Health Information Exchange Coordinating Committee

November 15, 2023

This meeting is being recorded

Jason Weida, Secretary
Agency for Health Care Administration

Members

Craig Dalton - Chair
Strategic Health Intelligence

Tab Harris – Vice Chair
Blue Cross & Blue Shield of Florida

Kayvan Amini
Florida Osteopathic Medical Association

Ankush Bansal
Florida Chapter of the American College of Physicians

Melanie Brown-Woofter
Florida Council for Community Mental Health

Jarrod Fowler
Florida Medical Association

Dennis Hollingsworth
Clinical Informatics
Florida Department of Health

Peter Kress
Long-term Post-Acute Care

Alejandro Romillo
Health Choice Network

Marie Ruddy
Nemours Hospital

Helen Sairany
Florida Pharmacy Association

Kim Streit
Florida Hospital Association

Kim Tendrich
Florida Department of Health

Vacant
Florida Association of Health Plans

Melissa Vergeson
AHCA Medicaid

Hymin Zucker, MD
Florida Association of Accountable Care Organizations

AGENDA

Health Information Exchange Coordinating Committee (HIECC)

Meeting Date: November 15, 2023
Meeting Time: 12:00 PM to 4:00 PM

Location: 2727 Mahan Dr, Tallahassee, FL 32308 **OR Virtual:**
https://events.gcc.teams.microsoft.com/event/c7bd8a6f-8b1c-4dd2-9188-95c823ac7b04@583c5f19-3b64-4ced-b59e-e8649bdc4aa6

Dial-in Information: Will be provided upon registration.

TIME	ITEM
12:00 PM	Welcome
12:05 PM	Roll Call
	Review & Approve Previous Meeting Minutes
	Previous Action Item Review and Status Updates
12:20 PM	Agency Updates
12:30 PM	Election of Officers for 2024
12:40 PM	Legal Work Group Update
12:50 PM	Health Information Exchange Vendor Transition
1:10 PM	Input on Current ENS Solution
	Retention of ADT data
	Interstate exchange of ADT data
	Consent Policy
3:40 PM	2024 HIECC Meeting Dates
3:45 PM	Public Comments
3:50 PM	Meeting Summary
	Next Steps
	Adjournment

Welcome

Roll Call

Review and Approve Previous Meeting Minutes

Health Information Exchange Coordinating Committee (HIECC)
Meeting Minutes

Date: August 16, 2023
Time: 1:00 PM to 3:00 PM
Location: Virtual Meeting

Members Present: Craig Dalton, Tab Harris, Dennis Hollingsworth, Peter Kress, Melissa Vergeson, Kimberly Tendrich, Kayvan Amini, Ankush Bansal, Jarrod Fowler, Kim Streit, Marie Ruddy

Presenters: Craig Dalton, Jaime Bustos, Michelle Salzman, Jennifer Grove, ABM Uddin

Agency Staff Present: AMB Uddin, Crystal Ritter, Jaime Bustos, Kim Davis-Allen, Corinne Slautterback, Ericka Pearce, Dana Watson, Sketch Piers, Dylan Dunlap

Interested Parties Present: Ashley Tait-Dinger, Brian Smart, George Cedemo, Michael Craig, Bruse Culpepper, Eric Rutledge, Jesse Herbert, Jennifer Grove, Karen van Caulil, Michael Karris, Samuel Lewis, Linda McDonald, Michelle Salzman, Angelina Rivers

Meeting Materials: HIECC Meeting Packet. Copies of meeting materials are posted on: Health Information Exchange Coordinating Committee (myflorida.com)

Welcome and Call to Order: Craig Dalton welcomed everyone and called the meeting to order at 1:04 pm on August 16, 2023, and reminded everyone the meeting is being recorded. Mr. Dalton welcomed the new HIECC members Dr. Kayvan Amini, and Dr. Ankush Bansal and asked Jaime Bustos to call the roll.

Roll Call: Jaime Busto took roll, and noted a quorum was present.

Review and Approval of Minutes and Previous Action Items: Mr. Dalton asked members if they had an opportunity to review the minutes and if there was a motion to approve. Tab Harris made a motion to approve the minutes. Kimberly Tendrich seconded the motion which carried unanimously.

Agency Updates: Mr. Dalton asked Mr. Bustos to give the Agency updates.
Mr. Bustos shared that the Agency's FloridaHealthFinder website had a soft launch. This is the Agency's largest transparency website. It has been updated to have a similar look and feel to the other transparency websites and cover page. We have some instructional videos being created that will show how to use the site and how to pull reports. If you have any feedback or comments, please send them to the Agency.

Mental Health Collaborative Overview and Discussion: Mr. Dalton gave an overview of what to expect during the discussion and asked Representative Michelle Salzman to provide background on the Escambia County Collaborative. Representative Salzman gave a background on the collaboration, and the funding behind the Mental Health Collaborative and introduced Jennifer Grove, who led the efforts in their community. During the overview Ms. Grove went over vital information, the strategic plan and roadmap. She gave in-depth timelines of the past and future. After the presentation the members and interested parties discussed the value of community collaborations for behavioral health models. Mr. Dalton requested the members consider how this model could be implemented in other communities in Florida.

HIE Updates: Mr. Dalton requested ABM Uddin present Florida HIE updates. Mr. Uddin shared the discussions around Florida HIE participants' transition to the PointClickCare (PCC) national platform. He shared that PCC proposals around data sharing are being presented to the State Consumer Health Information and Policy (SCHIP) Advisory Council, the HIE Coordinating Committee (HIECC), the HIE Legal Work Group, and other stakeholders for input. The Legal Work Group's first meeting is set for Oct 10, 2023. He also shared information from the Health Tech Solutions' findings on HIE gaps in rural communities and the status of connectivity to the national networks, stating that the Agency will continue to work with other State agencies, the HIE vendor, and all stakeholders to facilitate and adopt data sharing nationally by rural hospitals. He also shared latest updates on ePrescribing rates in Florida, as well as E-PLUS adoption by partners to provide continuity of care and find missing persons during times of disasters. Uddin shared that the E-PLUS team continues to invest in education and outreach to onboard more pharmacies onto the platform to facilitate richer and better data for the users. Lastly, noted an increased interest of law-enforcement in using ENS to enable their ability to find missing persons during normal times, and the Agency will work with stakeholders for input.

Next steps:

Mr. Dalton reminded the members that the next meeting of the HIECC will be November 15, 2023.

New Action Items	Owner
Share Mental Health Collaboration presentation with Members.	Crystal Ritter
Provide feedback to the Agency on potential Mental Health Collaboration opportunities in their communities.	HIECC Members

With no further business to discuss, Peter Kress made a motion to adjourn. The motion was seconded by Kim Streit and carried unanimously.

Previous Action Items and Status Updates

New Action Items	Owner
Share Mental Health Collaboration presentation with Members.	Crystal Ritter
Provide feedback to the Agency on potential Mental Health Collaboration opportunities in their communities.	HIECC Members

Agency Updates

Election of Officers for 2024

Legal Work Group Update

The Legal Work Group met on October 10, 2023 to discuss the HIE Vendor Transition and Policies for Consideration relating to Infrastructure, Data Retention, and Consent Process Modifications.

Representatives from PointClickCare discussed how the Florida HIE would be affected by their recent acquisition of Audacious Inquiry. They indicated it would include increasing post-acute data sources, allowing for the sharing of 42CFR Part 2 data with a change in the current consent model, allowing for interstate data exchange within their vendor network by switching to their national model, and allow for the retention of data. Hospitals would need to sign a new ENS Addendum to allow for these changes.

There were concerns from the work group members about data security if it was stored for two years and that there would be more risk placed on the business associates with this change. PointClickCare emphasized their focus on security and risk management and that hospitals can request a purge of their data on an annual basis. The Advisory Council previously suggested the addendum include that the data should be retained for at least a year, but there is flexibility in the length of data retention after that time.

When discussing moving from a Florida-centric model to the vendor's national model, the Legal Work Group emphasized the need for everything to be HITRUST compliant and confirmed with PointClickCare that they were reviewing and complying with various state laws for interstate exchange of sensitive data. They did not have any legal concerns about moving to a national model, as long as it could be done securely and meet the legal requirements.

The Legal Work Group brought up concerns about who owns the data and patient denial of care. PointClickCare emphasized that data retention and flagging features should help improve patient care and that their solutions have worked well in multiple other states, including Oregon and Virginia. The Agency was advised to review the training materials that are given to the providers that direct them about how to use the security plans in this solution. The Agency is also working on surveys and listening sessions that would get feedback from providers on topics recommended by the work group, including the length of data retention that would best serve them.

When considering changing the consent model, the Legal Work Group advised that the Agency consider a comprehensive review on moving data sources from opt out to opt in to due to the likelihood of confusion or push back from patients. There were also concerns about the time commitment involved with switching consent models and the possibility of hesitation towards establishing a model for sharing substance use disorders until potential federal changes are implemented.

There were no public comments. There was not enough time for specific recommendations for changes to the ENS Agreement, so the Legal Work Group will be meeting again on November 17, 2023. These recommendations may assist the Agency in getting clarity regarding their procurement for Florida HIE Services.

- Input on Current ENS Solution
- Retention of ADT data
- Interstate exchange of ADT data
- Consent Policy

Input on Current ENS Solution

Retention of ADT data

Data Retention

Background:

The current Florida Health Information Exchange (HIE) Encounter Notification Service (ENS) began operations in November 2013 with one hospital data source. ENS delivers alerts about a patient's inpatient or emergency department encounter to a permitted recipient with an existing relationship to the patient, such as a health plan or primary care provider. In June 2014, the Agency informed hospitals that the Low-Income Pool (LIP) participation requirements for SFY 2014-2015 include participation in ENS as a data source. Organizations representing 203 hospitals signed the ENS agreement for participation as a data source in 2014.

As of September 30, 2023, ENS has around 800 data sources made up of hospitals, home health agencies, skilled nursing facilities, crisis stabilization units, urgent care facilities, hospice, and county health departments. Of the 800 data sources, 551 are subscribed to receive ENS encounter data with a total of 244 subscription agreements.

March 28, 2016, the Agency presented an addendum to the ENS agreement that would allow data segments from ENS to be retained for 30 days to allow reporting of 30-day readmissions to subscribers to the Legal Workgroup. There was no objection to the proposed addendum or readmissions alerting feature, so the Agency moved forward with the implementation.

December 1, 2017, the Legal Workgroup supported an addendum to allow hospitals to voluntarily allow for the retention of data for care coordination purposes. The addendum was subsequently supported by the HIECC on December 5, 2017.

The current Florida Health Information Exchange (HIE) Encounter Notification Service (ENS) does not allow for the retention of data, unless a separate addendum is signed by a participating data source. A more extensive addendum to allow for the retention of data and inter-state data exchange was approved by the SCHIP Advisory Council on February 23, 2023.

Current Issue:

The current vendor for the Florida HIE, Audacious Inquiries, was acquired by another vendor, Point Click Care in 2022. Although, an ENS Addendum was approved as voluntary for data sources to allow for retention of data, now that more information is understood about the new vendor's infrastructure there would need to be a change to the current Florida HIE ENS model to require data retention in order for the vendor to support the Florida HIE system.

In addition to the changes suggested by the vendor, the current contract for the Florida HIE Vendor ends in September 2024. The Agency will be procuring for the HIE Vendor in 2024. These events provide an opportunity for the Agency to seek insight regarding the direction the Florida HIE should be moving, including prospective on data retention.

Discussion:

- What, if any, are technical or operational considerations for providers does the Agency needs to consider if a decision is made to move from the current ENS model, that does not retain data

and is Florida centric, to a model that does retain data and would move end points to the vendor's network platform?

- Would technical or operational considerations be different toward retention of data if the model were a Florida centric vs vendor network centric?
- Are there any security considerations the Agency needs to consider for the described infrastructure?
- Are there security considerations the Agency needs to consider with the retention of data in either a Florida centric model or a vendor network centric model?

Supplemental Information:

- Minutes Legal Workgroup March 28, 2016
- Excerpt from Legal Workgroup December 5, 2016, Minutes
- Excerpt from Legal Workgroup December 1, 2017, and HIECC December 5, 2017 Minutes
- Excerpt from the SCHIP February 23, 2023, Minutes

MINUTES

Health Information Exchange Legal Work Group Conference Call (HIE LWG)

Meeting Date: March 28, 2016

Time: 2:00 p.m. – 3:00 p.m.

