MTSS-B data sharing and consent considerations

Given that data are central to MTSS-B, so are considerations about their use and security. Effective MTSS-B implementation includes local district policies that establish practices for student data sharing/privacy and informed parent/guardian consent for supports and services.

The information provided in this document should not be relied upon or construed as legal advice. Districts and schools should seek the opinion of local district legal counsel when creating data privacy and security policies and consent procedures. The NH MTSS-B TA Center does not directly advise districts and schools on interpreting state laws or ethics codes related to student privacy, sharing of student data, and/or consent for tiered social-emotional, behavioral or mental health supports and services in schools.

Define your service array

School counseling in NH is considered to be part of a school's general education program (see NH State Board of Education's Ed 306.39). Some schools also employ social workers, clinical mental health counselors, and/or contract with co-located community-based providers to deliver portions of their tiered supports and services. Districts should first establish clear definitions and categorizations of supports and services across tiers in order to understand what is available to students, and which professionals are responsible for monitoring the intervention.

Consent for supports and services

Once supports and services are well defined and categorized, districts should establish clear policies for supports and services that require parent/guardian consent. When partnering with a community agency that has its own procedure for obtaining parent/guardian consent, districts should also establish a consent process for co-located services in their own policies.

Districts should also consider statutes (e.g., NH RSA 135-C) regarding the age at which a minor may be able to consent on their own behalf for mental health and/or substance-related treatment (e.g., mental health emergencies, minors age 12 or older for problems related to the use of drugs, etc.) when developing their local policies.

Communication and confidentiality

Districts and partnering community mental health agencies providing services in schools should establish communication and confidentiality protocols that ensure adherence to HIPAA, FERPA, and all applicable ethical guidelines.

HIPAA vs. FERPA

Districts should become well-versed, with the help of legal counsel, in how FERPA and HIPAA interact in a school setting. FERPA applies to students' educational records, while HIPAA applies to electronic healthcare transactions (e.g., billing mental health services under Medicaid to Schools). More information about application of FERPA and HIPAA can be found in the U.S. Department of Education's Joint Guidance on the Application of FERPA and HIPAA to Student Health Records.

Sharing information between school staff

Under FERPA, school staff are generally able to share information and data about student needs and progress to support team-based coordination of care. Districts/schools should be explicit in their policies about the circumstances under which such information sharing is appropriate (e.g., on a need to-know basis, only between certain staff/teams, etc.) and consult FERPA guidelines and legal counsel to ensure compliance.

Sharing information between school- and co-located community mental health providers

To ensure high-quality care coordination, co-located community mental health clinicians (who typically fall under HIPAA) can seek parent/guardian consent to share information about a student with relevant teachers and school staff. Community mental health agency release of information forms will specify the types of information that can be shared and with whom. Districts and community mental health agencies' service contracts should establish clear policies and procedures for sharing of student information.

Sharing information with other external entities

In some cases, a district may be asked to share student-level data for other purposes. This data may be sensitive and/or contain personally identifying information (PII). FERPA does allow for disclosure of student information to particular outside agencies without parent/guardian consent in specific circumstances, when the external entity is recognized by the district/school as their authorized agent. Some examples include, but are not limited to:

- ✓ Sharing student information with school officials who have a legitimate educational interest. School officials include other school employees such as teachers, school nurses, and counselors. It can also include consultants, volunteers, contractors, or other outside parties that provide a service for the district/school;
- ✓ Sharing student information, pursuant to a written agreement, to public health agencies, mental health agencies, and other organizations to evaluate and improve health education programs and health accommodations in schools;
- ✓ Entering into an agreement that designates a public health agency or community mental health or other organization to serve as its authorized representative; e.g., a district might designate a community mental health agency or other organization as its authorized agent to evaluate how well the district is meeting the mental and behavioral health needs of its students.

Districts should establish a data privacy agreement (DPA) or a business associate agreement (BAA) with any outside entity serving in a data collection/evaluation/audit (or similar) role in their schools in order to designate that entity as an authorized agent of the district/school. This agreement should establish the purposes and boundaries of student data collection and include the types of data that will be collected, how student data will be stored and student privacy protected, who can access the data, how the data will be used and reported, and plans for destruction of data at the completion of a project. The DPA/BAA allows for sharing of student information within the bounds of the agreement. Districts/schools will then need to determine how they will inform parents about student data sharing with the external entity, and options for opting-out of data collection or other relevant activities if desired.

Data security

As with all sensitive and PII data, district privacy guidelines and protections should be followed at all times. Districts should implement and enforce policies and procedures that are reasonably designed to protect the security, privacy, confidentiality, and integrity of student data against risks. Some recommended best practices to support data privacy and security are described below.

Laptop/work area

Before leaving your work area, secure your computer (log off/lock); protect PII from the eyes of passersby (e.g., orient your screen or use a privacy screen). Regularly delete the contents of your downloads folder and empty your desktop recycling bin. Make sure there are no paper records displaying PII around your work area and lock any paper records in a file cabinet when you leave your work area.

Email and cell phone

Refrain from using student/family names in emails to external agencies/individuals, emailing documents containing PII, and taking personally identifying photos of students/families on your phone.

Passwords

Refrain from sharing your passwords with other people and using the "remember password" feature in your web browser. Update your password if your account may have been compromised. Keep passwords in a secured place (locked drawer or encrypted electronic file).

Social media

Refrain from contributing content or images about or related to any student or family member on social media.

Wireless networks

Only use secure password-protected networks. Do not view PII at public settings such as cafés or over other public wireless networks.