TELEHEALTH IN SCHOOLS
BLUEPRINT 2.0

BroadbandOhio
INNOVATE Ohio
Mike DeWine, Governor | Jon Husted, Lt. Governor and Director
# Table of Contents

1 Switzerland of Ohio Telehealth Pilot ........................................................................... 3
2 Switzerland of Ohio Telehealth Pilot Project Overview ........................................ 4
3 The Ohio State University Wexner Medical Center Telehealth Pilot Report ...... 5
4 Switzerland of Ohio Telehealth Pilot Project Timeline ............................................ 6
5 Why Should My School District Implement a Telehealth Program? ...................... 6
6 Checklist for Telehealth ............................................................................................... 7
7 Telehealth Protocols and Organizational Operations ............................................. 14

Appendix 1: SOH Initial Needs for Phase 1................................................................. 20
Appendix 2: SOH IT Professional Staff Costs........................................................... 22
Appendix 3: OSUWMC Report ................................................................................... 23
In March 2020, the state announced a telehealth pilot project to connect students with behavioral health providers in the Switzerland of Ohio Local School District (SOH). SOH is Ohio's largest school district by geographic size, covering all of Monroe County and parts of Belmont and Noble Counties. The district serves over 2,000 students in eight buildings across 536 square miles.

The project will improve infrastructure to support telehealth services, taking a step toward implementing InnovateOhio's “Ohio Broadband Strategy” to improve access to high-speed internet connectivity for all Ohioans.

The first phase of the project created spaces for providers to deliver care within each of SOH’s school buildings that are safe, comfortable, compliant with state and federal regulations, and capable of live video and audio. SOH’s school buildings already had access to a fiber-optic connection through OARnet. Phase one enhanced and added interactive video capabilities and limited travel required by existing behavioral health counselors between SOH’s eight buildings, some of which are over 30 miles apart and require an hour to travel between, to deliver needed care in a more timely and efficient manner.

The second phase of the project will connect SOH’s existing fiber-optic network directly to the remote offices of the district’s behavioral health provider partner, Southeast Healthcare Facilities.

Students will then have access to care and additional services beyond those provided by the counselors working in-person in the district. This phase may result in the addition of fiber-optic lines running through Monroe County.

The main-fiber optic conduit may then be accessible to the general public as a last-mile connection point for the community, expanding broadband internet to underserved areas of the county.

The project’s goals are to expand access to behavioral health services for SOH students and provide the opportunity for expanded access to broadband internet to underserved areas of Monroe County, while creating a blueprint to be used in other districts and communities across the state.
The objective is to connect the school district with behavioral health services while also providing high-speed internet connections to Ohioans who have been left behind. This project has two phases:

**Phase 1: School-to-school connectivity**

Ohio’s Academic Resource Network (OARnet) connects the school buildings in the district through a fiber-optic connection. This project will create telehealth spaces within the schools that are compliant with federal regulation and are capable of live video and audio feed. This meets the need, in a virtualized manner, with the district’s health professionals.

**Phase 2: Connect schools to local behavioral health provider**

Connect the school’s existing fiber-optic network directly to remote offices of behavioral health professionals, so students can have access to care and additional services.

This project also serves a dual purpose in connecting the surrounding communities with high-speed internet access. Additional fiber-optic lines being run through rural areas of the county to connect the remote provider with the school could potentially be accessible to the general public in the area as a possible last-mile connection point.

The guidelines outlined in this document result from the pilot project with Switzerland of Ohio Local School District. This blueprint is intended to be a living document that is updated as the pilot progresses.
The Ohio State University Wexner Medical Center Telehealth Pilot Report

The Ohio State University Wexner Medical Center (OSUWMC), in a collaborative effort with the Ohio Department of Medicaid (ODM) and in concert with Phase 1 of the telehealth pilot provided consultative services to SOH.

The overarching goals of this initiative are: 1) to ensure behavioral health services are accessible in nine school sites within SOH, 2) Increase behavioral health providers in SOH, and allow students, school personnel, parents and caregivers at varying locations the opportunity to access crisis services from counselors situated at different sites, and 3) serve as a flagship initiative to other school districts across Ohio, for use of telehealth, particularly in Medicaid, to address barriers to behavioral health care, such as insufficient supply of providers, inadequate transportation options, and long distances between patient and providers, as is the case for individuals and families in rural/remote areas and/or sprawling urban cities.

Phase One specifically includes the implementation of school to school communication of behavioral health providers within SOH, equipping each building with appropriate technology to allow for behavioral health sessions from one building to another and establishing proper protocols necessary to allow for a safe and confidential telehealth session from one building to another. Considerations include access to high-speed internet, broadband connectivity and establishing sites where behavior telehealth may be provided.

The OSUWMC’s responsibilities included participating in planning meetings and on-site visits to assist in identifying the SOH’s readiness for providing these services, evaluating the designated environment, analyzing the connectivity and assisting in developing the protocol for providing telebehavioral health services to students in need.

Additional activities will include participating in testing the workflow and technology, providing consultation on arising issues during the planning and set up period, assisting ODM in writing the training manual for the staff personnel and end-user protocol manual and assisting in the orientation and training of the staff personnel.

*The full OSUWMC report is attached as Appendix 3.*
Switzerland of Ohio Telehealth Pilot Project Timeline

- **November 2019**: Initial Conversations
- **February 2020**: MOU development and site visit
- **May 2020**: Transfer of funds to school for Phase 1 purchases
- **July 2020**: Begin second fiscal year spending
- **October 2020**: OSUWMC Contracted for Report
- **December 2020**: Phase 1 Operational

- **December 2019**: Location Identified
- **March 2020**: Announcement
- **June 2020**: End first fiscal year spending
- **September 2020**: Begin services in school Initial Blueprint Released
- **October/November 2020**: OSUWMC-State of Ohio Staff Visits

Why Should My School District Implement a Telehealth Program?

Telehealth adoption allows health care providers to increase continuity of care, extend access beyond normal clinic hours, reduce patient travel burden, and help overcome clinician shortages, especially in rural and other underserved populations. This ultimately helps health systems and physicians focus more on chronic disease management, enhance patient wellness, improve efficiency, provide higher quality of care, and increase patient satisfaction. Telehealth services, by their inherent remote nature, are also less likely to contribute to infectious disease spread.¹

6 Checklist for Telehealth

This blueprint details the steps taken by the telehealth working group when standing up the initial SOH pilot project. It is provided in a question and answer format. As additional school districts utilize this blueprint, answers will be expanded to include lessons learned through new projects.

6.01 Understanding Your District’s Needs

The initial question is to determine what need you want to address with telehealth. Each school district will be different. Your needs will not necessarily match those of the SOH pilot project. You may need to provide speech therapy services remotely, or give a nurse the ability to connect with students from the office. Here, we provide the needs of the SOH pilot project as an example:

1. **Time lost travelling from school to school**
   
   The SOH pilot is working to address the challenge behavioral health therapists face when driving from one building to another in a large district. Because the school district encompassed eight school buildings and over 500 square miles, time was lost as therapists needed to travel from one building to the other. Phase One connected the eight schools in the district together so that school counselors could more quickly meet with any students at any school, addressed this need.

2. **Inadequacy of connectivity between the provider and the school**
   
   The contracted local community behavioral health provider had only two therapists providing services within the schools, and limited ability to provide remote telehealth services from their office. Phase Two addresses this need, making sure that the therapists can communicate with students from the office, and possibly into their homes, instead of being limited to providing services in the school.

6.02 Identify Partners

1. **Are there other school districts to partner with?**
   
   The SOH pilot project was focused on a single school district as it had eight separate buildings and over 500 square miles in the district. You may have a smaller district and fewer miles to cover. You may be in a different scenario, and may want to partner with another school district to provide services.

2. **Do you have an existing partner for the services you want to provide through telehealth?**
   
   The SOH school district was already partnered with a behavioral health provider, and was able to work with them quickly to determine some of the needs for the project. Do you already have a provider that will be able to assist you in providing these services?