Location: Call-in Number: (888) 670-3525
Pass Code: 934-890-7894#

Members Present: Kathy Pilkenton, Chair; Bill Bell, Florida Hospital Association; William P. Dillon, Messer, Caparello; Jarrod Fowler, Florida Medical Association; Diane Gaddis, Community Health Centers Alliance; Diane Godfrey, Florida Hospital; Melanie Brown-Woofter, proxy for Mike Hansen, Florida Council for Community Mental Health, Inc.; Samuel Lewis, Feldman Gale; Kimberly Tendrich, Florida Department of Health; and Wences Troncoso, Florida Association of Health Plans.

Members Absent: Jan Gorrie, Ballard Partners; Gabriel Hartsell, Galloway, Johnson, Tompkins, Burr & Smith PLC; and Julie Meadows-Keefe, Grossman, Furlow and Bayó.

Staff Present: Vance Burns, Heidi Fox, Carrie Gaudio, Michael Hardy, Pamela King, Kevin Marker, Aaron Parsons and Dana Watson.

Meeting Materials: Proposed Changes to Event Notification Service (ENS) Subscription Agreement;

Copies of meeting materials are posted at: http://www.fhin.net/content/committeesAndCouncils/index.shtml

Call to Order, Welcome and Roll Call
Ms. Kathy Pilkenton called the meeting of the Health Information Exchange Legal Work Group (HIE LWG) to order at 2:00 p.m., welcomed members and guests, and had Vance Burns conduct the roll call. A quorum was present.

Proposed Changes to the Event Notification Service (ENS) Agreement
Ms. Fox informed the workgroup that they will be considering a proposed addendum to the ENS agreement. She introduced Mr. Aaron Parsons to lead the discussion.

Mr. Parsons presented on the benefits of allowing hospitals which provide encounter data to ENS to also receive encounter data from other participating hospitals. The benefits include better coordinated post-discharge care, reduced hospital readmissions, increased primary care utilization, medication reconciliation, transitional care management reimbursement opportunities, etc. Data could be provided based on the treatment relationship which exists between the hospital and the patient, given the patients' recent hospital encounter.

Mr. Parsons referenced the proposed addendum to the ENS subscription agreement presented at the previous HIE LWG meeting. The proposed addendum would allow the Florida HIE vendor to retain demographic information from the hospital encounter data for the purpose of building a subscription panel for interested hospitals. This subscription panel would then be used to identify patients' subsequent hospital encounters at other hospitals occurring within 30 days of a discharge from the interested hospital.

It was noted that signing the proposed addendum and receiving the readmissions alerts would be entirely voluntary. It was also noted that, if necessary, the primary complaint and diagnosis code fields could be removed before the readmission alerts are routed to the subscribing hospital. Mr. Parsons stated that the 30-day window for retaining encounter data and sending notification of subsequent hospital encounters was based

on the 30-day readmissions metric used by the Centers for Medicare and Medicaid Services (CMS) as part of the Hospital Readmissions Reduction Program.

Mr. Bill Bell commented that the Florida Hospital Association believes that unnecessary hospital readmissions can be reduced through better coordinated follow-up care. He stated that receiving readmissions notifications through ENS could be helpful for hospitals.

Ms. Diane Godfrey inquired about which data elements the vendor would retain as part of the proposed readmissions alerting process. It was noted that the patient's name, gender, date of birth, and other demographic information would be copied from the encounter data, timestamped, and then entered into the vendor's MPI as part of the hospital's subscription panel. The encounter data would then be deleted and the information copied into the MPI would be deleted 30 days from the timestamp. A question was also raised about the ability of hospitals to opt out of providing encounter data to other hospitals that have decided to participate as subscribers to the service. Mr. Parsons noted that the ENS platform would provide access to the same encounter data to all subscribing organizations.

Mr. Samuel Lewis asked about only having records for a 30-day window. He also asked what action a hospital should take if a patient is readmitted within the 30 days. Mr. Parsons responded that the hospital can reach out to the prior hospital and/or to the patient's primary care provider to discuss the patient's medical history and treatment.

Ms. Pamela King reported that the stakeholders interested in the service feel that it would be a value to them and their operations. Mr. Parsons reminded the group that this is voluntary.

Mr. Samuel Lewis inquired if this is going to be a separate opt in/opt out issue or if hospitals already participating as data sources will automatically be included in alerts. Mr. Parsons responded that hospitals would need to opt in by signing the addendum in order to receive readmissions alerts.

Mr. Troncoso asked about the security controls around the service. Ms. Fox responded that the HIE vendor, Harris Corp., had provided a technical memorandum describing in detail how the security is provided. Harris did a HIPAA risk assessment as well. Mr. Troncoso inquired if any health plans had indicated interest. Ms. Fox will resend the technical memo to Mr. Troncoso and suggested a follow up conversation.

Mr. Troncoso asked if there was any proposed language to implement this change. Mr. Parsons stated that the proposed addendum is posted on www.fhin.net. He will send a copy of the Addendum to the work group.

Mr. Bell supports the change to the service as a voluntary option to the data sources to also receive notices for a minimal fee after a pilot program is complete.

No HIE LWG member stated any specific objections to the proposed addendum or readmissions alerting feature. Hearing no objections, the Agency noted its intent to move forward with the project.

Adjournment:

There being no further business to discuss, the committee adjourned at 3:00 p.m.

Excerpt from December 5, 2016 Legal Workgroup meeting:

Patient Look-Up Service Agreement: Ms. Fox also reported that the Service Level Agreements would be included in each of the subscription agreements. Another change to the PLU agreement is that the vendor no longer has to retain the audit trail data for 8 years. Ms. Keefe inquired what was currently being stored. Ms. Fox responded that only the metadata from the transactions was stored.

Event Notification Service Agreement: Included in the changes to the ENS agreement is the deletion of the requirement to hold audit trail data for 8 years. After discussion, the Agency agreed to investigate how long audit trail data should be retained by the vendor and update the draft language accordingly. Another suggested change was to remove the sentence on minimum necessary PHI in the Permitted Purposes section of the ENS agreement, as the language is thought to duplicate requirements already found in 45 CFR. Mr. Lewis and Ms. Godfrey both suggested retaining the minimum necessary PHI language.

General Terms and Conditions: The first change to the Terms and Conditions is the deletion of language relating to breach, citing the law rather than stating it. Vendor responsibilities were discussed next. The language preventing the vendor from storing health data was struck from the Permitted Purposes section of the Terms and Conditions, while maintaining the existing language that prohibits the vendor from using health data in any way not permitted by the relevant subscription agreement.

The phrase "Alerting Services" was added to the network operations to be provided by the vendor. The vendor will also be required to keep an updated data source list on a public website. The "Accounting for Disclosures" provision was struck as no Personal Health Information (PHI) is being stored beyond the metadata. Other provisions were deleted that were included in the past due to the requirements tied to the American Recovery and Reinvestment Act (ARRA) that were never implemented in final rule. Ms. Fox reported that the only change to the Participant responsibilities is to remove the requirement for organizations to hold on to consent forms collected from the patients. Both the Business Associate Agreement (BAA) and the Qualified Service Organization (QSO) provisions were moved from the main body of the Florida HIE General Participation Terms and Conditions and are now listed as Attachments A and B respectively.

Excerpt from December 1, 2017 Legal Workgroup Minutes:

Data Retention Addendum to the ENS Agreement

Based on feedback from stakeholders across the state, the Agency decided to pursue a federated model of health information exchange when we built the services for the Florida HIE under the Cooperative Agreement with the ONC. In this model, each participating organization maintains control of its own data while agreeing to a technical and policy framework to facilitate exchange between participants. When the Agency implemented the Event Notification Service (ENS) in 2013, the agreements prohibited the vendor from retaining any of the incoming hospital encounter data beyond the timeframe necessary to match and route this data to the appropriate health plan or provider organization. This policy decision limits the functionality of the service. The HIE environment in Florida has evolved considerably since the creation of the Florida HIE. The blanket prohibition on data retention is now preventing connected hospitals from getting the most out of the available services. The Agency believes a better approach going forward would be to allow hospitals to choose whether to allow the Florida HIE vendor to retain data in order to offer enhanced services. The proposed Data Retention Addendum to the ENS Agreement would allow interested hospitals to permit the vendor to retain their hospital encounter data in order to enable additional functionality and value.
Permitted purposes for data retention may include:

- Allowing the vendor to use the incoming encounter data to build a subscription panel for the hospital. Interested hospitals could then be notified when their patient is seen at another facility, allowing better care coordination and reduced admissions and readmissions.
- Notifying ED doctors and hospital admissions staff about a patient's prior hospital encounters at the time of admission. This would allow pro-active identification of complex patients, chronic disease patients, frequent ED utilizers, and others who could benefit from more intensive care management.
- Enhanced matching between incoming hospital Encounter Data and subscriber patient panels by retaining demographic data from data sources such as Patient ID. Access to more data will drive better matching, which benefits the hospital, subscriber, and patient.

Hospitals that choose not to pursue these additional opportunities could maintain the status quo – the vendor would continue to routinely purge their data from the system in accordance with the current agreement.
An optional addendum to the existing agreement strikes a balance, allowing each health system to choose their level of engagement with the Florida HIE.

Mr. Sam Lewis asked how many hospitals were connected to the ENS. Ms. Fox responded that there are 216 hospitals connected as data sources and two hospitals are in the process of becoming data subscribers. Mr. Lewis inquired if the two new subscribers were "ok" with their data being retained. Ms. Fox explained that there would be other services offered to subscribers allowing for data retention. Gaddis is there an expectation that the new functionality and retention, increase subscriber fees. Mr. Even Carter, with Ai responded that the price would be the same as it is now, with the same base functionality as there is now. There will be an al-le-cart menu of other services with other costs for subscribers to choose from.

Excerpt from December 5, 2017 HIECC Minutes:

HIECC 12/5/2017

Legal Work Group Report: The LWG reviewed and discussed an addendum to the Encounter Notification Service (ENS) to allow Ai to retain data for specified enhanced services. Ms. Fox reported that members of the LWG inquired about participants' feedback regarding retention of data. She responded that there is interest in the additional services which data retention would allow. Dr. Saver remarked that retention of the data was not part of the originally planned service. Ms. Fox responded that data retention and analysis would lead to better care coordination, and the addendum is voluntary so the only data retained would be for organizations who elect to do so.

Excerpt from the SCHIP February 23, 2023 Minutes:

Encounter Notification Service Addendum Discussion

Dr. van Caulil introduced the topic of the Encounter Notification Service (ENS) Addendum and asked Ms. King to provide more details on this discussion topic.

Ms. King thanked the members of the Ad Hoc Committee and reviewed the modification to the Addendum based on their input. She highlighted a change in the language to clarify the document was an addendum to the current agreement and not an amendment; noted that the permitted purposes and prohibited purpose language would prevent the commercialization or selling of Florida HIE data, and noted the addition of language for flexibility on length of time for retention of data depending on the needs of facilities sharing data.

Ms. King advised that the new retention language would allow participants to choose how long they would like the data to be retained, with a limitation of only one request for purging data per year and does allow up to a year for deletion. The consensus of the Council was that these changes did address prior concerns.

Ms. King shared as a final discussion topic that during the last review of the language the vendor noted the agreement language recognizes data servers only in the United States. However, Audacious Inquiry was acquired by Point Click Care in 2022. Point Click Care is a Toronto-based organization. They are asking for clarifying language that would allow their help desk staff in Canada to have access to information for the purpose of assisting Florida HIE Users.

After much discussion about unknown risks related to the Personal Information Protection and Electronic Documents Act (PIPEDA) data privacy laws in Canada versus Health Insurance Portability and Accountability Act (HIPAA) laws in the United States, the Council asked that this section be tabled for further discussion at a later meeting.

After further discussion, Dr. Shapiro moved to approve the Addendum language submitted with the exception of the Canadian provision. The motion was seconded by Ms. Kennedy and approved unanimously.

Dr. van Caulil suggested that we consider reconvening a legal workgroup to support the Council in making recommendations and decisions like the ENS Addendum that we just worked through. Ms. King agreed with the idea and will work with the Chair to bring information back the Council for the next meeting.

