

Virtual Service Delivery During COVID-19

Guidance on Federal Privacy Laws for Behavioral
Health Practitioners and Peer Support Specialists



**CoE-PHI Presentation to the
Mountain Plains ATTC (Region 8)
*July 29th, 2020: 1:00 PM MT***



Center of Excellence for Protected Health Information

Funded by SAMHSA, the CoE-PHI develops and disseminates resources, training, and TA for states, healthcare providers, school administrators and individuals and families to improve understanding and application of federal privacy laws and regulations, **including FERPA, HIPAA, and 42 CFR Part 2**, when providing and receiving treatment for SUD and mental illness.

Resources, training, technical assistance, and any other information provided through the CoE-PHI do not constitute legal advice.



Presenters

Name	Title
Christine Khaikin, JD	CoE-PHI Health Privacy Associate
Caroline Waterman, MA, LRC, CRC	CoE-PHI SUD Project Lead
Jacqueline Seitz, JD	CoE-PHI Health Privacy Lead
Michael Graziano, MPA	CoE-PHI Project Director



Presentation Objectives

**Identify basic requirements of
42 CFR Part 2 and HIPAA**

**Cite at least two ways privacy laws apply
to telehealth in accordance with recently
released SAMHSA and OCR guidance**

**Explore recent changes to federal
privacy laws outlined in the CARES Act
and recent Part 2 amendments**

**Describe how to access resources and
TA provided by the CoE-PHI**



OVERVIEW

FEDERAL PRIVACY LAWS



HIPAA

Applies to covered entities (healthcare providers, health plans, healthcare clearinghouses) and BAs

- Protects privacy and security of general health information

Purpose: to protect health data integrity, confidentiality, and accessibility

Permits disclosures without patient consent for treatment, payment, and healthcare operations

42 CFR Part 2

Applies to SUD patient records from federally-assisted “Part 2 programs”

- Protects privacy and security of records identifying individual as seeking/receiving SUD treatment

Purpose: to encourage people to enter and remain in SUD treatment by guaranteeing confidentiality

Requires patient consent for treatment, payment, and healthcare operations, with limited exceptions



Case Study #1

- Ana is a nurse in a federally qualified health center (FQHC).
- Her patient needs a referral to a specialist in another practice area of the FQHC.

Q: Does Ana need to obtain the patient's written consent before making the referral?



Poll Question #1

Based on the previous case study example, *does Ana need to obtain the patient's written consent before making the referral??*

- Yes
- No
- It depends...



Case Study #1 (Answer)

A: It depends on whether Ana works in an SUD treatment unit

- If Ana works in an SUD treatment unit that meets the definition of a Part 2 program, *she needs patient consent to make the disclosure.*
- If Ana does NOT work in an SUD treatment unit, she may make the referral without written consent because HIPAA* permits disclosures for “treatment”.