3. **Do you have community partners and champions?**
   
   You may find that local industry and employer groups, patient advocacy groups, parent groups and health care provider organizations may be able to provide various types of support and champion the project in the community.
6.03 Understand Capacity
Do you have the capacity to add more services and/or additional students with existing staff, resources, and funding?

1. Recommend conducting a needs assessment
The pilot focused on increasing behavioral health services to students. SOH was chosen as the pilot in part because of the district’s distinct need for an increase in behavioral health services. As each school district faces unique challenges, a needs assessment will assist in identifying the services that the students require.

2. Recommend conducting a gap analysis
Like the needs assessment, a gap analysis will provide additional guidance on possibly utilizing telehealth services to meet the health needs of students. The State of Ohio identified SOH as a district in need of behavioral health services.

6.04 Gauge School Readiness for Change

1. Are there internal change champions? (business unit, licensed providers, support personnel, patients/consumers, other healthcare partners)
SOH is a rural district that was short-handed with counselors. The superintendent and the district’s lead counselor both recognized the lack of resources and need for increased services, resulting in open-mindedness in implementing a pilot. Their leadership from the beginning resulted in a cohesive team approach and implementations from the start. SOH also had some experience with telehealth, as they had piloted using it as a means to connect students with the speech therapist.

2. Is there community support?
SOH suffered recent deaths in the surrounding communities resulting from behavioral health issues, leading to a community-wide acceptance of identifying and implementing new measures for help.

3. What did OSUWMC identify for SOH?
In-person behavioral health services are provided at scheduled times and in crisis situations by Southeast counselors who rotate between all schools throughout the school district.

Dedicated rooms were identified at some locations. At other locations, space was a challenge for in-person services and will continue to be so for telehealth. In preparation for delivering telehealth services between facilities, SOH updated its technical infrastructure and connectivity. Because staff and students have experience with audio/video meetings and educational activities, they were ready to integrate technology into the provision of behavioral health services.

While the counselors have laptops or surface pros, 25 percent of students and families do not have internet or cell service in their homes so being able to provide these services in the school is invaluable.

6.05 Assess Access to Reliable High-Speed Internet
You will need to conduct an impact analysis on your district’s current capabilities.

1. At primary site
SOH, along with most K-12 districts around the state, are connected by OARnet, one of the most advanced statewide telecommunications networks. This network provides a 100Gbps connection.

2. Will your existing internet connection support both your current school needs (data/phones) and the addition of bi-directional video? The speed and bandwidth must be acceptable for both receiving video as well as sending.
OARnet’s capabilities meet SOH’s needs.
6.06 Evaluating Space Needs

Will you have space, especially if you decide on larger-sized equipment or need to have dedicated desktop computers and/or internet connections vs. mobile equipment with secure, encrypted WIFI connections?

1. Will the space accommodate the new equipment?

SOH identified a room or rooms within each of its buildings to designate as telehealth rooms. Minimal construction and/or updates were needed to accommodate the necessary equipment. Additionally, OSUWMC identified tiers:

<table>
<thead>
<tr>
<th>Facility</th>
<th>Dedicated</th>
<th>Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swiss Hills Career Center</td>
<td></td>
<td>• Conference room in office area</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Principal’s office with partition for ad-hoc secondary office</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Counselor’s office</td>
</tr>
<tr>
<td>Skyvue Elementary School</td>
<td></td>
<td>• Possibly office due to size of student population size</td>
</tr>
<tr>
<td>Woodsfield Elementary School</td>
<td></td>
<td>• Shared office</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Waiting room</td>
</tr>
<tr>
<td>Monroe Central High School</td>
<td></td>
<td>• Conference room</td>
</tr>
<tr>
<td>Beallsville Schools</td>
<td></td>
<td>• Conference room</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Office (due to Covid-19, currently being used by assistant principal)</td>
</tr>
<tr>
<td>River Elementary School</td>
<td></td>
<td>• Conference room</td>
</tr>
<tr>
<td>River High School</td>
<td></td>
<td>• Conference room</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• School counselor’s office</td>
</tr>
<tr>
<td>Powhatan Elementary School</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Will you need to paint, add additional lighting, other furniture, cover windows or install sound buffers?

These additions were much more sustentative to the pilot in order to have the designated rooms meet standards and comfort levels. New lighting, desks, chairs, and sound barriers were needed before services could begin. See appendix for a complete list of items.

OSUWMC environment recommendations for SOH:

- Paint Color: Use neutral paint color in a low reflective sheen
- Acoustics: Meet sound absorption and sound isolation requirements
- Lighting: Control for glare by using direct frontal lighting and overhead lighting
- Privacy: Provide for speech and visual privacy
- Safety: Secure equipment and maintain room accessibility
3. **What if there is not a designated space?**

When one designated area is not available, creating a room availability schedule may be necessary for quickly having designated space to provide services in the instance of a crisis situation.

4. **Example room setup at Swiss Hills Career Center**

More detailed environmental recommendations can be found in the OSUWMC report.
6.07 Qualified IT Support

Will you need any qualified IT technical support that does not already exist within your organization? What about technical support at any partner or remote sites?

SOH needed to onboard an additional IT staffer to help with the increased caseload of implementing the pilot. See Appendix 2 for SOHIT staff costs.

6.08 Designing the Workflow

Telehealth appointments will likely require an adjusted workflow to ensure that you are offering a positive experience for both your students and care team. Daily logistics such as your physical workspace arrangement, appointment scheduling procedure, staff time, and communication may have to be altered to integrate telehealth into your school.

Consider how to incorporate telehealth appointments with the least amount of workflow disruption, especially at first, to help seamlessly introduce the technology to your school. Seek to understand the preferences and needs of both students and counselors, such as the times of day that may work best for them and what types of barriers they may have to engage in a telehealth visit, to ensure your workflow accounts for these details.

1. How will you schedule patients/consumers, provider time, support staff and space?
2. How will you allocate resources? (front desk time, support staff, clinical staff)
3. Will your billing process need to change?
4. How and what will need to be documented?
5. How will you share or communicate clinical information in a manner that meets HIPAA, HITECH and 42 CFR requirements when needed across sites? (i.e. physical exams, medication lists, medical or psycho-social history, etc.)
6. How will you collect clinical information, billing/insurance Information and signed informed consents from patients/consumers?
7. Will you need additional staff or other resources?
8. How will you orient patients/consumers?
9. How will you collect parental informed consents for health services?
10. Do you have a HIPAA compliant electronic health record system and will it need to be updated?
OSUWMC recommended the following telebehavioral health processes in its report:

<table>
<thead>
<tr>
<th>Crisis Situation</th>
<th>Ongoing Intervention</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiation</strong></td>
<td>The Crisis Team is notified of situation and the Counselor is called per District policy.</td>
</tr>
<tr>
<td><strong>Preparation</strong></td>
<td>The Crisis Team escorts the student to the telehealth area.</td>
</tr>
<tr>
<td><strong>Provision</strong></td>
<td>The telehealth room including safety and privacy of the area is secured by the District telepresenter.</td>
</tr>
<tr>
<td></td>
<td>If a mobile endpoint is used a telepresenter will bring it to the telehealth area and plug it in. The telepresenter will turn on the equipment and accept the telehealth appointment from the Counselor to begin the telehealth session.</td>
</tr>
<tr>
<td><strong>Documentation</strong></td>
<td>The Counselor and District telepresenter communicates via secure text or monitored email, as needed during the session. If there are audio video technical issues, the behavioral health session will be completed via phone.</td>
</tr>
<tr>
<td><strong>Follow up</strong></td>
<td>The school, student and parent/caregiver shall be advised of recommended follow up. The telehealth technology is turned off by the telepresenter. Mobile endpoints are returned to the designated storage area and plugged in.</td>
</tr>
</tbody>
</table>
6.09 Minimum Technical Specifications

1. **Internet speed of 384 kbps**
   SOH, along with most K-12 districts around the state, are connected by OARnet, one of the most advanced statewide telecommunications networks. This network provides a 100Gbps connection.