Interstate exchange of ADT data

Interstate Data Exchange

Background:

The current Florida Health Information Exchange (HIE) Encounter Notification Service (ENS) began operations in November 2013 with one hospital data source. ENS delivers alerts about a patient's inpatient or emergency department encounter to a permitted recipient with an existing relationship to the patient, such as a health plan or primary care provider. In June 2014, the Agency informed hospitals that the Low-Income Pool (LIP) participation requirements for SFY 2014-2015 include participation in ENS as a data source. Organizations representing 203 hospitals signed the ENS agreement for participation as a data source in 2014.

As of September 30, 2023, ENS has around 800 data sources made up of hospitals, home health agencies, skilled nursing facilities, crisis stabilization units, urgent care facilities, hospice, and county health departments. Of the 800 data sources, 551 are subscribed to receive ENS encounter data with a total of 244 subscription agreements.

From 2011 through 2014 the Agency participated in pilot projects for interstate exchange using Direct Secure Messaging (secure email) HISP connections. One for sharing data during disasters and the other for sharing behavioral health data between states.

There was a push for query exchange through a hub connection to the eHealthExchange from 2014 to 2017. In 2017 a decision to leverage the national market for query model exchange was made, thereby reducing burden and cost of providers while still supporting data exchange. The Florida query service transitioned from a state specific infrastructure to one connecting through the eHealth Exchange (eHX), Carequality, or other platforms.

December 2016, the Legal Workgroup discussed modification to the ENS agreement that would remove the "Accounting for Disclosures" provision as no Personal Health Information (PHI) is being stored beyond the metadata.

At the March and June 2018 HIECC meetings the decision was made to have providers connect directly to the national exchanges for the purpose of sharing patient clinical records (query exchange). Discussion around interstate data sharing focused on the Data Use and Reciprocal Support Agreement (DURSA) for sharing through the national exchanges.

At the November 2018 HIECC meeting there was discussion about the Patient Centered Data Home concept for ENS data and the barriers in Florida concerning sharing mental health data across states.

Current Issue:

The current vendor for the Florida HIE, Audacious Inquiries, was acquired by another vendor, Point Click Care in 2022. Although, an Addendum was approved as voluntary for data sources to allow for retention of data, now that more information is understood about the new vendor's infrastructure there would need to be a change to the current Florida HIE ENS model to require data retention in order for the vendor to support the Florida HIE system.

In addition to the changes suggested by the vendor, the current contract for the Florida HIE Vendor ends in September 2024. The Agency will be procuring for the HIE Vendor in 2024. These events provide an

opportunity for the Agency to seek insight and direction regarding the direction the Florida HIE should be moving, including prospective on inter-state data exchange of encounter data.

The current Florida Health Information Exchange (HIE) Encounter Notification Service (ENS) does not allow for the interstate data exchange, unless a separate addendum is signed by a participating data source. An addendum to allow for the retention of data and inter-state data exchange was approved by the SCHIP Advisory Council in February of this year. To meet the Florida law around sharing of mental health data consent to share data would be needed to be obtained prior to being able to share data to other states.

Discussion:

What technical and operational considerations does the Agency need to consider when looking at interstate sharing of ADT data?

Would there be more support for interstate data sharing if the connection was through other state HIE entities versus connectivity to the HIE vendor connections?

Would there be concerns if connectivity is limited to only the vendor connected entities?

Would having inter-state data be valuable enough to warrant a change in the current consent model?

Supplemental Information:

- Excerpt from December 5, 2016 Legal Workgroup Minutes
- Section 394.4615, Florida Statutes, Mental Health
- Department of Health and Human Services, Office of Civil Rights, Guidance on HIPAA Privacy Rule and Sharing Information Related to Mental Health
- Civitas Patient Centered Data Home Overview

Excerpt from December 5, 2016 Legal Workgroup Minutes:

Event Notification Service Agreement: Included in the changes to the ENS agreement is the deletion of the requirement to hold audit trail data for 8 years. After discussion, the Agency agreed to investigate how long audit trail data should be retained by the vendor and update the draft language accordingly. Another suggested change was to remove the sentence on minimum necessary PHI in the Permitted Purposes section of the ENS agreement, as the language is thought to duplicate requirements already found in 45 CFR. Mr. Lewis and Ms. Godfrey both suggested retaining the minimum necessary PHI language.

General Terms and Conditions: The first change to the Terms and Conditions is the deletion of language relating to breach, citing the law rather than stating it. Vendor responsibilities were discussed next. The language preventing the vendor from storing health data was struck from the Permitted Purposes section of the Terms and Conditions, while maintaining the existing language that prohibits the vendor from using health data in any way not permitted by the relevant subscription agreement.

The phrase "Alerting Services" was added to the network operations to be provided by the vendor. The vendor will also be required to keep an updated data source list on a public website. The "Accounting for Disclosures" provision was struck as no Personal Health Information (PHI) is being stored beyond the metadata. Other provisions were deleted that were included in the past due to the requirements tied to the American Recovery and Reinvestment Act (ARRA) that were never implemented in final rule. Ms. Fox reported that the only change to the Participant responsibilities is to remove the requirement for organizations to hold on to consent forms collected from the patients. Both the Business Associate Agreement (BAA) and the Qualified Service Organization (QSO) provisions were moved from the main body of the Florida HIE General Participation Terms and Conditions and are now listed as Attachments A and B respectively.

Section 394.4615, Florida Statutes, Mental Health

394.4615 Clinical records; confidentiality.—

(1) A clinical record shall be maintained for each patient. The record shall include data pertaining to admission and such other information as may be required under rules of the department. A clinical record is confidential and exempt from the provisions of s. 119.07(1). Unless waived by express and informed consent, by the patient or the patient's guardian or guardian advocate or, if the patient is deceased, by the patient's personal representative or the family member who stands next in line of intestate succession, the confidential status of the clinical record shall not be lost by either authorized or unauthorized disclosure to any person, organization, or agency.

(2) The clinical record shall be released when:

(a) The patient or the patient's guardian authorizes the release. The guardian or guardian advocate shall be provided access to the appropriate clinical records of the patient. The patient or the patient's guardian or guardian advocate may authorize the release of information and clinical records to appropriate persons to ensure the continuity of the patient's health care or mental health care. A receiving facility must document that, within 24 hours of admission, individuals admitted on a voluntary basis have been provided with the option to authorize the release of information from their clinical record to the individual's health care surrogate or proxy, attorney, representative, or other known emergency contact.

(b) The patient is represented by counsel and the records are needed by the patient's counsel for adequate representation.

(c) The court orders such release. In determining whether there is good cause for disclosure, the court shall weigh the need for the information to be disclosed against the possible harm of disclosure to the person to whom such information pertains.

(d) The patient is committed to, or is to be returned to, the Department of Corrections from the Department of Children and Families, and the Department of Corrections requests such records. These records shall be furnished without charge to the Department of Corrections.

(3) Information from the clinical record may be released in the following circumstances:

(a) When a patient has communicated to a service provider a specific threat to cause serious bodily injury or death to an identified or a readily available person, if the service provider reasonably believes, or should reasonably believe according to the standards of his or her profession, that the patient has the apparent intent and ability to imminently or immediately carry out such threat. When such communication has been made, the administrator may authorize the release of sufficient information to provide adequate warning to the person threatened with harm by the patient.

(b) When the administrator of the facility or secretary of the department deems release to a qualified researcher as defined in administrative rule, an aftercare treatment provider, or an employee or agent of the department is necessary for treatment of the patient, maintenance of adequate records, compilation of treatment data, aftercare planning, or evaluation of programs.

For the purpose of determining whether a person meets the criteria for involuntary outpatient placement or for preparing the proposed treatment plan pursuant to s. 394.4655, the clinical record may be released to the state attorney, the public defender or the patient's private legal counsel, the court, and to the

appropriate mental health professionals, including the service provider identified in s. 394.4655(7)(b)2., in accordance with state and federal law.

(4) Information from the clinical record must be released when a patient has communicated to a service provider a specific threat to cause serious bodily injury or death to an identified or a readily available person, if the service provider reasonably believes, or should reasonably believe according to the standards of his or her profession, that the patient has the apparent intent and ability to imminently or immediately carry out such threat. When such communication has been made, the administrator must authorize the release of sufficient information to communicate the threat to law enforcement. A law enforcement agency that receives notification of a specific threat under this subsection must take appropriate action to prevent the risk of harm, including, but not limited to, notifying the intended victim of such threat or initiating a risk protection order. A service provider's authorization to release information from a clinical record when communicating a threat pursuant to this section may not be the basis of any legal action or criminal or civil liability against the service provider.

(5) Information from clinical records may be used for statistical and research purposes if the information is abstracted in such a way as to protect the identity of individuals.

(6) Information from clinical records may be used by the Agency for Health Care Administration, the department, and the Florida advocacy councils for the purpose of monitoring facility activity and complaints concerning facilities.

(7) Clinical records relating to a Medicaid recipient shall be furnished to the Medicaid Fraud Control Unit in the Department of Legal Affairs, upon request.

(8) Any person, agency, or entity receiving information pursuant to this section shall maintain such information as confidential and exempt from the provisions of s. 119.07(1).

(9) Any facility or private mental health practitioner who acts in good faith in releasing information pursuant to this section is not subject to civil or criminal liability for such release.

(10) Nothing in this section is intended to prohibit the parent or next of kin of a person who is held in or treated under a mental health facility or program from requesting and receiving information limited to a summary of that person's treatment plan and current physical and mental condition. Release of such information shall be in accordance with the code of ethics of the profession involved.

(11) Patients shall have reasonable access to their clinical records, unless such access is determined by the patient's physician to be harmful to the patient. If the patient's right to inspect his or her clinical record is restricted by the facility, written notice of such restriction shall be given to the patient and the patient's guardian, guardian advocate, attorney, and representative. In addition, the restriction shall be recorded in the clinical record, together with the reasons for it. The restriction of a patient's right to inspect his or her clinical record shall expire after 7 days but may be renewed, after review, for subsequent 7-day periods.

(12) Any person who fraudulently alters, defaces, or falsifies the clinical record of any person receiving mental health services in a facility subject to this part, or causes or procures any of these offenses to be committed, commits a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083.

History.—s. 14, ch. 96-169; s. 98, ch. 99-8; s. 1, ch. 2000-163; s. 14, ch. 2000-263; s. 4, ch. 2004-385; s. 83, ch. 2014-19; s. 8, ch. 2016-127; s. 89, ch. 2016-241; s. 1, ch. 2019-134; s. 5, ch. 2022-36.

Excerpt from December 5, 2016 Legal Workgroup meeting:

Patient Look-Up Service Agreement: Ms. Fox also reported that the Service Level Agreements would be included in each of the subscription agreements. Another change to the PLU agreement is that the vendor no longer has to retain the audit trail data for 8 years. Ms. Keefe inquired what was currently being stored. Ms. Fox responded that only the metadata from the transactions was stored.

Event Notification Service Agreement: Included in the changes to the ENS agreement is the deletion of the requirement to hold audit trail data for 8 years. After discussion, the Agency agreed to investigate how long audit trail data should be retained by the vendor and update the draft language accordingly. Another suggested change was to remove the sentence on minimum necessary PHI in the Permitted Purposes section of the ENS agreement, as the language is thought to duplicate requirements already found in 45 CFR. Mr. Lewis and Ms. Godfrey both suggested retaining the minimum necessary PHI language.

General Terms and Conditions: The first change to the Terms and Conditions is the deletion of language relating to breach, citing the law rather than stating it. Vendor responsibilities were discussed next. The language preventing the vendor from storing health data was struck from the Permitted Purposes section of the Terms and Conditions, while maintaining the existing language that prohibits the vendor from using health data in any way not permitted by the relevant subscription agreement.

The phrase "Alerting Services" was added to the network operations to be provided by the vendor. The vendor will also be required to keep an updated data source list on a public website. The "Accounting for Disclosures" provision was struck as no Personal Health Information (PHI) is being stored beyond the metadata. Other provisions were deleted that were included in the past due to the requirements tied to the American Recovery and Reinvestment Act (ARRA) that were never implemented in final rule. Ms. Fox reported that the only change to the Participant responsibilities is to remove the requirement for organizations to hold on to consent forms collected from the patients. Both the Business Associate Agreement (BAA) and the Qualified Service Organization (QSO) provisions were moved from the main body of the Florida HIE General Participation Terms and Conditions and are now listed as Attachments A and B respectively.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

HIPAA Privacy Rule and Sharing Information Related to Mental Health

Background

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides consumers with important privacy rights and protections with respect to their health information, including important controls over how their health information is used and disclosed by health plans and health care providers. Ensuring strong privacy protections is critical to maintaining individuals' trust in their health care providers and willingness to obtain needed health care services, and these protections are especially important where very sensitive information is concerned, such as mental health information. At the same time, the Privacy Rule recognizes circumstances arise where health information may need to be shared to ensure the patient receives the best treatment and for other important purposes, such as for the health and safety of the patient or others. The Rule is carefully balanced to allow uses and disclosures of information—including mental health information—for treatment and these other purposes with appropriate protections.