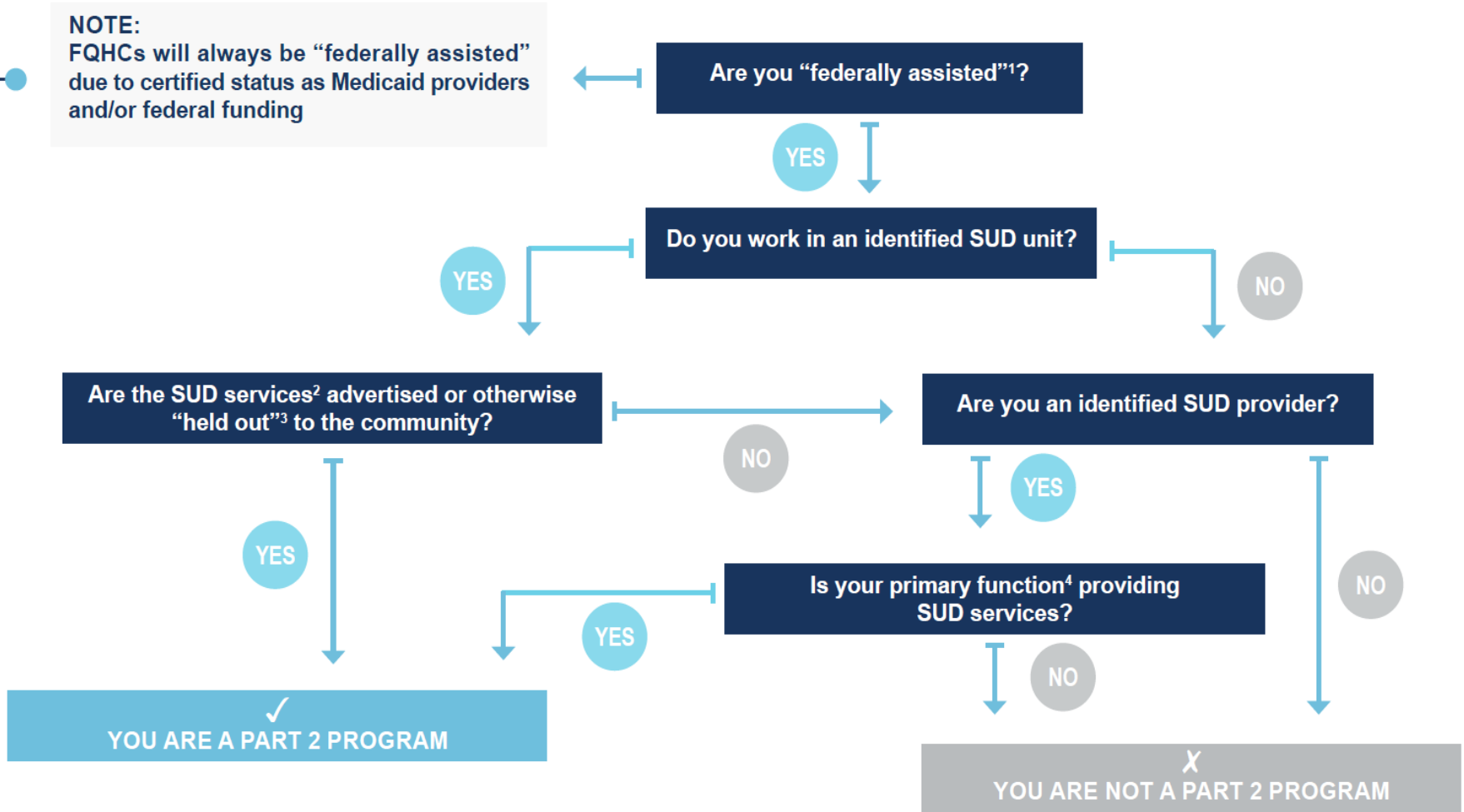
**Other privacy laws may also apply, in which case Ana should follow whichever law is most protective of privacy*

I Provide SUD Services in an FQHC: Does Part 2 Apply to Me?

Use the flowchart below to determine if Part 2 applies to you

NOTE:

FQHCs will always be “federally assisted” due to certified status as Medicaid providers and/or federal funding



For more information & resources, or to request technical assistance, please visit coephi.org.

Resources, training, technical assistance, and any other information provided through the Center of Excellence for Protected Health Information do not constitute legal advice. For legal advice, including legal advice on other applicable state and federal laws, please seek out local counsel.



Case Study #2

- Owen is a CASAC at a Part 2 program.
- He has a new patient joining a group session and wants to know more information about the patient's diagnosis and treatment history.

Q: Can Owen look at the patient's treatment record? Can he speak with his colleague about the patient?



Poll Question #2

Can Owen look at the patient's treatment record? Can he speak with his colleague about the patient?

- Yes, because he needs the information in order to provide SUD treatment to the patient.
- Yes, because he has access to the EHR system and the colleague is also his friend.
- No, because he has not met the patient yet.
- He can speak with his colleague, but not look in the patient record.



Case Study #2 (Answer)

A: Yes, Owen can access the patient's treatment record and speak with a colleague about the patient.

- Owen needs this information in order to provide SUD services to the patient.