2. **Fully encrypted transmissions that comply with HIPAA, HITECH and 42 CFR requirements with secure passwords (reminder that users should NEVER share their individual password nor should you ever have common passwords.)**
   SOH added a SonicWall TZ400 firewall to increase network security. Also, SOH purchased an antivirus Sophos Central Intercept X 3 year subscription.

3. **Can the equipment/software/service/program meet needs and expectations?**
   SOH subscribed to a licensed meeting software through Google to provide telehealth services. This subscription includes administrative privileges, ensures necessary cybersecurity and meets all compliance guidelines.

6.10 Hardware Specifications

1. **What are the specific hardware recommendations for applying telehealth services?**
   OSUWMC recommended the following telehealth equipment within the outlined tiers (see 6.06 of this document). Tier 1 is recommended wherever dedicated space is an option.

   **Tier 1: Dedicated Space**
   - Micro form factor Windows 10 PC (minimum specs: Intel i5 processor, 8GB RAM, 128 GB SSD and Intel Iris Graphics, 1 Gbps Ethernet, integrated Wi-Fi) (secondary connectivity)
   - USB Pan Tilt Zoom camera (1080P) (Zoom Certified)
   - Conferencing quality microphone with noise-cancelling function and built in speaker
   - 32-47” inch LED Monitor 37 to 48 inches from floor;
   - Dedicated Ethernet line on telehealth VLAN

   **Tier 2: Mobile Solution**
   - Slim profile media cart for 32-55” displays with adjustable height
   - Micro form factor Windows 10 PC (minimum specs: Intel i5 processor, 8GB RAM, 128 GB SSD and Intel Iris Graphics, 1 Gbps Ethernet, integrated Wi-Fi) (secondary connectivity)
   - USB Pan Tilt Zoom camera (1080P) (Zoom Certified)
   - Conferencing quality microphone with noise-cancelling function and built in speaker
   - 32-47” inch LED Monitor
   - Dedicated Ethernet line on telehealth VLAN

   **Tier 3: Contingency option (no far end camera control, lower quality interaction)**
   - District issued laptop OR video phone
Video conferencing technology can expand availability of behavioral health services to many patients and consumers. Use of this technology simply becomes a tool or mode of delivering the services you may already offer.

This means that you will need to provide the clinical care under the same Ohio laws, professional licensing rules, certification standards, ethics, professional scope and standards as you do when you provide in-person, face-to-face services. Care provided via interactive video should be of a quality that is equivalent to in-person services.

Many centers and states with active telebehavioral/telemedicine programs strongly recommend that an organization develop clear and detailed policies and operating procedures and protocols prior to the implementation of clinical service provision. We have consolidated many of those recommendations and best practices into the following list for your consideration and use. This is not an all-inclusive list and providers are encouraged to obtain legal guidance if there are any questions.

As with any change to an organization’s daily operations, the implementation of a telebehavioral health program will be more successful with careful detailed planning. While real-time interactive video is just another mode or vehicle to providing services, it does take on-going coordination and staff dedicated to keep things running smoothly. Assigning and communicating roles and responsibilities will minimize confusion, disruptions and assumptions. A simple way to think about it is as though you are opening another operational site. You will not have the building costs yet you need to have a staffing plan. Procuring adequate/suitable/the appropriate equipment is important but you will need the right people in the right roles at the right time to keep things running. You still need to build the relationships, both internal and external.

7.01 Determine Staff – Roles and Responsibilities

1. How will you schedule staff time to include video-related duties along with their other responsibilities?

2. Define and determine exact roles and responsibilities
   a. Who runs the system/equipment and provides technical system support?
   b. Who schedules patients?
   c. Who collects, organizes and/or finds any needed records/health information prior to the video appointment and transmits the information to other providers in a manner that is compliant with HIPAA, HITECH, 42 CFR and other Ohio laws regarding PHI?
   d. Who provides on-going orientation, training and support to patients/consumers?
   e. Who will provide on-going training/updates to staff?
   f. Who will work with vendors?
   g. Who will be responsible for repairs, maintenance, licensure, lease agreements, and upgrades?
   h. Who will confirm patient/consumer appointments?
   i. Who will follow-up with the patient/consumer after clinical service?
   j. Who will be the contact person/number for patients/consumers served through video?
   k. Who will be the lead staff person responsible for ensuring on-going daily operations?
   l. Who will be the liaison to partner/remote sites?
   m. Who will train remote site staff?
   n. Which providers will participate in telebehavioral health services?
   o. Who will perform quality improvement activities?
   p. Who will respond to crisis situations?
7.02 Determine Your Reach And Partners

1. Will you connect directly to patients/consumers/family in their homes?
   The pilot is currently limited to students during school hours and only within the schools. However, similar projects could be expanded outside of this setting if necessary and complies with guidelines and standards.

2. Will you connect and partner with other sites within your organization’s current business model?
   Currently, the pilot is only available to SOH students within the respective district. However, cross-collaboration between districts is certainly feasible, especially when encompassing entire counties. SOH is unique in that it covers the entirety of Monroe County, creating a large geographic footprint.

3. Will you connect and partner with contract providers for services and/or capacity that you do not currently have?
   SOH will partner with a locally certified community behavioral health center to provide ongoing behavioral health telehealth services outside of the scope of the district’s counselors.

7.03 Determine What Students You Will Serve Via Telehealth

1. Will you limit the types of services you provide through video?
   SOH pilot provides behavioral health services to students.

2. Do you have providers that are willing to provide all the services via video?
   Phase Two of the SOH pilot connected the district with a local behavioral health provider to provide additional services beyond the scope of the schools’ resources. The pilot required both setting up teleconferencing services within SOH as well as ensuring that these services work properly with the local behavioral health provider.

7.04 Develop Protocols

1. How and what will you document?
2. Where will the patient/consumer records reside?
3. How will emergencies/crisis situations be handled, how will staff/providers be trained?
4. Where will a written protocol be kept with emergency telephone numbers pertinent to the patient location, (suicidal, homicidal, psychosis, and other safety issues)?
5. How will disconnection of video during a service be handled?
6. How will the signing of informed consent be handled?
7. How will you verify identity of patient/consumer, especially if they are never seen in person?
8. How will you handle non-patients/consumers in the room with the patient/consumer?
9. If the patient/consumer is at the location of another school will you need to determine clear roles and responsibilities between the sites?
10. Will there be any formal documentation generated to other providers (consult report, case notes, updates, treatment plans, other health reports, etc.)?
11. How can the student request or schedule a video appointment?
12. Will there need to be any adjustments or accommodations in treatment plans to allow for video-based services?
13. Will you be recording and storing the sessions? How will this be handled?
7.05 Ensure Quality of Service

1. Address Facility Issues
   SOH faced upgrading the designated rooms at every building where services are provided. For Phase One, SOH requested $215,000 in funding for supplies and aids. This includes medical supplies to support clinical professional for nine rooms, office and room aids for visual communication, and medical supplies such as blankets, sheets, and gloves. SOH requested an additional $35,000 for Phase Two medical supplies.

2. Set up a Quality Improvement Process
   a. Will there be a way for students to provide feedback to improve the teleconferencing services?

3. Orientation and Training
   a. Develop a staff/provider orientation plan and curriculum.
   b. Develop a patient/consumer orientation plan and curriculum.
   c. Set up an ongoing training plan (new procedures/services, new technology, new staff, refreshers for existing staff, updates on trouble shooting technical or safety issues).
   d. Orientation and marketing to parents.

7.06 Technology Considerations

1. Equipment
   SOH required front-end funding to build out equipment to provide the appropriate services. The following items were needed initially:
   - Direct attached optical transreceiver
   - Multinode jumper
   - Backup power rack mount
   - Access points for redundancy with licensing and management software
   - Managed switches
   - Microsoft Office subscriptions
   - TVs and stands
   - Additional routers
   - Computers for each room
   - Basic office equipment such as printers

   See Appendix for list and prices of items.