In this guidance, we address some of the more frequently asked questions about when it is appropriate under the Privacy Rule for a health care provider to share the protected health information of a patient who is being treated for a mental health condition. We clarify when HIPAA permits health care providers to:

- Communicate with a patient's family members, friends, or others involved in the patient's care;
- Communicate with family members when the patient is an adult;
- Communicate with the parent of a patient who is a minor;
- Consider the patient's capacity to agree or object to the sharing of their information;
- Involve a patient's family members, friends, or others in dealing with patient failures to adhere to medication or other therapy;
- Listen to family members about their loved ones receiving mental health treatment;
- Communicate with family members, law enforcement, or others when the patient presents a serious and imminent threat of harm to self or others; and
- Communicate to law enforcement about the release of a patient brought in for an emergency psychiatric hold.

In addition, the guidance provides relevant reminders about related issues, such as the heightened protections afforded to psychotherapy notes by the Privacy Rule, a parent's right to access the protected health information of a minor child as the child's personal representative, the potential applicability of Federal alcohol and drug abuse confidentiality regulations or state laws that may provide more stringent protections for the information than HIPAA, and the intersection of HIPAA and FERPA in a school setting.

AGENCY FOR HEALTH CARE ADMINISTRATION
STATE OF FLORIDA

Questions and Answers about HIPAA and Mental Health

Does HIPAA allow a health care provider to communicate with a patient's family, friends, or other persons who are involved in the patient's care?

Yes. In recognition of the integral role that family and friends play in a patient's health care, the HIPAA Privacy Rule allows these routine – and often critical – communications between health care providers and these persons. Where a patient is present and has the capacity to make health care decisions, health care providers may communicate with a patient's family members, friends, or other persons the patient has involved in his or her health care or payment for care, so long as the patient does not object. See 45 CFR 164.510(b). The provider may ask the patient's permission to share relevant information with family members or others, may tell the patient he or she plans to discuss the information and give them an opportunity to agree or object, or may infer from the circumstances, using professional judgment, that the patient does not object. A common example of the latter would be situations in which a family member or friend is invited by the patient and present in the treatment room with the patient and the provider when a disclosure is made.

Where a patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others involved in the patient's care or payment for care, as long as the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient. Note that, when someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care.

In all cases, disclosures to family members, friends, or other persons involved in the patient's care or payment for care are to be limited to only the protected health information directly relevant to the person's involvement in the patient's care or payment for care.

OCR's website contains additional information about disclosures to family members and friends in fact sheets developed for consumers - PDF and providers - PDF.

Does HIPAA provide extra protections for mental health information compared with other health information?

Generally, the Privacy Rule applies uniformly to all protected health information, without regard to the type of information. One exception to this general rule is for psychotherapy notes, which receive special protections. The Privacy Rule defines psychotherapy notes as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record. Psychotherapy notes do not include any information about medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, or results of clinical tests; nor do they include summaries of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date. Psychotherapy notes also do not include any information that is maintained in a patient's medical record. See 45 CFR 164.501.

Psychotherapy notes are treated differently from other mental health information both because they contain particularly sensitive information and because they are the personal notes of the therapist that typically are not required or useful for treatment, payment, or health care operations purposes, other than by the mental health professional who created the notes. Therefore, with few exceptions, the Privacy Rule requires a covered entity to obtain a patient's authorization prior to a disclosure of psychotherapy notes for any reason, including a disclosure for treatment purposes to a health care provider other than the originator of the notes. See 45 CFR 164.508(a)(2). A notable exception exists for disclosures required by other law, such as for mandatory reporting of abuse, and mandatory "duty to warn" situations regarding threats of serious and imminent harm made by the patient (State laws vary as to whether such a warning is mandatory or permissible).

Is a health care provider permitted to discuss an adult patient's mental health information with the patient's parents or other family members?

In situations where the patient is given the opportunity and does not object, HIPAA allows the provider to share or discuss the patient's mental health information with family members or other persons involved in the patient's care or payment for care. For example, if the patient does not object:

- A psychiatrist may discuss the drugs a patient needs to take with the patient's sister who is present with the patient at a mental health care appointment.
- A therapist may give information to a patient's spouse about warning signs that may signal a developing emergency.

BUT:

- A nurse may not discuss a patient's mental health condition with the patient's brother after the patient has stated she does not want her family to know about her condition.

In all cases, the health care provider may share or discuss only the information that the person involved needs to know about the patient's care or payment for care. See 45 CFR 164.510(b). Finally, it is important to remember that other applicable law (e.g., State confidentiality statutes) or professional ethics may impose stricter limitations on sharing personal health information, particularly where the information relates to a patient's mental health.

When does mental illness or another mental condition constitute incapacity under the Privacy Rule? For example, what if a patient who is experiencing temporary psychosis or is intoxicated does not have the capacity to agree or object to a health care provider sharing information with a family member, but the provider believes the disclosure is in the patient's best interests?

Section 164.510(b)(3) of the HIPAA Privacy Rule permits a health care provider, when a patient is not present or is unable to agree or object to a disclosure due to incapacity or emergency circumstances, to determine whether disclosing a patient's information to the patient's family, friends, or other persons involved in the patient's care or payment for care, is in the best interests of the patient.1 Where a provider determines that such a disclosure is in the patient's best interests, the provider would be permitted to disclose only the PHI that is directly relevant to the person's involvement in the patient's care or payment for care.

This permission clearly applies where a patient is unconscious. However, there may be additional situations in which a health care provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to the sharing of personal health information at a particular time and that sharing the information is in the best interests of the patient at that time. These may include circumstances in which a patient is suffering from temporary psychosis or is under the influence of drugs or alcohol. If, for example, the provider believes the patient cannot meaningfully agree or object to the sharing of the patient's information with family, friends, or other persons involved in their care due to her current mental state, the provider is allowed to discuss the patient's condition or treatment with a family member, if the provider believes it would be in the patient's best interests. In making this determination about the patient's best interests, the provider should take into account the patient's prior expressed preferences regarding disclosures of their information, if any, as well as the circumstances of the current situation. Once the patient regains the capacity to make these choices for herself, the provider should offer the patient the opportunity to agree or object to any future sharing of her information.

Note 1: The Privacy Rule permits, but does not require, providers to disclose information in these situations. Providers who are subject to more stringent privacy standards under other laws, such as certain state confidentiality laws or 42 CFR Part 2, would need to consider whether there is a similar disclosure permission under those laws that would apply in the circumstances.

If a health care provider knows that a patient with a serious mental illness has stopped taking a prescribed medication, can the provider tell the patient's family members?

So long as the patient does not object, HIPAA allows the provider to share or discuss a patient's mental health information with the patient's family members. See 45 CFR 164.510(b). If the provider believes, based on professional judgment, that the patient does not have the capacity to agree or object to sharing the information at that time, and that sharing the information would be in the patient's best interests, the provider may tell the patient's family member. In either case, the health care provider may share or discuss only the information that the family member involved needs to know about the patient's care or payment for care.

Otherwise, if the patient has capacity and objects to the provider sharing information with the patient's family member, the provider may only share the information if doing so is consistent with applicable law and standards of ethical conduct, and the provider has a good faith belief that the patient poses a threat to the health or safety of the patient or others, and the family member is reasonably able to prevent or lessen that threat. See 45 CFR 164.512(j). For example, if a doctor knows from experience that, when a patient's medication is not at a therapeutic level, the patient is at high risk of committing suicide, the doctor may believe in good faith that disclosure is necessary to prevent or lessen the threat of harm to the health or safety of the patient who has stopped taking the prescribed medication, and may share information with the patient's family or other caregivers who can avert the threat. However, absent a good faith belief that the disclosure is necessary to prevent a serious and imminent threat to the health or safety of the patient or others, the doctor must respect the wishes of the patient with respect to the disclosure.

Can a minor child's doctor talk to the child's parent about the patient's mental health status and needs?

With respect to general treatment situations, a parent, guardian, or other person acting in loco parentis usually is the personal representative of the minor child, and a health care provider is permitted to share patient information with a patient's personal representative under the Privacy Rule. However, section 164.502(g) of the Privacy Rule contains several important exceptions to this general rule. A parent is not treated as a minor child's personal representative when: (1) State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, the minor consents to the health care service, and the minor child has not requested the parent be treated as a personal representative; (2) someone other than the parent is authorized by law to consent to the provision of a particular health service to a minor and provides such consent; or (3) a parent agrees to a confidential relationship between the minor and a health care provider with respect to the health care service.2 For example, if State law provides an adolescent the right to obtain mental health treatment without parental consent, and the adolescent consents to such treatment, the parent would not be the personal representative of the adolescent with respect to that mental health treatment information.

Regardless, however, of whether the parent is otherwise considered a personal representative, the Privacy Rule defers to State or other applicable laws that expressly address the ability of the parent to obtain health information about the minor child. In doing so, the Privacy Rule permits a covered entity to disclose to a parent, or provide the parent with access to, a minor child's protected health information when and to the extent it is permitted or required by State or other laws (including relevant case law). Likewise, the Privacy Rule prohibits a covered entity from disclosing a minor child's protected health information to a parent when and to the extent it is prohibited under State or other laws (including relevant case law). See 45 CFR 164.502(g)(3)(ii).

In cases in which State or other applicable law is silent concerning disclosing a minor's protected health information to a parent, and the parent is not the personal representative of the minor child based on one of the exceptional circumstances described above, a covered entity has discretion to provide or deny a parent access to the minor's health information, if doing so is consistent with State or other applicable law, and the decision is made by a licensed health care professional in the exercise of professional judgment. For more information about personal representatives under the Privacy Rule, see OCR's guidance for consumers and providers.

In situations where a minor patient is being treated for a mental health disorder and a substance abuse disorder, additional laws may be applicable. The Federal confidentiality statute and regulations that apply to

federally-funded drug and alcohol abuse treatment programs contain provisions that are more stringent than HIPAA. See 42 USC § 290dd–2; 42 CFR 2.11, et. seq.

Note 2: A parent also may not be a personal representative if there are safety concerns. A provider may decide not to treat the parent as the minor's personal representative if the provider believes that the minor has been or may be subject to violence, abuse, or neglect by the parent or the minor may be endangered by treating the parent as the personal representative; and the provider determines, in the exercise of professional judgment, that it is not in the best interests of the patient to treat the parent as the personal representative. See 45 CFR 164.502(g)(5).

At what age of a child is the parent no longer the personal representative of the child for HIPAA purposes?

HIPAA defers to state law to determine the age of majority and the rights of parents to act for a child in making health care decisions, and thus, the ability of the parent to act as the personal representative of the child for HIPAA purposes. See 45 CFR 164.502(g).

Does a parent have a right to receive a copy of psychotherapy notes about a child's mental health treatment?

No. The Privacy Rule distinguishes between mental health information in a mental health professional's private notes and that contained in the medical record. It does not provide a right of access to psychotherapy notes, which the Privacy Rule defines as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record. See 45 CFR 164.501. Psychotherapy notes are primarily for personal use by the treating professional and generally are not disclosed for other purposes. Thus, the Privacy Rule includes an exception to an individual's (or personal representative's) right of access for psychotherapy notes. See 45 CFR 164.524(a)(1)(i).

However, parents generally are the personal representatives of their minor child and, as such, are able to receive a copy of their child's mental health information contained in the medical record, including information about diagnosis, symptoms, treatment plans, etc. Further, although the Privacy Rule does not provide a right for a patient or personal representative to access psychotherapy notes regarding the patient, HIPAA generally gives providers discretion to disclose the individual's own protected health information (including psychotherapy notes) directly to the individual or the individual's personal representative. As any such disclosure is purely permissive under the Privacy Rule, mental health providers should consult applicable State law for any prohibitions or conditions before making such disclosures.

What options do family members of an adult patient with mental illness have if they are concerned about the patient's mental health and the patient refuses to agree to let a health care provider share information with the family?