Internal Communications

The “need to know” rule:

- You may share and receive patient information within your Part 2 program, *if necessary, to provide SUD services to the patient*
- Information should be limited to the ***minimum necessary***



Internal Communications

**For Part 2 programs within a larger entity –
(like an FQHC or Community Health Center)**

- The Part 2 program may share patient information *for administrative purposes* with the larger entity (e.g., billing)
- Disclosures for *treatment* purposes (e.g., with a primary care practitioner) - **still need consent**

Case Study #3



- Mario is a nurse at an opioid treatment program (OTP).
- One morning, a patient suddenly collapses to the floor and loses consciousness.
- Paramedics arrive and ask Mario a few questions about the pt.

Q: Can Mario share patient information with the paramedics?



Poll Question #3

Can Mario share patient information with the paramedics?

- Yes, because it is a medical emergency.
- Yes, but Mario can't share anything about the patient's substance use disorder.
- Yes, because HIPAA permits disclosures for "treatment" purposes.
- No, because Part 2 requires written patient consent.



Case Study #3 (Answer)

A: Yes, Mario can share patient information with the paramedics.

- If necessary, to help the paramedics address the medical emergency, Mario can share SUD information, as well as basic information like the patient's name, age, date of birth, and emergency contacts.



Medical Emergency

- You may share information with *medical personnel* in order to meet a medical emergency in which patient's prior consent could not be obtained
 - If patient has capacity to consent and chooses not to authorize the disclosure, *you may not use the medical emergency exception*



Medical Emergency

- The Part 2 program needs to ***document*** the disclosure in the patient's record:
 - Name of the medical personnel and their affiliation with a healthcare facility
 - Name of individual making the disclosure
 - Date and time of disclosure
 - Nature of the emergency



Case Study #4

- Annabelle is a receptionist at a Part 2 program.
- Four police officers arrive at the program to investigate a series of burglaries in the area.
- The officers ask for a list of the patients, so they can run background checks.

Q: Can Annabelle give the officers the list of patient names?



Poll Question #4

Can Annabelle give the officers the list of patient names?

- Yes, because they are investigating an ongoing crime.
- Yes, because they are the police.
- No, because they don't have a warrant.
- No, because they don't have a court order signed by a judge.



Case Study #4 (Answer)

A: No, Annabelle cannot give the officers the list of patient names unless there is a court order authorizing the disclosure.

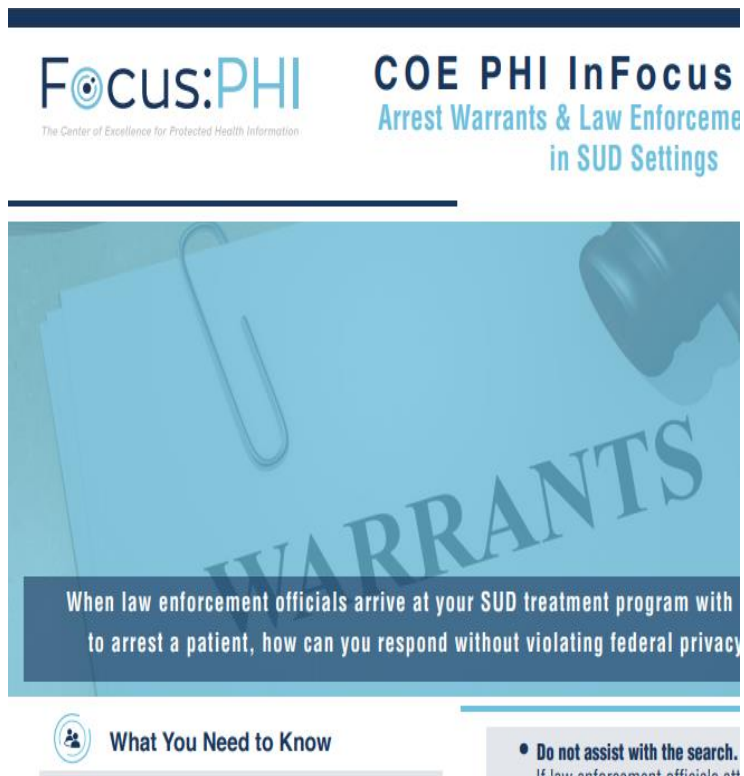
- Even a warrant is *not enough* to authorize disclosure of Part 2 records



