



This learning module is intended for privacy officers.

We will cover:

- About SYNCRONYS
- Security
- Patient right to Opt-Out
- User Roles



This module will introduce the SYNCRONYS health information exchange and discuss information security, patient rights, and access level roles you will be able to grant your employees.

WHAT IS SYNCRONYS?



- The nonprofit, statewide, health information exchange (HIE) for New Mexico.
- SYNCRONYS enables the electronic exchange of patient health information among different and unrelated healthcare organizations to provide timely access to a patient's information in one centralized record.
- Its objective is to exchange essential patient information between New Mexico's hospitals, tribal/IHS hospitals/clinics, skilled nursing facilities, long term care, home health and hospice, independent clinics, and behavioral health clinicians.



SYNCRONYS is New Mexico's Health Information Exchange. An HIE enables the electronic exchange of patient health information among different and unrelated healthcare organizations to provide timely access to a patient's information in one centralized record. We work with many types of organizations and receive data using a variety of methods and electronic medical record systems.

ENHANCING THE HIE HAS BROUGHT
TOGETHER INNOVATORS . . .



. . . TO TRANSFORM LIVES & DELIVER HIGH QUALITY
SOLUTIONS FOR HEALTHCARE IN NEW MEXICO



SYNCRONYS is recognized as the statewide HIE for New Mexico, but we are made stronger and better by our partnerships with innovators in health information technology. The vendor partners you see in this slide work together to expand and enhance services using their expertise. They help us provide data analytics, event notification, population health management, image exchange, regional and national connectivity, and advance care planning workflows. Some have their own dashboards that have been integrated into the HIE.

- HBI – analytics and dashboards
- Rhodes Group – labs
- Vynca Care – Advanced directives
- eHealth Technologies – Images and X-rays
- Collective Medical – ADT messages

THE INFORMATION IS SECURE



- The SYNCRONYS HIE is subject to Federal and State Privacy and Security Regulations, including HIPAA, HITECH, and other regulations.
- Information is encrypted.
- The SYNCRONYS HIE is not a patient portal. Access is limited to authorized users only.



Rest assured that the information is secure. The SYNCRONYS HIE is subject to Federal and State Privacy and Security Regulations, including HIPAA, HITECH, and other regulations.

Information is encrypted and the framework is HITECH certified.

The SYNCRONYS HIE is not available to the public; access is limited to authorized users only, and your role as a privacy officer plays an important part in protecting this information.

Because this is not a patient portal, users should not access their own information via this portal but ask their healthcare provider to use the HIE.

SYSTEM SAFEGUARDS



- Unique user IDs and strong passwords required.
- Inactivity timeout at 15 minutes.
- All activity is logged/tracked in the HIE.
- Auditing possible by you, as the organization's privacy officer, and by SYNCRONYS.
- Access levels appropriate to one's work task – Minimum Necessary.
- SYNCRONYS will disable accounts after 90 days of inactivity if the privacy officer fails to do so.

Safeguards around access that are built into the clinical portal include:

- Unique usernames and strong passwords.
- The ability to audit what users do in the system.
- A global setting for time-out after 15 minutes of inactivity.
- User roles that allow you to grant access in terms of minimum necessary patient information.

SYNCRONYS also provides you with a safety net by deactivating user accounts that are not used for 90 days.



PATIENT RIGHT TO OPT-OUT OF THE HEALTH INFORMATION EXCHANGE

Let's dive into some important patient privacy concepts related to the HIE, starting with "Opt-out."

PATIENT RIGHT TO OPT-OUT

- Patients have a right to completely opt-out of participation in the HIE.
- Opting-out is at the statewide HIE level when an individual does not want their records viewed within the HIE—even in a life-threatening emergency.



By virtue of the New Mexico Electronic Medical Records Act, patient consent is not needed to send patient records to the HIE, with one exception we'll discuss later. However, under state law patients have a right to opt-out of the HIE entirely. This hides their information from view, even in the event of a life-threatening emergency. Remaining opted-in ensures that information will be available quickly in such an event.

REASONS TO REMAIN IN THE HIE

- The HIE makes obtaining records faster and easier for the clinic staff.
- The HIE can give the care team helpful notices of important events, like hospitalizations or emergency visits.
- Only those with a Treatment, Payment, or Operations relationship with patients are authorized to access their records, in compliance with HIPAA.



If a patient is interested in opting out - your staff may want to help explain why it is beneficial for the patient to participate in health information exchange. Though you are not expected to try to persuade anyone, we have provided some talking points that may help answer questions about why the HIE is beneficial.

If a patient wishes to opt-out, your staff can simply direct them to the SYNCRONYS website or have them call SYNCRONYS to accomplish this.

OPT-OUT / OPT-BACK-IN




- “Patient Not Found” will appear in search for that individual.
- Opting-out is done by the SYNCRONYS privacy officer and impacts all HIE participating organizations.
- Opting-out does not stop data from coming to the HIE.
- Individuals may Opt-Back-In at any time by contacting SYNCRONYS; there will not be a gap in data.