The HIPAA Privacy Rule permits a health care provider to disclose information to the family members of an adult patient who has capacity and indicates that he or she does not want the disclosure made, only to the extent that the provider perceives a serious and imminent threat to the health or safety of the patient or others and the family members are in a position to lessen the threat. Otherwise, under HIPAA, the provider must respect the wishes of the adult patient who objects to the disclosure. However, HIPAA in no way prevents health care providers from listening to family members or other caregivers who may have concerns about the health and well-being of the patient, so the health care provider can factor that information into the patient's care.

In the event that the patient later requests access to the health record, any information disclosed to the provider by another person who is not a health care provider that was given under a promise of confidentiality (such as that shared by a concerned family member), may be withheld from the patient if the disclosure would be reasonably likely to reveal the source of the information. 45 CFR 164.524(a)(2)(v). This exception to the

patient's right of access to protected health information gives family members the ability to disclose relevant safety information with health care providers without fear of disrupting the family's relationship with the patient.

Does HIPAA permit a doctor to contact a patient's family or law enforcement if the doctor believes that the patient might hurt herself or someone else?

Yes. The Privacy Rule permits a health care provider to disclose necessary information about a patient to law enforcement, family members of the patient, or other persons, when the provider believes the patient presents a serious and imminent threat to self or others. The scope of this permission is described in a letter to the nation's health care providers - PDF

Specifically, when a health care provider believes in good faith that such a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others, the Privacy Rule allows the provider, consistent with applicable law and standards of ethical conduct, to alert those persons whom the provider believes are reasonably able to prevent or lessen the threat. These provisions may be found in the Privacy Rule at 45 CFR § 164.512(j).

Under these provisions, a health care provider may disclose patient information, including information from mental health records, if necessary, to law enforcement, family members of the patient, or any other persons who may reasonably be able to prevent or lessen the risk of harm. For example, if a mental health professional has a patient who has made a credible threat to inflict serious and imminent bodily harm on one or more persons, HIPAA permits the mental health professional to alert the police, a parent or other family member, school administrators or campus police, and others who may be able to intervene to avert harm from the threat.

In addition to professional ethical standards, most States have laws and/or court decisions which address, and in many instances require, disclosure of patient information to prevent or lessen the risk of harm. Providers should consult the laws applicable to their profession in the States where they practice, as well as 42 USC 290dd-2 and 42 CFR Part 2 under Federal law (governing the disclosure of alcohol and drug abuse treatment records) to understand their duties and authority in situations where they have information indicating a threat to public safety. Note that, where a provider is not subject to such State laws or other ethical standards, the HIPAA permission still would allow disclosures for these purposes to the extent the other conditions of the permission are met.

If a law enforcement officer brings a patient to a hospital or other mental health facility to be placed on a temporary psychiatric hold, and requests to be notified if or when the patient is released, can the facility make that notification?

The Privacy Rule permits a HIPAA covered entity, such as a hospital, to disclose certain protected health information, including the date and time of admission and discharge, in response to a law enforcement official's request, for the purpose of locating or identifying a suspect, fugitive, material witness, or missing person. See 45 CFR § 164.512(f)(2). Under this provision, a covered entity may disclose the following information about an individual: name and address; date and place of birth; social security number; blood type and rh factor; type of injury; date and time of treatment (includes date and time of admission and discharge) or death; and a description of distinguishing physical characteristics (such as height and weight). However, a covered entity may not disclose any protected health information under this provision related to DNA or DNA analysis, dental records, or typing, samples, or analysis of body fluids or tissue. The law enforcement official's request may be made orally or in writing.

Other Privacy Rule provisions also may be relevant depending on the circumstances, such as where a law enforcement official is seeking information about a person who may not rise to the level of a suspect, fugitive, material witness, or missing person, or needs protected health information not permitted under the above provision. For example, the Privacy Rule's law enforcement provisions also permit a covered entity to respond to an administrative request from a law enforcement official, such as an investigative demand for a patient's protected health information, provided the administrative request includes or is accompanied by a written statement specifying that the information requested is relevant, specific and limited in scope, and that de-identified information would not suffice in that situation. The Rule also permits covered entities to respond to court orders and court-ordered warrants, and subpoenas and summonses issued by judicial officers. See 45 CFR § 164.512(f)(1). Further, to the extent that State law may require providers to make certain disclosures,

the Privacy Rule would permit such disclosures of protected health information as "required-by-law" disclosures. See 45 CFR § 164.512(a).

Finally, the Privacy Rule permits a covered health care provider, such as a hospital, to disclose a patient's protected health information, consistent with applicable legal and ethical standards, to avert a serious and imminent threat to the health or safety of the patient or others. Such disclosures may be to law enforcement authorities or any other persons, such as family members, who are able to prevent or lessen the threat. See 45 CFR § 164.512(j).

If a doctor believes that a patient might hurt himself or herself or someone else, is it the duty of the provider to notify the family or law enforcement authorities?

A health care provider's "duty to warn" generally is derived from and defined by standards of ethical conduct and State laws and court decisions such as Tarasoff v. Regents of the University of California. HIPAA permits a covered health care provider to notify a patient's family members of a serious and imminent threat to the health or safety of the patient or others if those family members are in a position to lessen or avert the threat. Thus, to the extent that a provider determines that there is a serious and imminent threat of a patient physically harming self or others, HIPAA would permit the provider to warn the appropriate person(s) of the threat, consistent with his or her professional ethical obligations and State law requirements. See 45 CFR 164.512(j). In addition, even where danger is not imminent, HIPAA permits a covered provider to communicate with a patient's family members, or others involved in the patient's care, to be on watch or ensure compliance with medication regimens, as long as the patient has been provided an opportunity to agree or object to the disclosure and no objection has been made. See 45 CFR 164.510(b)(2).

Does HIPAA prevent a school administrator, or a school doctor or nurse, from sharing concerns about a student's mental health with the student's parents or law enforcement authorities?

Student health information held by a school generally is subject to the Family Educational Rights and Privacy Act (FERPA), not HIPAA. HHS and the Department of Education have developed guidance clarifying the application of HIPAA and FERPA - PDF

In the limited circumstances where the HIPAA Privacy Rule, and not FERPA, may apply to health information in the school setting, the Rule allows disclosures to parents of a minor patient or to law enforcement in various situations. For example, parents generally are presumed to be the personal representatives of their unemancipated minor child for HIPAA privacy purposes, such that covered entities may disclose the minor's protected health information to a parent. See 45 CFR § 164.502 (g)(3). In addition, disclosures to prevent or lessen serious and imminent threats to the health or safety of the patient or others are permitted for notification to those who are able to lessen the threat, including law enforcement, parents or others, as relevant. See 45 CFR § 164.512(j).

Additional FAQs on Sharing Information Related to Treatment for Mental Health or Substance Use Disorder—Including Opioid Abuse

ADULT PATIENTS

Does having a health care power of attorney (POA) allow access to the patient's medical and mental health records under HIPAA?

Generally, yes. If a health care power of attorney is currently in effect, the named person would be the patient's personal representative (The period of effectiveness may depend on the type of power of attorney: Some health care power of attorney documents are effective immediately, while others are only triggered if and when the patient lacks the capacity to make health care decisions and then cease to be effective if and when the patient regains such capacity).

"Personal representatives," as defined by HIPAA, are those persons who have authority, under applicable law, to make health care decisions for a patient. HIPAA provides a personal representative of a patient with the same rights to access health information as the patient, including the right to request a complete medical record containing mental health information. The patient's right of access has some exceptions, which would also apply to a personal representative. For example, with respect to mental health information, a psychotherapist's separate notes of counseling sessions, kept separately from the patient chart, are not included in the HIPAA right of access.

Additionally, a provider may decide not to treat someone as the patient's personal representative if the provider believes that the patient has been or may be subject to violence, abuse, or neglect by the designated person or the patient may be endangered by treating such person as the personal representative, and the provider determines, in the exercise of professional judgment, that it is not in the best interests of the patient to treat the person as the personal representative. See 45 CFR 164.502(g)(5).

Does HIPAA permit health care providers to share protected health information (PHI) about an individual who has mental illness with other health care providers who are treating the same individual for care coordination/continuity of care purposes?

HIPAA permits health care providers to disclose to other health providers any protected health information (PHI) contained in the medical record about an individual for treatment, case management, and coordination of care and, with few exceptions, treats mental health information the same as other health information. Some examples of the types of mental health information that may be found in the medical record and are subject to the same HIPAA standards as other protected health information include:

- medication prescription and monitoring
- counseling session start and stop times
- the modalities and frequencies of treatment furnished
- results of clinical tests
- summaries of: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

HIPAA generally does not limit disclosures of PHI between health care providers for treatment, case management, and care coordination, except that covered entities must obtain individuals' authorization to disclose separately maintained psychotherapy session notes for such purposes. Covered entities should determine whether other rules, such as state law or professional practice standards place additional limitations on disclosures of PHI related to mental health.

For more information see:

Does HIPAA provide extra protections for mental health information compared with other health information?

Does HIPAA permit health care providers to share protected health information (PHI) about an individual with mental illness with a third party that is not a health care provider for case management or continuity of care purposes? For example, can a health care provider refer a homeless patient to a social services agency, such as a housing provider, when doing so may reveal that the basis for eligibility is related to mental health?

HIPAA, with few exceptions, treats all health information, including mental health information, the same. HIPAA allows health care providers to disclose protected health information (PHI), including mental health information, to other public or private-sector entities providing social services (such as housing, income support, job training) in specified circumstances. For example:

- A health care provider may disclose a patient's PHI for treatment purposes without having to obtain the authorization of the individual. Treatment includes the coordination or management of health care by a health care provider with a third party. Health care means care, services, or supplies related to the health of an individual. Thus, health care providers who believe that disclosures to certain social service entities are a necessary component of, or may help further, the individual's health or mental health care may disclose the minimum necessary PHI to such entities without the individual's authorization. For example, a provider may disclose PHI about a patient needing mental health care supportive housing to a service agency that arranges such services for individuals.
- A covered entity may also disclose PHI to such entities pursuant to an authorization signed by the individual. HIPAA permits authorizations that refer to a class of persons who may receive or use the PHI. Thus, providers could in one authorization identify a broad range of social services entities that may receive the PHI if the individual agrees. For example, an authorization could indicate that PHI will be disclosed to "social services providers" for purposes of "supportive housing, public benefits, counseling, and job readiness."

EMERGENCIES, EMERGENCY HOSPITALIZATION OR DANGEROUS SITUATIONS

When does HIPAA allow a doctor to notify an individual's family, friends, or caregivers that a patient has overdosed, e.g., because of opioid abuse?

As explained more thoroughly below, when a patient has overdosed, a health care professional, such as a doctor, generally may notify the patient's family, friends, or caregivers involved in the patient's health care or payment for care if:

(1) the patient has the capacity to make health care decisions at the time of the disclosure, is given the opportunity to object, and does not object;

(2) the family, friends, or caregivers have been involved in the patient's health care or payment for care and there has been no objection from the patient;

(3) the patient had the capacity to make health care decisions at the time the information is shared and the doctor can reasonably infer, based on the exercise of professional judgment, that the patient would not object;

(4) the patient is incapacitated and the health care professional determines, based on the exercise of professional judgment, that notification and disclosure of PHI is in the patient's best interests;

(5) the patient is unavailable due to some emergency and the health care professional determines, based on the exercise of professional judgment, that notification and disclosure of PHI is in the patient's best interests; or

(6) the notification is necessary to prevent a serious and imminent threat to the health or safety of the patient or others.

If the patient who has overdosed is incapacitated and unable to agree or object, a doctor may notify a family member, personal representative, or another person responsible for the individual's care of the patient's location, general condition, or death. See 45 CFR 164.510(b)(1)(ii). Similarly, HIPAA allows a doctor to share additional information with a patient's family member, friend, or caregiver as long as the information shared is directly related to the person's involvement in the patient's health care or payment for care. 45 CFR 164.510(b)(1)(i). Decision-making incapacity may be temporary or long-term. If a patient who has overdosed regains decision-making capacity, health providers must offer the patient the opportunity to agree or object to sharing their health information with involved family, friends, or caregivers before making any further disclosures. If a patient becomes unavailable due to some emergency, a health care professional may

determine, based on the exercise of professional judgment, that notification and disclosure of PHI to someone previously involved in their care is in the patient's best interests. For example, if a patient who is addicted to opioids misses important medical appointments without any explanation, a primary health care provider at a general practice may believe that there is an emergency related to the opioid addiction and under the circumstances, may use professional judgment to determine that it is in the patient's best interests to reach out to emergency contacts, such as parents or family, and inform them of the situation. See 45 CFR 164.510(b)(3).