2. Services and Video Connections

3. System and Transmission Security
   SOH added a SonicWall TZ400 firewall to increase network security. Also, SOH purchased an antivirus Sophos Central Intercept X 3 year subscription.

   Additionally, the meeting software is licensed through Google and includes the necessary compliance and security measures. SOH also onboarded an additional IT staffer to assist with this project.
4. Component options

OSUWMC identified the following components. More details can be found within the report in Appendix 3.

<table>
<thead>
<tr>
<th>User Experience</th>
<th>Good</th>
<th>Better</th>
<th>Best</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS 8.0 or later (iPhone 4 or later, iPad Pro, iPad Mini, iPad 2 or later, iPod touch 4th Generation)</td>
<td></td>
<td></td>
<td>All can be mounted on a cart if desired</td>
<td></td>
</tr>
<tr>
<td>Android OS 5.0 or newer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any 1 Ghz single core processor or better (non-Intel)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Camera</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated Camera, Microphone and Speaker:</td>
<td>Combination USB Camera and Microphone:</td>
<td>USB Point/Tilt/Zoom</td>
<td>Camera and microphone selection impacts the other user’s experience</td>
<td></td>
</tr>
<tr>
<td>• Integrated camera (720p–1080p, Zoom Certified)</td>
<td>• Integrated camera (720p–1080p, Zoom Certified)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Integrated microphone and speaker</td>
<td>• Integrated microphone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Microphone</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated</td>
<td>Combination USB Camera and Microphone:</td>
<td>USB video conferencing microphone speaker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>microphone and speaker</td>
<td>• Integrated microphone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Speakers</strong></td>
<td>USB Sound Bar</td>
<td>Conferencing quality microphone with beam-forming, noise/echo cancelling and built in dual or quad speaker</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Display</strong></td>
<td>Integrated</td>
<td>External 27–32 inch LED</td>
<td>External 32–47 inch LED or OLED monitor</td>
<td>Preferred location 37–48 inches from floor</td>
</tr>
<tr>
<td><strong>Can be mounted to cart or wall</strong></td>
<td>Wi-Fi</td>
<td>Wi-Fi or Ethernet</td>
<td>Wi-Fi or Ethernet line on telehealth VLAN</td>
<td>Recommend minimum 100 Mbps up/down link</td>
</tr>
</tbody>
</table>
7.07 Parental Consent

The purpose of parental consent is to assure that a student’s family both acknowledges and approves of interaction(s) between the education system and healthcare providers, which can include:

- Assessing and treating the patient
- Keeping the community of care in the loop
- Getting reimbursed
- Evaluating program outcomes

Consent is sought in medical settings to assure that healthcare services are both acceptable and allowable to the recipient. Parental consent typically consists of a short form that requests the ability to treat a student. Consent can either be a blanket consent to deliver any needed healthcare services over a given period of time (e.g., a school year, or the enrollment span of a student in a district), or can be per encounter (e.g., each time a student seeks health services).

There are no federal or state requirements for additional consent to provide services via telehealth. However, some professional licensure boards require written parental consent to provide services via telehealth. For more information, providers may wish to check with the schools they work with along with their professional licensure boards.
7.08 Protecting Student Privacy

Both the healthcare and education realms are governed by specific laws that limit the use and disclosure of data generated within that specific realm, including the Health Insurance and Portability and Accountability Act (HIPAA), Confidentiality of Substance Use Disorder Patient Records regulations, (42 CFR Part 2), and Family Educational Rights and Privacy Act (FERPA).

HIPAA protects the privacy of a student’s medical records and applies to all health services provided in a school building or in the community. Health care providers in schools should obtain parental authorization to share health information protected by HIPAA, which is no different than the authorization that is sought prior to sharing protected health information for any patient records in your usual course of practice. Providers do not need parental authorization to share information with a school nurse or other Ohio Department of Education-licensed school health provider (as per HHS guidance), or general information that does not contain a student’s protected health information (PHI). See also HIPPA Compliance and COVID-19 Coronavirus and HIPPA Telehealth.

Regulations at 42 CFR Part two protect the confidentiality of patient identified records relating to substance use disorder diagnosis, referral, or treatment. A part two program or other lawful holder of records from a part two program generally must obtain consent prior to release of such records.

FERPA protects the privacy of a student’s education records and applies to all public and private educational institutions who receive federal funds for programs, including the IDEA. School staff should obtain parental consent to share FERPA-protected data that normally is not shared outside the school setting. School staff does not need parental consent to share longitudinal data that does not contain a student’s protected health information (PHI). See Protecting Student Privacy – FERPA and the Coronavirus 2019 (COVID-19).

The U.S. Departments of Health and Human Services and Education have also issued joint guidance on the application of FERPA and HIPAA to student health records to explain the relationship between the FERPA statute and implementing regulations and the HIPAA Privacy Rule.

In considering telehealth options, it is essential to review important resources that explain HIPAA and FERPA laws and how they may apply to telehealth services, as well as the coronavirus (COVID-19) compliance updates to ensure student and family privacy is protected during this time.

Schools should make every effort to use platforms that are HIPAA compliant for telehealth services. In addition, service providers should check with their professional licensure boards for any requirements to use encrypted platforms. The Ohio Department of Education does not endorse or recommend any platform, but the following platforms represent that they are HIPAA compliant:

- Skype for Business / Microsoft Teams
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite
- Amazon Chime
- GoToMeeting
- Spruce Health Care Messenger
- Hangouts Meet

Given the continued presence of COVID-19, rules may continue to change. See the U.S. Department of Health and Human Services’ Health Information Privacy webpage for updates.
Appendix 1: SOH Initial Needs for Phase 1

Initial Funding and Descriptions

<table>
<thead>
<tr>
<th>Item/Position</th>
<th>Brief Description of Need</th>
<th>Anticipated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Specialist</td>
<td>Additional IT person to help additional case load for new project.</td>
<td>$6,777.00</td>
</tr>
<tr>
<td>SFP - 10G LRM</td>
<td>Direct attached optical transceiver SFP+ (QTY: 16) Double for redundancy</td>
<td>$7,008.00</td>
</tr>
<tr>
<td>SFP - Multimode Fiber</td>
<td>100M OM3 LC LC Fiber Patch Cable</td>
<td>Indoor/Outdoor 10Gb Duplex 50/125 LC to LC Multimode Jumper (Qty:16) Double for redundancy</td>
</tr>
<tr>
<td>Sonic Wall - Firewall</td>
<td>TZ400-w Sonic Firewall</td>
<td>$980.00</td>
</tr>
<tr>
<td>OAW-AP</td>
<td>Access Points Indoor (Qty: 16) Double for redundancy</td>
<td>$10,386.00</td>
</tr>
<tr>
<td>OV-AP Licensing</td>
<td>Access Point Licensing for Management (Qty:16) Double to cover for redundancy units</td>
<td>$5,280.00</td>
</tr>
<tr>
<td>Cabling for AP</td>
<td>Cat6 cable drops for APs (plenum for 16 AP drops)</td>
<td>$4,640.00</td>
</tr>
<tr>
<td>Switch POE</td>
<td>Managed switches with POE - 24 Port (Alcatel Lucent) - (Qty: 8) - Redundancy</td>
<td>$31,536.00</td>
</tr>
<tr>
<td>Switch POE</td>
<td>Managed switches with POE - 5 Port (DLink) - (Qty: 2) - Redundancy (ASOS)</td>
<td>$124.00</td>
</tr>
<tr>
<td>Computer Software</td>
<td>MS Office 2019 PRO- Home and Business (Qty: 12) - Cover PCs and Admin Team</td>
<td>$5,280.00</td>
</tr>
<tr>
<td>Computer Software</td>
<td>Antivirus Sophos Central Intercept X (Qty: 12) - Cover PCs and Admin Team -3yr subscription</td>
<td>$243.00</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>(Current Configuration) - Upgrade to 1Gb to all buildings that will be housing telehealth. (Qty:6)</td>
<td>$66,186.00</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Redundancy</td>
<td>$54,540.00</td>
</tr>
<tr>
<td>Router</td>
<td>Redundancy Equipment for Fiber line</td>
<td>$8,833.00</td>
</tr>
<tr>
<td>TV Mobile Stand</td>
<td>ONKRON Mobile TV Stand (Qty: 9) White</td>
<td>$1,440.00</td>
</tr>
<tr>
<td>TV</td>
<td>Samsung ALED 55&quot; Flat Screen TV (Qty:9)</td>
<td>$6,462.00</td>
</tr>
<tr>
<td>Printer</td>
<td>Office Printer all in one - HP Color Laser Jet (Qty:9)</td>
<td>$3,860.00</td>
</tr>
<tr>
<td>Office Equipment</td>
<td>IP Phones tied into Head End Equipment</td>
<td>$7,781.00</td>
</tr>
<tr>
<td>Computer/Laptop</td>
<td>TM 5010 - Windows 10 Pro - Anti-bacteria seamless enclosed unit (Qty 9)</td>
<td>$24,183.00</td>
</tr>
</tbody>
</table>