Law Enforcement

- Part 2 strictly protects the confidentiality of treatment records from law enforcement
- Disclosures only permissible if:
 - Court order authorizes the disclosure
 - Patient consents to disclosure
 - Program is reporting a crime on program premises, or against program personnel

Law Enforcement



Focus:PHI
The Center of Excellence for Protected Health Information

COE PHI InFocus
Arrest Warrants & Law Enforcement
in SUD Settings

When law enforcement officials arrive at your SUD treatment program with to arrest a patient, how can you respond without violating federal privacy

What You Need to Know

- Do not assist with the search.
If law enforcement officials att

- Even though Part 2 has strict confidentiality protections, *it does not require you to get arrested!*
 - When responding to police inquiries, it can be helpful to:
 - Have a supervisor or colleague present
 - Show the officers a copy of the law and the
- [CoE-PHI resource on warrants](#)



OVERVIEW

CHANGES TO PART 2



Changes to the Law and Regulations

Statute 42 USC § 290dd-2	Regulations 42 CFR Part 2
<p>March 27, 2020 – Congress amended statute, required new regulations</p>	<p>July 15, 2020 – SAMHSA amended regulations – <i>transitional only</i></p>
<p>Effective: March 27, 2021</p>	<p>Effective: August 14, 2020</p>



Timeline

Aug. 2019: Proposed Rule (SAMHSA)

Fall 2019: Public Comments

March 2020: CARES Act (Congress)

July 2020: Final Rule (SAMHSA)

Before March 2021: New rulemaking implementing CARES Act (SAMHSA)



Changes to Part 2 (July 2020)

42 CFR §	Provision
2.11	Definition of “records”
2.12	Applicability and re-disclosure
2.31	Requirements for written consent forms
2.32	Notice of prohibition on re-disclosure
2.33	Disclosures permitted with written consent (P/HCO)
2.34	Disclosures by central registries
2.36	Disclosures to prescription drug monitoring programs
2.51	Medical emergencies
2.52	Research
2.53	Audit and evaluation
2.67	Court orders for undercover agents and informants
Guidance	Disposition of records on employees’ personal devices, data segmentation



Review (Main Points)

- July 2020 Final Rule changed requirements for consent forms and made some changes to the ways information can be shared without patient consent
 - Effective date: August 14, 2020
- Overall framework didn't change
- July 2020 Final Rule is ***transitional*** –
CARES Act means more changes



Key Steps to Implement Changes

for August 14, 2020

- **Update Prohibition on Re-Disclosure Notice**
 - New language can be found [here](#)
- **Optional:** Consent forms – update “recipient” description to permit naming entity



Key Steps to Implement Changes (2)

for August 14, 2020

- **For opioid treatment programs (OTPs):**
 - Check state law requirements for Central Registry and PDMPs and **update consent forms as needed**
- **Revise/develop policies and procedures for all other changes.**
 - Resources available at coephi.org
- **Train staff and educate clients about all changes.**



Changes in the CARES Act

- Still requires initial patient consent to disclose protected SUD records
- After initial consent, some re-disclosures permitted:
 - For treatment/payment/healthcare operations (“TPO”) by HIPAA covered entities, business associates, and Part 2 programs
 - Patient still has right to revoke initial consent



Poll Question #5

True or False: The CARES ACT repealed 42 CFR Part 2.

- True
- False
- Not Sure



Poll Question #5 Answer

False: The CARES Act makes some *changes* to the SUD privacy law, and will require future changes to the Part 2 regulations.

- The CARES Act goes into effect March 27, 2021.
- The CARES Act does not repeal the SUD privacy law or regulations.



PHI regulations protect patient privacy, give you flexibility to provide the best possible treatment, and help clarify the boundaries in protecting and sharing patient information.