If the patient is deceased, a doctor may disclose information related to the family member's, friend's, or caregiver's involvement with the patient's care, unless doing so is inconsistent with any prior expressed preference of the patient that is known to the doctor. If the person who will receive notification is the patient's personal representative, that person has a right to request and obtain any information about the patient that the patient could obtain, including a complete medical record, under the HIPAA right of access. See 45 CFR 164.524.

When a patient poses a serious and imminent threat to his own or someone else's health or safety, HIPAA permits a health care professional to share the necessary information about the patient with anyone who is in a position to prevent or lessen the threatened harm--including family, friends, and caregivers--without the patient's permission. See 45 CFR 164.512(j). HIPAA expressly defers to the professional judgment of health care professionals when they make determinations about the nature and severity of the threat to health or safety. See 45 CFR 164.512(j)(4). Specifically, HIPAA presumes the health care professional is acting in good faith in making this determination, if the professional relies on his or her actual knowledge or on credible information from another person who has knowledge or authority. For example, a doctor whose patient has overdosed on opioids is presumed to have complied with HIPAA if, based on talking with or observing the patient, the doctor determines that the patient poses a serious and imminent threat to his or her own health. Even when HIPAA permits this disclosure, however, the disclosure must be consistent with applicable state law and standards of ethical conduct. HIPAA does not preempt any state law or professional ethics standards that would prevent a health care professional from sharing protected health information in the circumstances described here. For example, the doctor in this situation still may be subject to a state law that prohibits sharing information related to mental health or a substance use disorder without the patient's consent in all circumstances, even if HIPAA would permit the disclosure.

For more information see OCR's guidance, *How HIPAA Allows Doctors to Respond to the Opioid Crisis*, https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf

When does HIPAA allow a hospital to notify an individual's family, friends, or caregivers that a patient who has been hospitalized for a psychiatric hold has been admitted or discharged?

Hospitals may notify family, friends, or caregivers of a patient in several circumstances:

- **When the patient has a personal representative**

A hospital may notify a patient's personal representative about their admission or discharge and share other PHI with the personal representative without limitation. However, a hospital is permitted to refuse to treat a person as a personal representative if there are safety concerns associated with providing the information to the person, or if a health care professional determines that disclosure is not in the patient's best interest.

- **When the patient agrees or does not object to family involvement**

A hospital may notify a patient's family, friends, or caregivers if the patient agrees, or doesn't object, or if a health care professional is able to infer from the surrounding circumstances, using professional judgment that the patient does not object. This includes when a patient's family, friends, or caregivers have been involved in the patient's health care in the past, and the individual did not object.

- **When the patient becomes unable to agree or object and there has already been family involvement**

When a patient is not present or cannot agree or object because of some incapacity or emergency, a health care provider may share relevant information about the patient with family, friends, or others involved in the patient's care or payment for care if the health care provider determines, based on professional judgment, that doing so is in the best interest of the patient.

For example, a psychiatric hospital may determine that it is in the best interests of an incapacitated patient to initially notify a member of their household, such as a parent, roommate, sibling, partner, or spouse, and inform them about the patient's location and general condition. This may include, for example, notifying a patient's spouse that the patient has been admitted to the hospital.

If the health care provider determines that it is in the patient's interest, the provider may share additional information that is directly related to the family member's or friend's involvement with the patient's care or payment for care, after they clarify the person's level of involvement. For example, a nurse treating a patient may determine that it is in the patient's best interest to discuss with the patient's adult child, who is the patient's primary caregiver, the medications found in a patient's backpack and ask about any other medications the patient may have at home.

Decision-making incapacity may be temporary or long-term. Upon a patient's regaining decision-making capacity, health providers should offer the patient the opportunity to agree or object to sharing their health information with involved family, friends, or caregivers.

- **When notification is needed to lessen a serious and imminent threat of harm to the health or safety of the patient or others**

A hospital may disclose the necessary protected health information to anyone who is in a position to prevent or lessen the threatened harm, including family, friends, and caregivers, without a patient's agreement. HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health or safety. For example, a health care provider may determine that a patient experiencing a mental health crisis has ingested an unidentified substance and that the provider needs to contact the patient's roommate to help identify the substance and provide the proper treatment, or the patient may have made a credible threat to harm a family member, who needs to be notified so he or she can take steps to avoid harm. OCR would not second guess a health care professional's judgment in determining that a patient presents a serious and imminent threat to their own, or others', health or safety.

What constitutes a "serious and imminent" threat that would permit a health care provider to disclose PHI to prevent harm to the patient, another person, or the public without the patient's authorization or permission?

HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health or safety posed by a patient. OCR would not second guess a health professional's good faith belief that a patient poses a serious and imminent threat to the health or safety of the patient or others and that the situation requires the disclosure of patient information to prevent or lessen the threat. Health care providers may disclose the necessary protected health information to anyone who is in a position to prevent or lessen the threatened harm, including family, friends, caregivers, and law enforcement, without a patient's permission.

See Guidance on Sharing Information Related to Mental Health, https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html

If an adult patient who may pose a danger to self stops coming to psychotherapy sessions and does not respond to attempts to make contact, does HIPAA permit the therapist to contact a family member to check on the patient's well-being even if the patient has told the therapist that they do not want information shared with that person?

Yes, under two possible circumstances:

1. Given that the patient is no longer present, if the therapist determines, based on professional judgment, that there may be an emergency situation and that contacting the family member of the absent patient is in the patient's best interests; or
2. If the disclosure is needed to lessen a serious and imminent threat and the family member is in a position to avert or lessen the threat.

In making the determination about the patient's best interests, the provider may take into account the patient's prior expressed preferences regarding disclosures of their information, if any, as well as the circumstances of the current situation. In either case, the health care provider may share or discuss only the information that the family member involved needs to know about the patient's care or payment for care or the minimum necessary for the purpose of preventing or lessening the threatened harm.

Additionally, if the family member is a personal representative of the patient, the therapist may contact that person. However, a provider may decide not to treat someone as a personal representative if the provider believes that the patient has been or may be subject to violence, abuse, or neglect by the personal representative, or the patient may be endangered by treating the person as the personal representative; and the provider determines, in the exercise of professional judgment, that it is not in the best interests of the patient to treat the person as the personal representative. See 45 CFR 164.502(g)(5).

See Guidance on Sharing Information Related to Mental Health, https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html

Guidance on Personal Representatives, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html

Does HIPAA require a mental health provider to let a patient know that the provider is going to share information with others before disclosing PHI to prevent or lessen a serious and imminent threat?

Not at the time of disclosure; however, the Notice of Privacy Practices should contain an example of this type of disclosure so patients are informed in advance of that possibility. See 45 CFR 164.520(b). In situations that also involve reports to the appropriate government authority that the patient may be an adult victim of abuse, neglect, or domestic violence, the mental health provider must promptly inform the patient that a report has been or will be made, unless:

- informing the patient would create a danger to the patient; or
- the provider would be informing a personal representative, and the provider reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the patient is determined by the provider, in the exercise of professional judgment. See 45 CFR 164.512(c).

Other standards, such as clinical protocols, ethics rules, or state laws, may also be applicable to patient notification about disclosures in situations involving threats of imminent harm.

SUBSTANCE USE DISORDER TREATMENT

How does HIPAA interact with the federal confidentiality rules for information about substance use disorder treatment, including treatment for opioid abuse, in an emergency situation—which rules should be followed?

A health provider that provides treatment for substance use disorders, including opioid abuse, needs to determine whether it is subject to 42 CFR Part 2 (i.e., a "Part 2 program") and whether it is a covered entity under HIPAA. Generally, the Part 2 rules provide more stringent privacy protections than HIPAA, including in emergency situations. If an entity is subject to both Part 2 and HIPAA, it is responsible for complying with the more protective Part 2 rules, as well as with HIPAA. HIPAA is intended to be a set of minimum federal privacy standards, so it generally is possible to comply with HIPAA and other laws, such as 42 CFR Part 2, that are more protective of individuals' privacy.

For example, HIPAA permits disclosure of protected health information (PHI) for treatment purposes (including in emergencies) without patient authorization, and allows PHI to be used or disclosed to lessen a threat of serious and imminent harm to the health or safety of the patient or others (which may occur as part of a health emergency) without patient authorization or permission. Because HIPAA permits, but does not require, disclosures for treatment or to prevent harm, if Part 2 restricts certain disclosures during an emergency, an entity subject to both sets of requirements could comply with Part 2's restrictions without violating HIPAA.

For more information about applying 42 CFR Part 2 in an emergency, see https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs

Patient Centered Data Home® (PCDH)

Leadership : PCDH Governance Council (Chair: Keith Kelley; Vice-Chair: Brandon Neiswender; Civitas Networks for Health: Lisa Bari, CEO
Website Information : http://www.civitasforhealth.org
Date Formed : 2015 (PCDH concept)

Ownership

Non-profit

Governance

Allows for the independent regional and statewide HIEs that are members of Civitas Networks for Health (formerly known as the Strategic Health Information Exchange Collaborative (SHIEC)) to maintain their autonomy and governance while gaining economies of scale. The key issues of disparate data use agreements, policies and patient privacy and consent models are overcome in this framework of patient data exchange

Geographic Reach (within US)

Regional/Nationwide

Mission

Civitas Networks for Health is a national collaborative comprised of member organizations working to use health information exchange, health data, and multi-stakeholder, cross-sector approaches to improve health. We were previously known as the Strategic Health Information Exchange Collaborative and the Network for Regional Healthcare Improvement. We represent more than 150 local health innovators from across the US, moving data to improve health outcomes for more than 95% of the U.S. population. Civitas educates, promotes, and influences both the private sector and policy makers on matters of interoperability, quality, coordination, health equity, and cost-effectiveness of health care. Working with health innovators at state and local levels, we facilitate the exchange of valuable resources, tools, and ideas—and offer a national perspective on upcoming standards and regulations, emerging technologies, and best practices.

How does this approach facilitate exchange?

PCDH enables the exchange of patient information across HIE organizations. Patients are assigned a "home HIE" based on zip codes associated with an HIE. This exchange depends on triggering episode alerts that notify the home HIE of an event that occurs outside the patient's residing region. This trigger alert enables the non-home HIE and the home HIE to share relevant patient information to coordinate better patient care.

Access Method (Use Cases)

Peer-to-peer push and/or query-based exchange triggered by automated notification of care event.

Primary Goals/Objectives

Civitas Networks for Health:

- Improving care coordination and care management across disparate health care systems and the health care community
- Enabling more informed clinical decision making through more comprehensive patient records and near real-time notification of health care events and results
- Aggregating better information and analysis through cross-system risk stratification and population health analytics
- Eliminating unnecessary or duplicative tests and procedures, and reducing hospital readmissions and other preventable expenditures.

Patient Centered Data Home™ (PCDH):

- Notify providers a care event occurred outside of the patients' "home" HIE.
- Confirm availability and location of clinical data. Transmit all relevant clinical data for "away" care event and to "home" HIE to contribute to a longitudinal patient record.
- Enable providers to initiate a simple query to access real-time information across state and regional lines and the care continuum.

Type

Patient-centric network

Number of Live Connections and/or Participants

PCDH currently has 45 HIEs connected in regional settings; however, the member HIEs represent many data source connections in their individual markets. At present, the members of Civitas Networks for Health provide services the majority of the population of the United States.

(As of August 2022)

Members

Civitas Networks for Health member HIE entities/organizations

Primary Participants

As of August 2022, 45 HIEs from the Western, Central, Midwest, Heartland, and Eastern regions of the US.

Costs (Amount and/or Party Incurring Cost)

Civitas Networks for Health Membership for qualified HIE organizations start at $7,000 per year, and increase based on organizational revenue.

Strategic Business and Technology Partner Membership incur membership fees based on their organization's gross annual revenue.

Civitas Networks for Health does not have provisions permitting or prohibiting participants from charging one another fees for transactions made through PCDH.

Directory/MPI Details

PCDH does not maintain a central record locator service, the member HIEs transmit clinical based upon the zip codes that they serve, providing a simple method for record location, without extensive record maintenance/archival.