Total FY20 Phase 1 Costs: $275,000.00
<table>
<thead>
<tr>
<th>Item/Position</th>
<th>Brief Description of Need</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Specialist</td>
<td>Additional IT person to help additional case load for new project.</td>
</tr>
<tr>
<td>Additional Bandwidth per Building</td>
<td>Upgrade 1G bandwidth for each building per year</td>
</tr>
<tr>
<td>Medical Clinical Assist Carts</td>
<td>Carts for 9 building locations</td>
</tr>
<tr>
<td>Licensing for Meeting Software</td>
<td>Meeting Software with Admin Controls through Google per year</td>
</tr>
<tr>
<td>Wireless Equipment (New Installs)</td>
<td>New installs for 9 locations</td>
</tr>
<tr>
<td>Fiber Redundancy for Buildings</td>
<td>WAN Connectivity / Redundancy for 9 locations to serve Telemedicine Rooms per year</td>
</tr>
<tr>
<td>Computer/Laptop</td>
<td>Mobile devices for 9 medical rooms</td>
</tr>
<tr>
<td>TV</td>
<td>Monitors for Conferencing for 9 rooms with a Min of 42”</td>
</tr>
<tr>
<td>Cabling for Conferencing Connectivity</td>
<td>Misc Cabling for conferencing for 9 rooms</td>
</tr>
<tr>
<td>Office Equipment for Medical Room</td>
<td>Desk, chairs, tables, and misc room furniture for 9 rooms</td>
</tr>
<tr>
<td>Medical Office Supplies</td>
<td>Medical Supplies to support Clinical Professional for 9 rooms</td>
</tr>
<tr>
<td>Medical Visual Aids</td>
<td>Office and room aids for visual communication for 9 rooms</td>
</tr>
<tr>
<td>Medical Supplies</td>
<td>Medical Supplies - Blankets, sheets, gloves, masks, pillows, wipes, etc... for 9 buildings</td>
</tr>
</tbody>
</table>
### Appendix 2: SOH IT Professional Staff Costs

**Effective for school year 2019 – 2020 IT Technician Salary Schedule**

<table>
<thead>
<tr>
<th>Pay Scale (Effective July 2019)</th>
<th>Wages (255 Days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$38,300.00</td>
</tr>
<tr>
<td>1</td>
<td>$38,874.50</td>
</tr>
<tr>
<td>2</td>
<td>$39,457.62</td>
</tr>
<tr>
<td>3</td>
<td>$40,049.48</td>
</tr>
<tr>
<td>4</td>
<td>$40,650.22</td>
</tr>
<tr>
<td>5</td>
<td>$41,259.98</td>
</tr>
<tr>
<td>6</td>
<td>$41,878.88</td>
</tr>
<tr>
<td>7</td>
<td>$42,507.06</td>
</tr>
<tr>
<td>8</td>
<td>$43,144.67</td>
</tr>
<tr>
<td>9</td>
<td>$43,791.84</td>
</tr>
<tr>
<td>10</td>
<td>$44,448.71</td>
</tr>
<tr>
<td>11</td>
<td>$45,337.68</td>
</tr>
<tr>
<td>12</td>
<td>$46,244.43</td>
</tr>
<tr>
<td>13</td>
<td>$47,169.32</td>
</tr>
<tr>
<td>14</td>
<td>$48,112.71</td>
</tr>
<tr>
<td>15</td>
<td>$49,074.96</td>
</tr>
<tr>
<td>18</td>
<td>$50,056.46</td>
</tr>
<tr>
<td>20</td>
<td>$51,057.59</td>
</tr>
<tr>
<td>25</td>
<td>$52,078.74</td>
</tr>
</tbody>
</table>
Leadership and staff within the Switzerland of Ohio Local School District are engaged and committed to implementing telehealth to supplement in person behavioral health services provided by Southeast counselors. They look forward to having more timely access to counselors during crisis situations and are already considering where and how telehealth can be provided. Dedicated rooms have been identified at some locations. At other locations, space is a challenge for in person services and will continue to be so for telehealth. In preparation for delivering telehealth services between facilities, the District has been updating its technical infrastructure and connectivity. Because staff and students have experience with audio video meetings and educational activities, they are ready to integrate technology into the provision of behavioral health services.

The following recommendations are made to facilitate the implementation of these services.

### Readiness

1. Identify an administrative leader who has authority and will take responsibility for promoting telebehavioral health, monitoring implementation and removing barriers to success. The principal may be a good choice for assuming this role.

2. Establish a school project leader responsible for facilitating telehealth implementation and escalating issues to the administrative leader. This person should have good planning, decision-making and follow thru skills. They also should be willing to identify and escalate barriers to success. If a school has an assistant principal, that person may be a good option for assuming this responsibility. At some locations, it may make sense for the administrative lead and project leader to be the same individual.

3. Identify a school-based clinical champion to be the telebehavioral health expert and resource for other staff. It might make sense for the Behavior Therapist to serve in this capacity.

4. Identify core behavioral health certifications or competencies required for staff assisting with telebehavioral health.

5. Identify key staff and assure they have completed required certification, access and training.

6. At schools where shared space will be used for telehealth, document the schedule for room availability.

7. Create a dedicated technical support option for telehealth within the established incident response workflow. This should be readily accessible at any time.

### Designated Environment: Telehealth Equipment and Modifications

#### Environment

- **Paint Color:** Use neutral paint color in a low reflective sheen
- **Acoustics:** Meet sound absorption and sound isolation requirements
- **Lighting:** Control for glare by using direct frontal lighting and overhead lighting
- **Privacy:** Provide for speech and visual privacy
- **Safety:** Secure equipment and maintain room accessibility

#### Telehealth Equipment: Hardware

PC-based options for dedicated space and mobile solutions are recommended. Selecting the mobile option for all sites may add maximum flexibility and ease support requirements for District IT. A contingency-only option is included. This option utilizes existing District hardware in the event of unavailability or technical issues with the primary solution. This existing hardware can provide means to an interaction via the audio video platform in an emergency, but does not offer advanced features like far end camera control and offers a lower quality interaction for student and Counselor in comparison to better solutions.

- **Option 1:** Dedicated Space
- **Option 2:** Mobile
- **Option 3:** Contingency
Telehealth Equipment: Software
Zoom for Healthcare, the HIPAA compliant version of the platform, is recommended as the base platform for telehealth visits between the District and Southeast.

General Guidelines for Software and Support
Ensure technology infrastructure and software configuration meets HIPAA security and privacy standards and is approved by the District’s privacy officer.

Use only software with HIPAA approved security and settings. Work closely with the vendor and privacy officer to ensure appropriate application of rules. Account-level configuration considerations include use of waiting room to control access, use of PIN and password, and limiting screen share and camera control.

Maintain telehealth endpoint software in accordance with District policies for managing and updating operating system and client software for static and mobile devices.

