client	6	Managing + Future Orders	4:01
Client	7	Results	2:37
Client	8	Patient History	1:29
Client	9	Pending Orders Reports	0:36
Client	10	IU Health Test Directory	0:57
		Total Training Time	21:08
		End User Initials	
		Manager Initials	

* = Required

Indiana University Health

Responsibility Statement: Information Security and Confidentiality

Indiana University Health is committed to protecting the privacy and security of its confidential information. As an Indiana University Health physician, employee, workforce member or other system user you play a crucial role in ensuring the privacy and security of this confidential information. Indiana University Health owns, control and stores paper, digital and electronic data about services, programs, systems, finances, patients, families, employees, physicians, payers, and other personally identifiable information – most of which is CONFIDENTIAL information. Access to such data is available through different formats and media and this Statement and Agreement applies to ALL the data regardless of how it is accessed.

You have requested access as a user of Lifepoint. As a user and steward of Indiana University Health's data, including in some instances protected health information (PHI) about its patients, you must agree to the following terms and obligations before being granted access. Please read your responsibilities carefully before agreeing to them by signing below:

1. Within the Indiana University Health organization, electronically stored information ("information") about services, programs, systems, costs, volumes, patients, guarantors, families, physicians, physician groups, other healthcare providers, payers and staff is available. Access to information is available in many formats and media. This statement applies to all Indiana University Health information, regardless of how it is accessed.

2. All Indiana University Health information is to be considered confidential. Reasonable precautions are to be taken to protect Indiana University Health information from unintentional or unauthorized inquiry, update, alteration, destruction or removal. It is to be safeguarded by all information customers at all times, both at work and off duty.

3. Information customers will only access (read, add, change or delete) or disclose information for which they have a business reason to do so. At no time, shall information be accessed or disclosed for an unauthorized, unethical or illegal reason.

4. Information access must be requested, approved and implemented through established protocols. Access to information will be granted on an appropriately identified, validated and authorized basis.

5. In order to maintain the integrity of electronic protected health information and safeguard it from improper alteration or destruction, individuals may not access their personal medical records through systems or processes for which they have been granted update capability.

6. Individuals authorized to access protected health information may not access the medical records of their family members, friends or colleagues unless such access is otherwise authorized by the individual's legitimate business purposes such as for treatment, payment or health care operations.

7. It is possible, that in the course of business, indirect access to information may become available. All responsibilities outlined in this statement apply to direct and indirect access to information.

* = Required

8. Certain personally identifiable information must be carefully protected, each individual is responsible for knowing and following applicable Indiana University Health policies and procedures that govern the storage, use and access of such information.

9. When unsure of the confidentiality or security precautions to be taken, it is the responsibility of the information customer to seek and obtain direction regarding release of information and/or information protection safeguards.

10. Information customers shall report suspected confidentiality breaches or other information violations to the Information Services Security Administrator immediately.

11. Failure to adhere to this responsibility statement will result in the appropriate disciplinary and/or legal action.

I have had the opportunity to read and understand this Responsibility Statement Information Security and Confidentiality and agree to its terms and conditions as indicated by signing my name below.

End User Approval

***End User Printed Name:**	
***End User Signature:**	
***Date:**	

Manager Approval

***Manager Printed Name:**	
***Manager Signature:**	
***Manager Email Address:**	
***Date:**	

This section to be completed by Indiana University Health Security

***Lifepoint Username Assigned:**	
***Request Implemented By:**	
***Date:**	