Standards Leveraged

Technical Standards: ADT Push, CCD Push, CCD Query (XCA)

Zip Code Surveillance standards: Synchronized MPI's around a specific patient

ADT Standards - content

Targeted XCA Query – event certainty and patient certainty

IHE profiles & HL7v2

Onboarding Process (Requirements to connect)

PCDH is an initiative solely with Civitas Networks for Health members and is currently structured as 5 regional efforts where policies and trust agreements have been outlined between participating HIEs.

As of August 28, 2017, at the national SHIEC conference, a National Master Collaboration Agreement was released to allow all

PCDH Regions to exchange with each other. This National Agreement provides national governance, sets national standards, policies and procedures for i) technical specifications, ii) national use cases and permitted uses, and iii) other needed policies and procedures to operate national structure.

Data Persistance

All clinical data becomes part of the comprehensive longitudinal patient record in the patients' data home, which is the community health information exchange associated with where the patient resides.

Certification Requirements for Participation

Participation requirements are governed by the PCDH National Master Collaboration Agreement.

Testing

Interested HIEs must complete the necessary testing before going live within PCDH.

Future Plans

Continue to service the local/regional/state communities in support of the current and changing healthcare landscape

Current Collaboration across Efforts

Regional and statewide HIEs and Regional Health Improvement Collaboratives make up Civitas membership and comprise the PCDH regions.

Consent Policy

Patient Consent Discussion

Background:

The current Florida Health Information Exchange (HIE) Encounter Notification Service (ENS) began operations in November 2013 with one hospital data source. ENS delivers alerts about a patient's inpatient or emergency department encounter to a permitted recipient with an existing relationship to the patient, such as a health plan or primary care provider. In June 2014, the Agency informed hospitals that the Low-Income Pool (LIP) participation requirements for SFY 2014-2015 include participation in ENS as a data source. Organizations representing 203 hospitals signed the ENS agreement for participation as a data source in 2014. The data sent from data sources is only retained long enough to ensure appropriate matching to data subscribers and is then deleted.

As of September 30, 2023, ENS has around 800 data sources made up of hospitals, home health agencies, skilled nursing facilities, crisis stabilization units, urgent care facilities, hospice, and county health departments. Of the 800 data sources, 551 are subscribed to receive ENS encounter data with a total of 244 subscription agreements.

Pursuant to Chapter 2009-172, Laws of Florida, patient records are confidential and must not be disclosed without the consent of the patient. Appropriate disclosure is permitted, without consent, for the purpose of treatment to other health care providers involved in patient care. The exception to treatment purpose disclosure is for behavioral health records. Section 394.4615, Florida Statutes currently requires the patient to provide explicit consent for the release of clinical records. The current consent model requires data recipients to obtain patient consent to ensure that the need to receive explicit consent for mental health data sharing is received, since there is no way to confirm consent to share is obtained from data sources.

At the February 2017 HIECC meeting the PLU User Group (now known as the HIE Alliance) reported concerns with moving from a consent to release versus a consent to query model due to technical and legal considerations that would need to be addressed by individual hospitals.

A discussion was had at the November 29, 2018 HIECC meeting regarding the barriers to participating in cross state data sharing based on consent restrictions for sharing mental health data.

Current Issue:

The current consent model does not prohibit ENS data sources from share data (including mental health data) without obtaining consent to share from the patient. Data recipients must obtain consent to receive patient information, consent must be received prior to data recipient putting a patient on their panel. To allow for data to be shared to HIE users in other states, the current Florida HIE consent model would need to be changed to require data sources to obtain consent to share information, in order to continue sharing mental health data.

Discussion:

- To enable the ability to share interstate data, that includes behavioral health data, what technical and operational consideration does the Agency need to consider if the consent model were changed to allow for consent to share versus consent to receive?

- Would data sources using opt-out models have to modify their consent policy to opt-in to meet a consent to share requirement?

Supplemental Information:

- Excerpt from February 10, 2017 HIECC Meeting Minutes
- Excerpt from December 1, 2017 Legal Workgroup Meeting Minutes
- Excerpts from November 29, 201 HIECC Meeting Minutes
- Section 394.4615, Florida Statutes
- Chapter 2009-172, Laws of Florida

Excerpt from February 10, 2017 HIECC Meeting Minutes

PLU User Group Report: Ms. Cole reported that the User Group had a discussion about AHCA's proposed changes to the subscription agreements. Service Level agreements will continue to be reviewed and, when finalized, will be added to the subscription agreements. She added that there was a lengthy discussion about the proposed shift in consent models. The Group determined, by majority vote, that members cannot feasibly make the shift from Consent to Query to Consent to Release at this time due to technical and legal considerations that must be addressed first. They will continue to move their organizations in that direction, realizing that Consent to Release is the preferred model of other stakeholders. Ms. Cole added that The User Group and AHCA will develop a roadmap for changing the consent model.

Program Metric and Updates: Ms. Fox addressed the PLU User Agreement and the consideration to move the current Consent to Query model to a Consent to Release model. She stated that most HIE organizations including the VA use the Consent to Release model. The Despite this, the PLU User Group voted unanimously to remain with the Consent to Query model due primarily to process and technical issues they will need to address before adopting the new model.

Excerpts from December 1, 2017 Legal Workgroup and December 5, 2017 HIECC Meeting Minutes:

Legal Workgroup 12/1/2017

Consent: Ms. Fox provided some background on consent policy. Given Florida's statutory restrictions on the release of mental health information, electronic health information exchange in Florida requires an "opt-in" consent policy. "Opt-in" requires express consent for a record to be accessed or released. There are two ways to comply with opt-in: consent to access (also known as consent to query) and consent to release. A consent to access policy was adopted for the PLU service where a treating provider at the point of care had to obtain patient consent to query for records from other providers. The infrastructure implemented for the PLU service included an audit application called FairWarning that allowed participants to see who had queried for their data, in order to monitor activity, and ensure appropriate patient consent had been obtained. This audit capability is not available in the eHX.

Ms. Fox explained that the eHX is governed by the DURSA (Data Use Reciprocal Support Agreement), which stipulates that participants are required to obtain appropriate consents for exchange. This very broad language puts the responsibility of consent compliance onto the participants, guided by state and local laws. For most query based health information exchange services, participants obtain consent prior to releasing patient records. This means that when a treating provider queries for records, participants responding with records have obtained patient consent prior to releasing the information. Participants have indicated that the consent forms can be broadly phrased to cover both forms of opt-in authorizations. For query based exchange, the Agency is leaving consent management in the hands of the covered entities. Ms. Fox noted that some types of exchange, such as providers subscribing to the ENS, consent to access patient information is required because patient data may be available for which consent to release was not obtained.

HIE Coordinating Committee 12/5/2017

LWG Report: The LWG members were interested in the type of Consent model required Florida. Ms. Fox clarified to the work group that although HIPAA allows the exchange of health information for treating purposes with an opt-out provision. Florida's statutory restrictions on the release of mental health information requires an "opt-in" process for release of electronic Health Information. "Opt in", in a broad sense, provides explicit consent for a record to be queried or released. There are two ways to comply with opt in, consent to query and consent to release. We used consent to query in our PLU service where a treating provider at the point of care had to acquire patient consent to query for records from other providers.

Ms. Fox explained that consent requirements for the e-Health Exchange are governed by the DURSA (Data Use Reciprocal Support Agreement), which stipulates that participants be required to obtain appropriate consents for exchange. The Florida HIE has therefore determined to leave consent management in the hands of participants, guided by the requirements of HIPAA and Florida law.

Excerpts from November 29, 201 HIECC Meeting Minutes

Florida HIE Advisory Strategies Follow-Up: Ms. Fox presented the current Quarterly Inquiries, which are focused around the topics that will be discussed in the upcoming Legal Work Group meeting. These topics potentially include a review of the ENS Participation Agreement with potential Addenda, a discussion on the Data Use and Reciprocal Support Agreement (DURSA) signatory as part of eHealth Exchange activities, Patient Centered Data Home and the barriers in Florida concerning sharing mental health data across states, and a discussion about adding pharmacists as subscribers to ENS and how the consent requirements can be met.

Section 394.4615, Florida Statutes, Mental Health

394.4615 Clinical records; confidentiality.—

(1) A clinical record shall be maintained for each patient. The record shall include data pertaining to admission and such other information as may be required under rules of the department. A clinical record is confidential and exempt from the provisions of s. 119.07(1). Unless waived by express and informed consent, by the patient or the patient's guardian or guardian advocate or, if the patient is deceased, by the patient's personal representative or the family member who stands next in line of intestate succession, the confidential status of the clinical record shall not be lost by either authorized or unauthorized disclosure to any person, organization, or agency.

(2) The clinical record shall be released when:

(a) The patient or the patient's guardian authorizes the release. The guardian or guardian advocate shall be provided access to the appropriate clinical records of the patient. The patient or the patient's guardian or guardian advocate may authorize the release of information and clinical records to appropriate persons to ensure the continuity of the patient's health care or mental health care. A receiving facility must document that, within 24 hours of admission, individuals admitted on a voluntary basis have been provided with the option to authorize the release of information from their clinical record to the individual's health care surrogate or proxy, attorney, representative, or other known emergency contact.

(b) The patient is represented by counsel and the records are needed by the patient's counsel for adequate representation.

(c) The court orders such release. In determining whether there is good cause for disclosure, the court shall weigh the need for the information to be disclosed against the possible harm of disclosure to the person to whom such information pertains.

(d) The patient is committed to, or is to be returned to, the Department of Corrections from the Department of Children and Families, and the Department of Corrections requests such records. These records shall be furnished without charge to the Department of Corrections.

(3) Information from the clinical record may be released in the following circumstances:

(a) When a patient has communicated to a service provider a specific threat to cause serious bodily injury or death to an identified or a readily available person, if the service provider reasonably believes, or should reasonably believe according to the standards of his or her profession, that the patient has the apparent intent and ability to imminently or immediately carry out such threat. When such communication has been made, the administrator may authorize the release of sufficient information to provide adequate warning to the person threatened with harm by the patient.

(b) When the administrator of the facility or secretary of the department deems release to a qualified researcher as defined in administrative rule, an aftercare treatment provider, or an employee or agent of the department is necessary for treatment of the patient, maintenance of adequate records, compilation of treatment data, aftercare planning, or evaluation of programs.

For the purpose of determining whether a person meets the criteria for involuntary outpatient placement or for preparing the proposed treatment plan pursuant to s. 394.4655, the clinical record may be released to the state attorney, the public defender or the patient's private legal counsel, the court, and to the

appropriate mental health professionals, including the service provider identified in s. 394.4655(7)(b)2., in accordance with state and federal law.

(4) Information from the clinical record must be released when a patient has communicated to a service provider a specific threat to cause serious bodily injury or death to an identified or a readily available person, if the service provider reasonably believes, or should reasonably believe according to the standards of his or her profession, that the patient has the apparent intent and ability to imminently or immediately carry out such threat. When such communication has been made, the administrator must authorize the release of sufficient information to communicate the threat to law enforcement. A law enforcement agency that receives notification of a specific threat under this subsection must take appropriate action to prevent the risk of harm, including, but not limited to, notifying the intended victim of such threat or initiating a risk protection order. A service provider's authorization to release information from a clinical record when communicating a threat pursuant to this section may not be the basis of any legal action or criminal or civil liability against the service provider.

(5) Information from clinical records may be used for statistical and research purposes if the information is abstracted in such a way as to protect the identity of individuals.

(6) Information from clinical records may be used by the Agency for Health Care Administration, the department, and the Florida advocacy councils for the purpose of monitoring facility activity and complaints concerning facilities.

(7) Clinical records relating to a Medicaid recipient shall be furnished to the Medicaid Fraud Control Unit in the Department of Legal Affairs, upon request.

(8) Any person, agency, or entity receiving information pursuant to this section shall maintain such information as confidential and exempt from the provisions of s. 119.07(1).

(9) Any facility or private mental health practitioner who acts in good faith in releasing information pursuant to this section is not subject to civil or criminal liability for such release.

(10) Nothing in this section is intended to prohibit the parent or next of kin of a person who is held in or treated under a mental health facility or program from requesting and receiving information limited to a summary of that person's treatment plan and current physical and mental condition. Release of such information shall be in accordance with the code of ethics of the profession involved.