IT support staff should have remote connectivity to all telehealth endpoints to provide support for technical issues.

IT should create and maintain knowledge documentation to facilitate quick resolution of common issues.

---

Information Technology (IT) Connectivity
Conduct load testing and Wi-Fi coverage mapping and performance analysis after the 100 Mbps line is installed and primary line capacity is increased to 1000 Mbps.

---

Provision of Behavioral Health Services to Students in Need
Implementation steps to include:

1. Review and update service agreements and policies based on regulatory considerations and using the School-based Health Care Support Toolkit as a resource.

2. Develop and approve Telehealth Standards including Space, Equipment, Competency Expectations and Protocol.

3. Establish technology support plan including reference documents.

4. Establish end user training plan including reference documents.

5. Acquire technology and validate designated environment, technology, and connectivity are ready for telehealth.

6. Schedule clinical and technical training.

7. Complete training and document competency.

8. Conduct practice sessions.


10. Evaluate and refine.

11. Provide refresher training as needed.
The Ohio State University Wexner Medical Center (OSUWMC), in a collaborative effort with the Ohio Department of Medicaid (ODM) and in concert with Phase 1 of Grant G-2020-00-0385 provided consultative services to the Switzerland of Ohio Local School District (District). The overarching goals of this initiative are: 1) to ensure behavioral health services are accessible in nine school sites within the (District), 2) Increase behavioral health providers in the District, and allow students, school personnel, parents and caregivers at varying locations the opportunity to access crisis services from counselors situated at different sites, and 3) serve as a flagship initiative to other school districts across Ohio, for use of telehealth, particularly in Medicaid, to address barriers to behavioral health care, such as insufficient supply of providers, inadequate transportation options, and long distances between patient and providers, as in the case for individuals and families in rural/remote areas and/or sprawling urban cities.

Phase One specifically includes the implementation of school to school communication of behavioral health providers within the District, equipping each building with appropriate technology to allow for behavioral health counseling to students in their home. While the counselors have laptops or surface pros, twenty-five percent of students and families do not have internet or cell service in their homes so being able to provide these services in the school is invaluable. Ms. McVey demonstrated an awareness of privacy and professional setting requirements. She was also thoughtful about how to modify existing processes from in-person to telehealth to care for students in a safe and timely manner. Crisis intervention for students and staff was identified as the top priority, however ongoing intervention for students was also an option. Not having adequate bandwidth during high utilization times, sufficient technology aptitude, appropriate and available rooms, dedicated leadership and expert champions at each school, role clarity, established protocols, and knowledge of expectations could present risks for rolling out a telehealth program however the District is well positioned to overcome those risks.

### Findings

#### Readiness

In person behavioral health services are provided at scheduled times and in crisis situations by Southeast counselors who rotate between all schools throughout the District. We spoke with staff and leadership at each school who are engaged and committed to implementing telehealth to supplement the in-person services. They look forward to having more timely access to counselors during crisis situations and are already considering where and how telehealth can be provided. Dedicated rooms have been identified at some locations. At other locations, space is a challenge for in-person services and will continue to be so for telehealth. In preparation for delivering telehealth services between facilities, the District has been updating its technical infrastructure and connectivity. Because staff and students have experience with audio/video meetings and educational activities, they are ready to integrate technology into the provision of behavioral health services. One counselor, Rebekah McVey, shared that during Covid restrictions this spring, she delivered tele behavioral sessions from one building to another and establishing proper protocols necessary to allow for a safe and confidential telehealth session from one building to another. Considerations include access to high-speed internet, broadband connectivity and establishing sites where behavior telehealth may be provided.

The OSUWMC's responsibilities included participating in planning meetings and on-site visits to assist in identifying the District's readiness for providing these services, evaluating the designated environment, analyzing the connectivity and assisting in developing the protocol for providing telebehavioral health services to students in need.

Additional activities will include participating in testing the workflow and technology, providing consultation on arising issues during the planning and set up period, assisting ODM in writing the training manual for the staff and end-user protocol manual and assisting in the orientation and training of the staff personnel. This report addresses OSUWMC's findings and recommendations.

#### Designated Environment: Telehealth Equipment and Modifications

The originating sites, nine schools at eight locations, were toured and the proposed environments evaluated for hosting individual and/or group behavioral health services via telehealth. (See Appendix A)

Five locations identified dedicated space for telehealth and three of those locations also identified shared space. Three locations have several telehealth-ready spaces identified, but cannot dedicate space. Network and power outlets are planned, but have not been implemented in all spaces. In general, the rooms evaluated are adequate for telehealth with a few modifications. Most of the spaces were well lit, but cluttered and were private or semi-private requiring a few minor modifications to become private.
Facility | Dedicated | Shared
--- | --- | ---
Swiss Hills Career Center |  | 
Skyvue Elementary School |  | Conference room in office area
|  | Principal’s office with partition for ad-hoc secondary office
|  | Counselor’s office
Woodsfield Elementary School |  | Possibly office due to size of student population size
Monroe Central High School |  | Shared office
|  | Waiting room
Beallsville Schools |  | Conference room
River Elementary School |  | Conference room
|  | Office (due to Covid, currently being used by assistant principal)
River High School |  | Conference room
|  | School counselor’s office
Powhatan Elementary School |  | 

Tess Hill, District Director of Information Technology, reported that Avaya Vantage K175 Dual Port with Camera Video phones have been purchased and are being placed at locations where dedicated telehealth rooms have been identified. Dell Touch Screen Laptops will be available as a backup to the room or mobile telehealth solution for counselor use in each room and where feasible large monitor screens will be installed for mirror casting the phone display to provide better video visualization. Zoom licensing has been purchased to allow meeting and private connectivity. Furniture and accessories have been ordered for dedicated rooms. No other equipment has been ordered pending consultant recommendations.

Information Technology (IT) Connectivity

Ms. Hill reported that the existing information technology infrastructure includes 500 Mbps fiber link with Wi-Fi available district wide. This primary fiber link will be expanded to 1000 Mbps. The network team will use VLANs to segment network traffic. A 100 Mbps redundancy line is planned as a contingency specific to telehealth needs. In addition, 184 Wi-Fi drops are being added to the existing environment.

The existing infrastructure was tested as a baseline. Network speeds of 200 Mbps upload and 200 Mbps download with low latency of less than 50ms were observed during random in-network tests. Additional testing will be necessary once the capacity is increased, redundancy is added and VLANs are configured. However, given the stability and performance observed during our site visits, it appears the sites have adequate baseline connectivity to support telehealth. There are no plans to utilize Wi-Fi coverage for telehealth at this time, so Wi-Fi was not evaluated. There was some concern that there may be bandwidth constraints on testing days where most students are online. The additional capacity, VLANs, and dedicated backup line should remediate those concerns.

Provision of Behavioral Health Services to Students in Need

Lydia Brodegard, Director of Special Education for the Ohio Valley Educational Service, provided a Policy and Procedure for Telehealth Practices in Switzerland of Ohio Local School District (See Appendix B). It describes how telehealth would be integrated into the current processes for in person behavioral health services. The building principal, GMN Tri-County CAC, Inc. case manager, prevention specialist, behavior staff, school counselor, school nurse, juvenile court or parent/guardian can submit a referral for Southeast Counseling services by completing a referral form. The use of telehealth for crisis situations is the first priority, followed by use for ongoing intervention. Staff who have a valid certificate for completing Non-violence Crisis Intervention training and who have been trained in the use of the telehealth technology will be identified at each building to assist with tele behavioral health. For crisis situations, the crisis team would be notified with the call going to the counselor per District policy. The identified person would secure the telehealth area and safety in the environment. The identified person would follow the telehealth quick guide to connect to the Southeast counselor (See Appendix C). If not in crisis, and safety is secured, the person may wait outside the room if the room has a window so the student can be in view. Other documents the District shared were: Behavioral Specialist Referral Form, GMN Referral Form, Prevention Programs 2020, Southeast Duty to Protect, Southeast Referral Form, Student Mental Health and Suicide Prevention, Student Services Referral Form, Suicide Intervention Process and Telehealth Zoom account.
Recommendations

Readiness

The District leaders and staff have been busy with preparations for adding telehealth as a supplement to in-person behavioral health services. Identifying key staff and establishing role expectations for the actual implementation will help to facilitate a smooth rollout. (See Appendix D)

1. Identify an administrative leader who has authority and will take responsibility for promoting telebehavioral health, monitoring implementation and removing barriers to success. The principal may be a good choice for assuming this role.