When a patient is opted-out, their records will not be seen in the HIE. “Patient Not Found” will appear when searching for that patient. It does not stop information from flowing to the HIE, so individuals who decide to opt-back-in in the future would not have a gap in their information. Opting-out is done by the SYNCRONYS privacy officer and impacts all HIE participating organizations.

OPT-OUT / OPT-BACK-IN



- Requests to Opt-Out of the HIE may be directed to SYNCRONYS:
 - Website www.SYNCRONYS.org
 - Call 505-938-9900
 - eMail Info@SYNCRONYS.org
- These requests usually take a few business days to fulfill.
- Patients will receive a letter to confirm and explain the right to opt-back-in if the patient changes their mind. 

Requests to opt-out or back in can be referred to SYNCRONYS for information.



UNDERSTANDING ACCESS LEVELS AND THEIR FUNCTIONS

Privacy officers are the authority when it comes to which employees get access and how much patient information they should have. Let's talk about those Access Levels and Functions to help you make those decisions.

ROLES

Most Common Access Roles & Their Permissions	Level 3: Clinical View	Level 4: Business Staff Limited PHI	Level 6c: Demographics Only	Level 7: Analyst Used for Analytic Dashboards	Level 5b: End User Admin Help Desk	Level 6b: Privacy Officer REQUIRED POST
Clinician Homepage	x					
Front Desk Homepage		x	x			x
Administrative Homepage				x	x	
Patient Search	x	x	x			x
Recent Patients	x	x	x			x
Patient Worklists	x	x	x			x
Patient Demographics	x	x	x			x
Patient Encounter History	x	x				
Patient Allergies	x					
Patient Meds / Medicines Viewer	x					
Patient Problems	x					
Patient Lab and Pathology Results	x					
Patient Radiology Images	x					
Patient Radiology Reports	x					
Patient Transcribed Documents	x					
eHealth Exchange (External Record)	x					
Notifications (direct, real-time)	x					
HIE Portal Messaging	x	x	x	x	x	x
User Admin Functions				x	x	
Audit Logs						x
Single Sign On to Communicate Direct Secure Messaging can be added to any role. For most organizations, Level 3 is most appropriate for clinical users.						



There are several access levels, called Roles, that you can choose from when you grant access to your employees. This matrix displays the most commonly-used roles and what functions they may perform. In addition, some permissions may be added to any user, for example, if the user is a prescriber with his or her own DEA#, they can be given a link to the New Mexico Board of Pharmacy's PDMP Narx report. There are other permissions that may be added, depending on the solutions your organization has subscribed to. Your customer relationship manager can help with that information when we create your initial users for you.

Most users require Level 3 access to the full patient record, which could contain some sensitive information, like sexually transmitted diseases and behavioral health diagnoses.

A Level 4 role provides patient demographics and information about encounter dates, locations, and diagnoses, but does not allow the user to see more.

The least amount of patient information is granted in a Level 6c. This role is useful for tracking down current addresses, phone numbers, and emergency contacts, and was in fact used extensively by contact tracers during the pandemic.

Levels 5b and 6b are administrative users and we'll cover those next.

SAFEGUARDS - ACCESS LEVELS

These high-level users must be created by SYNCRONYS:

- NMHIC Level 5b, **End User Administrator** – sees no patient information, but can create, modify, and deactivate user accounts (3, 4, and 6c) for one's own organization. They can also unlock accounts and reset passwords to support users in your organization.
- NMHIC Level 6b, **Privacy Officer** – sees no clinical info., but can monitor all activity by their organization's users and can monitor access to specific patients seen by his/her organization's authorized users.
- These can be combined, but not with a clinical view.



These two roles are administrative and are considered higher-level users that should be created by SYNCRONYS as you authorize them.

Level 5b is for help desk personnel who would support user creation, modification and trouble-shooting locked out users.

Level 6b is your level, the Privacy Officer, which we have been discussing. You will not see any clinical information but can see the activity of your users and run reports based on access to all or specific patients.

Some privacy officers request that the Level 5b permissions be added to their account, and we can accommodate that request. However, if you also need a clinical view of patient information, you will need a separate account for that.

ACCESS LEVEL AND FUNCTIONS

- NMHIC Level 3: (Full clinical view)
 - Patient Search
 - Recent Patients
 - Worklists
 - See all clinical tabs and documents
 - Image viewing
 - eHealth Exchange Gateway (*External Records*)
 - VyncaCare Advance Directives and M.O.S.T. forms
 - Portal Messaging



Reviewing what you saw in the matrix, the Level 3 users are your clinicians. These can be physicians, nurse practitioners, physician assistants, and nurses, but could also include support staff, such as medical assistants, medical records personnel, or others that in your assessment need full clinical access.