COVID-19 AND TELEHEALTH



Poll Question #6

What methods are you currently (or considering) using to provide telehealth services? (please choose all that apply)

- HIPAA-compliant video communications (e.g.; Skype for Business, Updox, Zoom Health, WebEx, GoTo Meeting)**
- Other video communications (e.g.; Apple FaceTime, Facebook Messenger video, Google Hangouts, Zoom, Skype)**
- Encrypted text messaging**
- Phone calls**
- other**



Privacy Considerations for Telehealth During COVID-19

- How do privacy laws apply?
- How to protect privacy and security at:
 - Provider's location
 - Patient's location



HIPAA

Applies to covered entities (healthcare providers, health plans, healthcare clearinghouses) and BAs

- Protects privacy and security of general health information

Purpose: to protect health data integrity, confidentiality, and accessibility

Permits disclosures without patient consent for treatment, payment, and healthcare operations

42 CFR Part 2

Applies to SUD patient records from federally-assisted “Part 2 programs”

- Protects privacy and security of records identifying individual as seeking/receiving SUD treatment

Purpose: to encourage people to enter and remain in SUD treatment by guaranteeing confidentiality

Requires patient consent for treatment, payment, and healthcare operations, with limited exceptions



OCR GUIDANCE AND HIPAA



OCR Bulletin: COVID-19

OCR announced it will waive potential penalties for HIPAA violations arising out of *good-faith use of telehealth*:

- Providers may use popular video chats, like FaceTime, Messenger, Google Hangouts, Zoom, or Skype
- Providers do not need to have a BAA in place
- *Does not matter whether telehealth service is directly related to COVID-19*

Still *best practice* to use secure, HIPAA compliant services and have BAA in place



OCR Bulletin: COVID-19

OCR's enforcement discretion will end when there is no longer a *national emergency*

- OCR is not the only entity that *enforces* HIPAA violations
- **Check with your state's Attorney General** to see if they have guidance about HIPAA compliance for telehealth during COVID-19



SAMHSA GUIDANCE AND PART 2



Quick Review: Medical Emergencies

42 CFR § 2.51

Part 2 permits disclosures w/o written consent to medical personnel in order to treat a

bona fide medical emergency

- Information may be re-disclosed for treatment purposes
- Cannot use this provision to “override” patient’s objection to a disclosure
- **Part 2 program must make note in patient file regarding disclosure**



SAMHSA Guidance: COVID-19

SAMHSA's COVID-19 Part 2 Guidance

emphasizes that providers have discretion to determine whether *bona fide* medical emergency exists



Key Points

SAMHSA has not eliminated Part 2's requirements for written consent to share information

As before - no consent is required in a medical emergency, but SAMHSA has emphasized that providers may determine COVID-19 may meet the requirements

E-signatures and photocopied signatures are okay!



Focus:PHI TIPS
The Center of Excellence for Protected Health Information

**TELEHEALTH AND PRIVACY:
Federal Guidance for SUD and
Mental Health Treatment Providers**

Providers of SUD and mental health services are working rapidly to make sure their patients have access to the care they need during the COVID-19 pandemic. This includes working to recreate the treatment experience in a virtual setting through telehealth. As part of this rapid transition providers are concerned about maintaining patient privacy when sharing protected health information in accordance with federal health privacy laws.


HERE IS WHAT YOU NEED TO KEEP IN MIND:

- You Should Still Take Action to Protect Client Confidential Information**
 - Telehealth may increase the number of people and systems with access to confidential health information. Providers should try to avoid public wi-fi, password protect their devices, and keep any confidential files secure.
- You Can Use Widely Available Apps to Support Service Delivery**
 - OCR announced that it will waive potential penalties for violations arising out of good faith use of telehealth. Providers can use widely available private facing apps such as Zoom, FaceTime, or Skype, even without a BAA in place. The OCR announcement includes a comprehensive list of telehealth options providers can use.
- Key Points for Part 2 Consent Forms**
 - In-person consent for sharing protected health information is not needed
 - Part 2 allows e-signatures on consent forms, as long as state law permits.
 - Providers should obtain consent from the patient to disclose to the telehealth service if it will have access to patient information.
 - Consent is needed for disclosures of patient-identifying information to payers and other non-medical third parties and must be accompanied by a [notice prohibiting re-disclosure](#).
- You Can Share Patient Information for Treatment Purposes When a Medical Emergency Exists**
 - Part 2's current exception for medical emergencies already permits the disclosure, or sharing, of patient identifying information for treatment purposes without a consent form¹ when a medical emergency exists.²
 - SAMHSA's [recent guidance](#) emphasizes that providers can make their own determinations whether a "medical emergency" exists.
 - Any disclosures must be documented in the patient record
 - Providers should remember that disclosures made under this exception do not continue to have Part 2 protections.