2. Establish a school project leader responsible for facilitating telehealth implementation and escalating issues to the administrative leader. This person should have good planning, decision-making and follow thru skills. They also should be willing to identify and escalate barriers to success. If a school has an assistant principal, that person may be a good option for assuming this responsibility. At some locations, it may make sense for the administrative lead and project leader to be the same individual.

3. Identify a school-based clinical champion to be the tele behavioral health expert and resource for other staff. It might make sense for the Behavior Therapist to serve in this capacity.

4. Identify core behavioral health certifications or competencies required for staff assisting with tele behavioral health. A consideration for non-licensed mental health professionals would be the Crisis Prevention Institute’s certification in non-violence crisis intervention crisisprevention.com. Other training may include Mental Health First Aid mentalhealthfirstaid.org. Kognito training may be helpful for teachers and staff who may not be directly assisting with the telehealth encounter but may be identifying or working with students at risk kognito.com.

5. Identify key staff and assure they have completed required certification, access and training.

6. At schools where shared space will be used for telehealth, document the schedule for room availability.

7. Create a dedicated technical support option for telehealth within the established incident response workflow. This should be readily accessible at any time.

Designated Environment: Telehealth Equipment and Modifications

Telehealth environments should be on par with other clinical environments where patient interactions occur. Rooms should be quiet, well-lit and free of clutter. Care should be taken to ensure patient and provider safety by securing all equipment including cabling, attached peripherals and other potentially loose desk items that could be distracting or used to cause harm.

Environment

- Paint Color
  - Select room finishes and colors to maintain natural rendition of color and pattern.
  - Backdrop wall color needs a light reflectance value of 30–40%.
  - Recommend neutral paint color in a low reflective sheen.

- Acoustics
  - Speech Intelligibility - Maintain the minimum sound absorption coefficient per FGI for a room’s clinical requirement.
  - Sound Isolation - Achieve minimum STC ratings per FGI for a room’s clinical requirement.
  - Background noise - Maintain background noise levels for a room’s clinical requirement.

- Lighting
  - Provide direct frontal lighting in addition to overhead lighting when possible.
  - Use natural and artificial light sources to control for glare. Dimmable lighting may be applicable.

- Privacy
  - Provide speech and visual privacy with adjacent spaces based on the room’s original function.
  - Arrange monitors and screens so they are not visible to casual observers outside the telemedicine room.
  - Patient should be visible to telepresenter while maintaining as much privacy as possible.

- Safety (specific to originating site)
  - Secure all equipment including cabling, peripheral devices and other desktop items to prevent harm.
  - Maintain accessibility to room (e.g., not locked)
  - Ensure telepresenter has visibility to student in room even if they are actually not in the room. A window with a shade installed on the outside of the room provides the option to have the shade up for full viewing during a crisis situation or down for more privacy during a therapeutic session.
Telehealth Equipment: Hardware (See Appendix E)

Providers and staff have communicated the need for a reliable, easy to use platform for telehealth. There were specific requests for particular capabilities, such as far end camera control and a more robust experience for the student. Camera control will allow the remote provider to easily move with the patient. Camera placement should allow for the participant and provider to be looking directly at each other. The camera should be mounted close to the display, either directly above or directly below the display. Medium sized screens will help the patient better connect with the provider since they provide a near life-sized experience. Combined microphone and speaker units will provide the most realistic audio experience for the student while also capably delivering the best audio to the provider. These recommendations are focused on the District endpoints. The best options for external providers are typically more portable options.

Telehealth hardware recommendations are categorized into good, better and best options. Additionally, implementation of these packages is categorized into three options: dedicated, mobile and contingency.

Dedicated implementations are recommended wherever dedicated space is an option. A typical dedicated implementation would involve a combination of better or best rated components. Mobile solutions can utilize the entire range of recommended hardware components with the use of specialized media carts. Since most locations do not have dedicated space and will require a mobile solution, this implementation may be desirable for all locations. The mobile option will require additional considerations, including identification of an easily accessible storage location for the cart and some additional preparation by the telepresenter at the time of a consultation. The contingency option is not recommended as a primary solution since these options offer a lower quality interaction and lack required features such as far end camera control. The contingency option is included solely as a backup in the event of technical failure or other situations that make the dedicated or mobile options unavailable such as emergent technical problems or budget constraints.

Component Options

- **Endpoint**
  - The endpoint component provides the power necessary to support real-time audio video interactions. Desktop endpoints are inherently more powerful and capable. These have more ports for peripheral components, more processing power and are highly customizable. Laptops offer a combination of some of the benefits of desktops and add portability. Laptops and desktops can both utilize USB or Bluetooth connectivity to accommodate peripherals including better camera, microphone, speaker, monitor and display components. Tablets are portable, but they have limited or no capability to accept peripheral components. Video phones are typically wired and not portable and have the same or increased limitations compared to tablets.

- **Camera**
  - Integrated cameras provide convenience but are often limited due to their size. USB Cameras offer flexibility and are easier to obtain in the highest available resolutions (1080p or higher). USB cameras also can offer additional advanced features like Point/Tilt/Zoom control. Point/Tilt/Zoom (PTZ) control means that the camera has motors that can be controlled remotely to change the direction and zoom of the camera. The best USB PTZ cameras also offer high quality optical zoom as well as digital zoom. Optical zoom involves an actual adjustment of the lens while digital zoom uses software to manipulate the image.

- **Microphone**
  - Most integrated cameras and USB cameras include a microphone. Integrated camera and microphone combinations are usually adequate for one-to-one conversations where the speaker is sitting close to the equipment. Integrated cameras are generally incapable of wide-angle views and their microphones are not suited for medium to large rooms or situations where the speaker is more than 3 feet away from the device. USB cameras can include better built-in microphone options than integrated cameras. These types of options include noise cancelling or even advanced beam-forming options. Beam-forming allows the microphone to adjust for the position of the speaker dynamically. Combining these devices can help save space and cost, but better performance and options are available with a separate, conferencing quality microphone speaker. Standalone USB microphones contain advanced hardware that helps keep voices clear at all times and excels in larger spaces with multiple participants in the room. These advanced, dedicated...
microphones also include two or more speakers for stereo or surround sound, making the remote speaker more clear as well. Microphones with integrated speakers will generally manage noise and echoes well since both incoming and outgoing audio are managed by the same device.

- **Speakers**
  Most endpoints will have integrated speakers that will adequately provide audio for telehealth. Separate speakers, such as a sound bar, will generally have more power and better fidelity. The best speaker option for the school-based endpoint is a conferencing-quality, combined microphone and speaker array. These devices are specifically intended to manage synchronous two-way communications. The microphone and speaker work together to provide clear audio in both directions in situations with multiple participants in one location.

- **Display**
  Most integrated displays are adequate for telehealth if they are capable of at least 720p HD resolution. The smaller integrated display of a tablet, video phone or laptop offers portability at the expense of a robust telehealth experience for the student. Desktops with integrated displays of 24” to 27” are also adequate but still offer a lesser telehealth experience for the student. The best option is to use a larger external display between 32” and 47” that is capable of 1080p or better HD resolution. Display size should be chosen based on the location and relative distance between the screen and the patient. The distant provider should appear life-sized to the student. A display that is too large or too small will create a more artificial experience for the patient and should be avoided.

  Displays should be wired to the endpoint. Some endpoint operating systems are capable of wirelessly connecting to an external display using technologies such as AirPlay or Chromecast. These wireless display technologies are not recommended for telehealth since they introduce lag and reduce framerate of incoming video.