ACCESS LEVEL AND FUNCTIONS

- NMHIC Level 4:
 - Patient Search
 - Recent Patients
 - Worklists
 - View Demographics
 - **View Encounters & their diagnoses**
 - Portal Messaging



Level 4 users can see demographics and a bit more clinical information, including the encounter history and diagnoses. This is less frequently used, as users that need access to encounter information typically need more to do their job.

ACCESS LEVEL AND FUNCTIONS

- NMHIC Level 6b: (Organization Privacy Officer)
 - Patient Search
 - Recent Patients
 - Worklists
 - View Demographics Only
 - Audit / Monitoring Logs (Organization-Specific Audit)
 - Portal Messaging



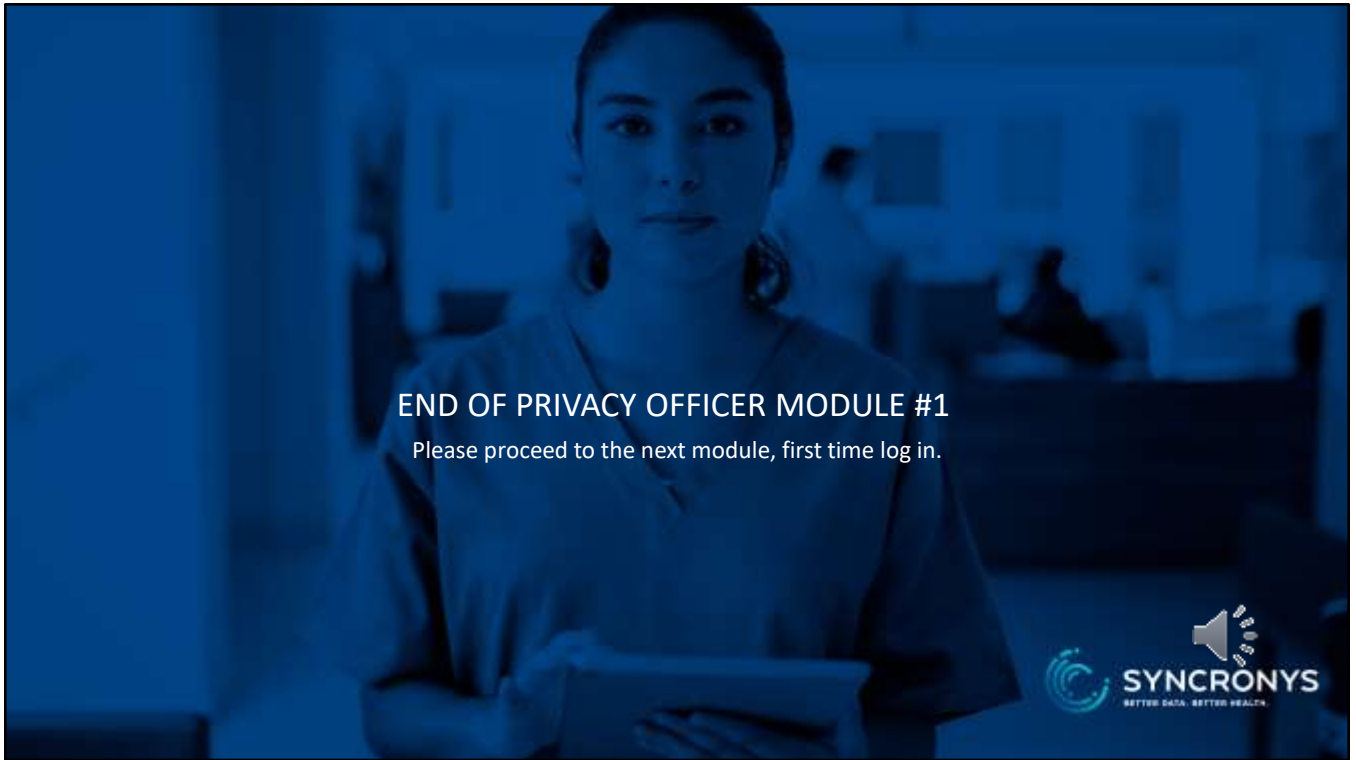
Your Privacy Officer account has a homepage that includes patient search, recent patients, worklists, and portal messaging. But, you also have a menu item for Monitoring Logs.

ACCESS LEVEL AND FUNCTIONS

- NMHIC Level 6c: *(Demographics only view)*
 - Patient Search
 - Recent Patients
 - Worklists
 - **View Demographics Only (No PHI/clinical information)**
 - Portal Messaging



Level 6c was referred to Consent Management in the past, but as the result of changes to New Mexico law, the need for tracking patient consent to view potentially sensitive conditions is no longer required. As mentioned earlier, this level user may find its access to patient demographics very useful. The Level 6c user has all the features that you do, except for the monitoring logs.



This is the end of the first privacy officer module. Please proceed to the second module and have your username and temporary password ready, so you can complete your account set up. If you have already done this, please proceed to the third module, monitoring logs.