(11) Patients shall have reasonable access to their clinical records, unless such access is determined by the patient's physician to be harmful to the patient. If the patient's right to inspect his or her clinical record is restricted by the facility, written notice of such restriction shall be given to the patient and the patient's guardian, guardian advocate, attorney, and representative. In addition, the restriction shall be recorded in the clinical record, together with the reasons for it. The restriction of a patient's right to inspect his or her clinical record shall expire after 7 days but may be renewed, after review, for subsequent 7-day periods.

(12) Any person who fraudulently alters, defaces, or falsifies the clinical record of any person receiving mental health services in a facility subject to this part, or causes or procures any of these offenses to be committed, commits a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083.

History.—s. 14, ch. 96-169; s. 98, ch. 99-8; s. 1, ch. 2000-163; s. 14, ch. 2000-263; s. 4, ch. 2004-385; s. 83, ch. 2014-19; s. 8, ch. 2016-127; s. 89, ch. 2016-241; s. 1, ch. 2019-134; s. 5, ch. 2022-36.

CHAPTER 2009-172

Committee Substitute for
Committee Substitute for Senate Bill No. 162

An act relating to electronic health records; amending s. 395.3025, F.S.; expanding access to a patient's health records in order to facilitate the exchange of data between certain health care facility personnel, practitioners, and providers and attending physicians; deleting the exemption that allows long-term ombudsman councils to have access to certain nursing home patient records; creating s. 408.051, F.S.; creating the "Florida Electronic Health Records Exchange Act"; providing definitions; authorizing the release of certain health records under emergency medical conditions without the consent of the patient or the patient representative; providing for immunity from civil liability; providing duties of the Agency for Health Care Administration with regard to the availability of specified information on the agency's Internet website; requiring the agency to develop and implement a universal patient authorization form in paper and electronic formats for the release of certain health records; providing procedures for use of the form; providing penalties; providing for certain compensation and attorney's fees and costs; creating s. 408.0512, F.S.; requiring the Agency for Health Care Administration to operate an electronic health record technology loan fund, subject to a specific appropriation; requiring the agency to adopt rules related to standard terms and conditions for the loan program; amending s. 409.916, F.S.; requiring that the agency deposit into the Grants and Donations Trust Fund private donations provided for the purpose of funding a certified electronic health record technology loan fund; amending s. 483.181, F.S.; expanding access to laboratory reports in order to facilitate the exchange of data between certain health care practitioners and providers; providing an effective date.

WHEREAS, the use of electronic health information technology has been proven to benefit consumers by increasing the quality and efficiency of health care delivery throughout the state, and

WHEREAS, clear and concise standards for sharing privacy-protected medical information among authorized health care providers will enable providers to have cost-effective access to the medical information needed to make sound decisions about health care, and

WHEREAS, maintaining the privacy and security of identifiable health records is essential to the adoption of procedures for sharing of electronic health records among health care providers involved in the treatment of patients, NOW, THEREFORE,

Be It Enacted by the Legislature of the State of Florida:

Section 1. Subsection (4) of section 395.3025, Florida Statutes, is amended to read:

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

395.3025 Patient and personnel records; copies; examination.—

(4) Patient records are confidential and must not be disclosed without the consent of the patient or his or her legal representative ~~person to whom they pertain~~, but appropriate disclosure may be made without such consent to:

(a) Licensed facility personnel, ~~and~~ attending physicians, or other health care practitioners and providers currently involved in the care or treatment of the patient for use only in connection with the treatment of the patient.

(b) Licensed facility personnel only for administrative purposes or risk management and quality assurance functions.

(c) The agency, for purposes of health care cost containment.

(d) In any civil or criminal action, unless otherwise prohibited by law, upon the issuance of a subpoena from a court of competent jurisdiction and proper notice by the party seeking such records to the patient or his or her legal representative.

(e) The agency upon subpoena issued pursuant to s. 456.071, but the records obtained thereby must be used solely for the purpose of the agency and the appropriate professional board in its investigation, prosecution, and appeal of disciplinary proceedings. If the agency requests copies of the records, the facility shall charge no more than its actual copying costs, including reasonable staff time. The records must be sealed and must not be available to the public pursuant to s. 119.07(1) or any other statute providing access to records, nor may they be available to the public as part of the record of investigation for and prosecution in disciplinary proceedings made available to the public by the agency or the appropriate regulatory board. However, the agency must make available, upon written request by a practitioner against whom probable cause has been found, any such records that form the basis of the determination of probable cause.

(f) The Department of Health or its agent, for the purpose of establishing and maintaining a trauma registry and for the purpose of ensuring that hospitals and trauma centers are in compliance with the standards and rules established under ss. 395.401, 395.4015, 395.4025, 395.404, 395.4045, and 395.405, and for the purpose of monitoring patient outcome at hospitals and trauma centers that provide trauma care services.

(g) The Department of Children and Family Services or its agent, for the purpose of investigations of cases of abuse, neglect, or exploitation of children or vulnerable adults.

~~(h) The State Long-Term Care Ombudsman Council and the local long-term care ombudsman councils, with respect to the records of a patient who has been admitted from a nursing home or long-term care facility, when the councils are conducting an investigation involving the patient as authorized under part II of chapter 400, upon presentation of identification as a council member by the person making the request. Disclosure under this paragraph shall only be made after a competent patient or the patient's representative has been advised that disclosure may be made and the patient has not objected.~~

(h)~~(i)~~ A local trauma agency or a regional trauma agency that performs quality assurance activities, ~~or~~ a panel or committee assembled to assist a local trauma agency, or a regional trauma agency ~~in~~ performing quality assurance activities. Patient records obtained under this paragraph are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

(i)~~(j)~~ Organ procurement organizations, tissue banks, and eye banks required to conduct death records reviews pursuant to s. 395.2050.

(j)~~(k)~~ The Medicaid Fraud Control Unit in the Department of Legal Affairs pursuant to s. 409.920.

(k)~~(l)~~ The Department of Financial Services, or an agent, employee, or independent contractor of the department who is auditing for unclaimed property pursuant to chapter 717.

(l)~~(m)~~ A regional poison control center for purposes of treating a poison episode under evaluation, case management of poison cases, or compliance with data collection and reporting requirements of s. 395.1027 and the professional organization that certifies poison control centers in accordance with federal law.

Section 2. Section 408.051, Florida Statutes, is created to read:

408.051 Florida Electronic Health Records Exchange Act.—

(1) SHORT TITLE.—This section may be cited as the "Florida Electronic Health Records Exchange Act."

(2) DEFINITIONS.—As used in this section, the term:

(a) "Electronic health record" means a record of a person's medical treatment which is created by a licensed health care provider and stored in an interoperable and accessible digital format.

(b) "Qualified electronic health record" means an electronic record of health-related information concerning an individual which includes patient demographic and clinical health information, such as medical history and problem lists, and which has the capacity to provide clinical decision support, to support physician order entry, to capture and query information relevant to health care quality, and to exchange electronic health information with, and integrate such information from, other sources.

(c) "Certified electronic health record technology" means a qualified electronic health record that is certified pursuant to s. 3001(c)(5) of the Public Health Service Act as meeting standards adopted under s. 3004 of such act which are applicable to the type of record involved, such as an ambulatory electronic health record for office-based physicians or an inpatient hospital electronic health record for hospitals.

(d) "Health record" means any information, recorded in any form or medium, which relates to the past, present, or future health of an individual for the primary purpose of providing health care and health-related services.

(e) "Identifiable health record" means any health record that identifies the patient or with respect to which there is a reasonable basis to believe the information can be used to identify the patient.

(f) "Patient" means an individual who has sought, is seeking, is undergoing, or has undergone care or treatment in a health care facility or by a health care provider.

(g) "Patient representative" means a parent of a minor patient, a court-appointed guardian for the patient, a health care surrogate, or a person holding a power of attorney or notarized consent appropriately executed by the patient granting permission to a health care facility or health care provider to disclose the patient's health care information to that person. In the case of a deceased patient, the term also means the personal representative of the estate of the deceased patient; the deceased patient's surviving spouse, surviving parent, or surviving adult child; the parent or guardian of a surviving minor child of the deceased patient; the attorney for the patient's surviving spouse, parent, or adult child; or the attorney for the parent or guardian of a surviving minor child.

(3) EMERGENCY RELEASE OF IDENTIFIABLE HEALTH RECORD.—A health care provider may release or access an identifiable health record of a patient without the patient's consent for use in the treatment of the patient for an emergency medical condition, as defined in s. 395.002(8), when the health care provider is unable to obtain the patient's consent or the consent of the patient representative due to the patient's condition or the nature of the situation requiring immediate medical attention. A health care provider who in good faith releases or accesses an identifiable health record of a patient in any form or medium under this subsection is immune from civil liability for accessing or releasing an identifiable health record.

(4) UNIVERSAL PATIENT AUTHORIZATION FORM.—

(a) By July 1, 2010, the agency shall develop forms in both paper and electronic formats which may be used by a health care provider to document patient authorization for the use or release, in any form or medium, of an identifiable health record.

(b) The agency shall adopt by rule the authorization form and accompanying instructions and make the authorization form available on the agency's website, pursuant to s. 408.05.

(c) A health care provider receiving an authorization form containing a request for the release of an identifiable health record shall accept the form as a valid authorization to release an identifiable health record. A health care provider may elect to accept the authorization form in either electronic or paper format or both. The individual or entity that submits the authorization form containing a request for the release of an identifiable health record shall determine which format is accepted by the health care provider prior to submitting the form.

(d) An individual or entity that submits a request for an identifiable health record is not required under this section to use the authorization form adopted and distributed by the agency.

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

(e) The exchange by a health care provider of an identifiable health record upon receipt of an authorization form completed and submitted in accordance with agency instructions creates a rebuttable presumption that the release of the identifiable health record was appropriate. A health care provider that releases an identifiable health record in reliance on the information provided to the health care provider on a properly completed authorization form does not violate any right of confidentiality and is immune from civil liability for accessing or releasing an identifiable health record under this subsection.

(f) A health care provider that exchanges an identifiable health record upon receipt of an authorization form shall not be deemed to have violated or waived any privilege protected under the statutory or common law of this state.

(5) PENALTIES.—A person who does any of the following may be liable to the patient or a health care provider that has released an identifiable health record in reliance on an authorization form presented to the health care provider by the person for compensatory damages caused by an unauthorized release, plus reasonable attorney's fees and costs:

(a) Forges a signature on an authorization form or materially alters the authorization form of another person without the person's authorization; or

(b) Obtains an authorization form or an identifiable health record of another person under false pretenses.

Section 3. Section 408.0512, Florida Statutes, is created to read:

408.0512 Electronic health records system adoption loan program.—

(1) Subject to the availability of eligible donations from public or private entities and funding made available through s. 3014 of the Public Health Service Act, the agency may operate a certified electronic health record technology loan fund subject to a specific appropriation as authorized by the General Appropriations Act or as provided through the provisions of s. 216.181(11)(a) and (b).

(2) The agency shall adopt rules related to standard terms and conditions for use in the loan program.

Section 4. Subsection (1) of section 409.916, Florida Statutes, is amended to read:

409.916 Grants and Donations Trust Fund.—

(1) The agency shall deposit any funds received from pharmaceutical manufacturers and all other funds received by the agency from any other person as the result of a Medicaid cost containment strategy, in the nature of a rebate, grant, or other similar mechanism into the Grants and Donations Trust Fund. The agency shall deposit any funds received from private donations for the purpose of funding a certified electronic health record technology loan fund into the Grants and Donations Trust Fund.

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

Section 5. Subsection (2) of section 483.181, Florida Statutes, is amended to read:

483.181 Acceptance, collection, identification, and examination of specimens.—

(2) The results of a test must be reported directly to the licensed practitioner or other authorized person who requested it, and appropriate disclosure may be made by the clinical laboratory without a patient's consent to other health care practitioners and providers involved in the care or treatment of the patient as specified in s. 456.057(7)(a). The report must include the name and address of the clinical laboratory in which the test was actually performed, unless the test was performed in a hospital laboratory and the report becomes an integral part of the hospital record.

Section 6. This act shall take effect upon becoming a law.

Approved by the Governor June 16, 2009.

Filed in Office Secretary of State June 16, 2009.

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

Meeting Dates for 2024

HIECC Meeting Dates for 2024

- February 14, 2024
- May 08, 2024
- August 08, 2024
- November 13, 2024

Public Comments

Meeting Summary

Next Steps

Adjournment