1. AKA authorization or Release of Information (ROI)
2. 42 CFR §2.51

Funded by Substance Abuse and Mental Health Services Administration
Resources, training, technical assistance, and any other information provided through the CoE-PHI do not constitute legal advice.

[Link to Provider TH Tips](#)



Focus:PHI TIPS
The Center of Excellence for Protected Health Information

TO KEEP YOUR TELEHEALTH VISIT PRIVATE

Seek Treatment and Support with Confidence
Understand your rights and responsibilities for protecting your personal health information.

PRIVACY IS IMPORTANT!
There are a few steps you can take to maintain your privacy when receiving mental health or substance use disorder services through telehealth.

PROTECT YOUR COMMUNICATIONS:

- ✓ If your provider gives you a choice between video apps (for example: Zoom, WhatsApp, or Facebook Messenger), use the most private option available.
 - If you're not sure, ask your provider.
 - Do NOT use apps like TikTok, Twitch, or Facebook Live, where posts can be viewed by more people.
- ✓ Make sure you adjust your privacy settings for the telehealth app (for example: turn on encryption and turn off location services).
- ✓ If you have to use someone else's device to receive treatment and you don't want them to have access to your treatment information, you should:
 - Inform your treatment provider that it is NOT your device so they don't send confidential treatment information to the device.
 - After using another's device, delete any history of communication about your treatment from the device. You can also set the device's browser to "Incognito" mode to prevent it from storing history.


PREPARE YOUR SURROUNDINGS:

- ✓ Make sure your roommates, friends, or family can't overhear you during a confidential telehealth session with your provider.
- ✓ Use headphones and find a quiet, private space for your visit to help protect your privacy.
- ✓ Use a "Safe Word" with your provider to alert them when someone enters your private space, so that private information isn't shared in their presence.
- ✓ Think about the privacy of others if participating in group telehealth sessions. Be aware that people in your surroundings may overhear other patients and take steps to protect their confidentiality.

PROTECT YOUR DEVICE (PHONE, TABLET, COMPUTER):

- ✓ Make sure your device is password protected.
- ✓ If using wireless internet, make sure your wi-fi is password protected and avoid using public wi-fi.
- ✓ Who else knows your password? If others know your password and you don't want them to have access to your treatment information, you may consider changing it now.

Funded by Substance Abuse and Mental Health Services Administration
Resources, training, technical assistance, and any other information provided through the CoE-PHI do not constitute legal advice.



[Link to Client TH Tips](#)

CoE-PHI Telehealth Resources

[Video - Tips to Keep Your Telehealth Visit Private](#)



Questions and Discusssion

*Please share with us any
questions that you have now*



Accessing the CoE-PHI

Request TA

coephi.org/technical-assistance

Resource Library

coephi.org/resource-center

Discussing privacy protections helps the care team to provide the best possible care.

The screenshot shows the Focus:PHI website interface. At the top, the Focus:PHI logo and tagline are displayed. Below the logo is a navigation menu with the following items: PROJECT OVERVIEW, WHO IS INVOLVED IN THE INITIATIVE? (with a dropdown arrow), CORE PROJECT STAFF, NATIONAL ADVISORY GROUP MEMBERS, HOW WILL WE KNOW WE ARE SUCCESSFUL?, REQUEST TA, RESOURCE CENTER, and CONTACT US. A prominent blue button labeled 'Join Our Mailing List' with a 'click here' link is also visible. The main content area is titled 'REQUEST TA' and contains the following text: 'Please use the form to request Technical Assistance.' The form fields include: Name, Role/Job Title, Organization Name, Organization Type (with a dropdown menu), Affiliation (with a dropdown menu), State/Territory (with a dropdown menu), Zip Code, Contact Phone Number, Email (with an asterisk), and Your Question (with a text area). At the bottom of the form, there is a question 'Is your question urgent?' with radio buttons for 'No' and 'Yes'.



Webinar Evaluation

Following the conclusion of this webinar, you will be sent a link to complete a brief evaluation.

We value your opinion- please take the time to complete our evaluation!



THANK YOU!