- **Network**
  Wi-Fi can be adequate for telehealth, but wired Ethernet should be used if it is available. Wired connections will be faster and more stable than Wi-Fi. Additionally, segmenting the network using a dedicated VLAN (virtual local area network) for the telehealth endpoint is recommended as a best practice for increased performance and increased security.

### User Experience Table

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Good</th>
<th>Better</th>
<th>Best</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tablet</td>
<td>iOS 8.0 or later (iPhone 4 or later, iPad Pro, iPad Mini, iPad 2 or later, iPod touch 4th Generation) Android OS 5.0 or newer Any 1 Ghz single core processor or better (non-Intel)</td>
<td>Windows 10 Processor: Intel i5 Memory: 8–16 GB RAM Storage Type: any Storage Capacity: 256–512 GB Graphics: Intel Iris Graphics Network: 1 Gbps Ethernet + Wi-Fi</td>
<td>Windows 10 Processor: Intel i7–i9 Memory: 16-24 GB RAM Storage Type: any Storage Capacity: 512 GB–2 TB Graphics: NVIDIA dedicated Graphics Network: 1 Gbps Ethernet + Wi-Fi</td>
</tr>
</tbody>
</table>

### Notes
- All can be mounted on a cart if desired

### Endpoint Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Good</th>
<th>Better</th>
<th>Best</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera</td>
<td>Integrated Camera, Microphone and Speaker:</td>
<td>Combination USB Camera and Microphone:</td>
<td>USB Point/Tilt/Zoom</td>
</tr>
<tr>
<td>Speakers</td>
<td>USB Sound Bar</td>
<td>Conferencing quality microphone with beam-forming, noise/echo cancelling and built in dual or quad speaker</td>
<td></td>
</tr>
<tr>
<td>Display</td>
<td>Integrated</td>
<td>External 27–32 inch LED</td>
<td>External 32–47 inch LED or OLED monitor</td>
</tr>
<tr>
<td>Can be mounted to cart or wall</td>
<td>Wi-Fi</td>
<td>Wi-Fi or Ethernet</td>
<td>Wi-Fi or Ethernet line on telehealth VLAN</td>
</tr>
</tbody>
</table>

Camera and microphone selection impacts the other user’s experience.

Preferred location 37–48 inches from floor.
Telehealth Equipment: Software

The District and Southeast Healthcare are both familiar with the Zoom platform, which is a popular, worldwide platform used for education, business, and personal interactions. Given student, staff and provider familiarity with Zoom, Zoom for Healthcare, the HIPAA compliant version of the platform, is recommended as the base platform for telehealth visits between the District and Southeast (See Appendix F for details about Zoom for Healthcare). While there may be waivers in place during the Covid pandemic, it is imperative that the technology infrastructure be secure and private (Appendix G).

General Guidelines for Software and Support:

- Ensure technology infrastructure and software configuration meets HIPAA security and privacy standards and is approved by the District’s privacy officer.
- Use only software with HIPAA approved security and settings. Work closely with the vendor and privacy officer to ensure appropriate application of rules. Account-level configuration considerations include use of waiting room to control access, use of PIN and password, and limiting screen share and camera control.
- Maintain telehealth endpoint software in accordance with District policies for managing and updating operating system and client software for static and mobile devices.
- IT support staff should have remote connectivity to all telehealth endpoints to provide support for technical issues.
- IT should create and maintain knowledge articles to facilitate quick resolution of common issues.

Information Technology (IT) Connectivity

Current and planned connectivity should be adequate for telehealth. It is recommended that the following extensive testing be conducted once the 100 Mbps line is installed.

1. Load testing
2. Wi-Fi coverage mapping and performance analysis

Provision of Behavioral Health Services to Students in Need

The provision of telehealth behavioral health services should be built on the foundation and best practices for in-person services with attention to HIPAA, FERPA and state law regulations. Specific application depends on who is providing the service, where the documentation is maintained and who is paying for the services. See Appendix H and I.

The more the process is the same as when care is provided in person, the easier it will be to implement. In addition, when the technology is reliable and the staff are well trained, the technology will be a silent partner for providing distant services. The focus will be on the student, rather than the technology.

The attached draft protocol is based on the District Suicide Intervention Process and the District’s other approved processes. (See Appendix J) Staff involved in the provision of behavioral health services to students in need must have the appropriate credentials, and clinical and technical competency. At all times, the therapist should have a telepresenter on site who is accessible and nearby the student. In a crisis situation, the student should also be viewable to the telepresenter.

The Quick Guide for Telehealth Sessions includes good recommendations on facilitating a therapeutic session. It would be helpful to add specifics regarding the actual technology. Another consideration is whether the intent is also to cover the actual clinical protocol.

Implementation steps to provision of services:

1. Review and update service agreements and policies based on regulatory considerations and using the School-based Health Care Support Toolkit as a resource. Include policies related to informed consent, documentation ownership, data sharing, communication, and disclosure of records.
2. Develop and approve Telehealth Standards including Space, Equipment, Competency Expectations and Protocol.
3. Establish technology support plan including reference documents.
4. Establish end user training plan including reference documents.
5. Acquire technology and validate designated environment, technology, and connectivity are ready for telehealth.
6. Schedule clinical and technical training.
7. Complete training and document competency.
8. Conduct practice sessions.
10. Evaluate and refine.
11. Provide refresher training as needed.
Pending OSUWMC Activities

1. Participate in testing the workflow and technology.
2. Provide consultation on arising issues during the planning and set up period. Not responsible for resolving problems.
3. Assist ODM in writing the training manual for the staff personnel and end-user protocol manual.
4. Assist in orienting and training the staff personnel. Trouble shoot problems.

Appendices

A. Originating Site Visit Participants
C. Quick Guide for Telehealth Session
D. Key Staff by Location
E. Telehealth Equipment: Hardware
F. Telehealth Equipment: Zoom Software
G. Telemedicine, privacy, and information security in the age of COVID-19
H. Regulatory Considerations
I. 2019 HIPAA FERPA Joint Guidance
J. Draft Protocol

References

• Practice Guidelines for Telemental Health with Children and Adolescents, The American Telemedicine Association, March 2017
• Best Practices in Videoconferencing-Based Telemental Health, The American Psychiatric Association and The American Telemedicine Association, April 2018
• Practical Considerations in Telebehavioral Health for Ohio Providers
• Telehealth Etiquette Checklist, January 2018
• Checklist for Initiating Telehealth Services, Great Plains Telehealth Resource and Assistance Center
• Program Developer Kit, The California Telehealth Resource Center, 2014
• Telehealth Compendium, Health Resources and Services Administration (HRSA), July 2019
• Telemental Health Guidebook, Department of Defense, 2011
• Facility Guidelines Institute 2018 Guidelines https://fgiguidelines.org/guidelines/purchase-the-guidelines/read-only-copy
Appendix A
Originating Site Visit Participants
Appendix A - Originating Site Visit Participants

October 26
Briana Lusheck - Deputy Director of Children’s Initiatives, Office of Governor Mike DeWine
Beth Ferguson - Department of Mental Health and Addiction Services, Office of Behavioral Health Policy
Tess Hill – SOLSD Director of Information Technology
Corey Stollar – SOLSD Information Technology Technician
John Wooten – Manager, Virtual Health Technology, The Ohio State University Wexner Medical Center
Karen Jackson – Director, Virtual Health, The Ohio State University Wexner Medical Center

<table>
<thead>
<tr>
<th>Site</th>
<th>Contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swiss Hills Career Center</td>
<td>Mark Romick, River AD &amp; Career Tech</td>
</tr>
<tr>
<td>Skyvue Elementary School</td>
<td>Christopher Caldwell, Principal</td>
</tr>
</tbody>
</table>

November 3
Anna Miller - Department of Education; School-Based Health Coordinator; Office of Integrated Student Supports
Briana Lusheck - Deputy Director of Children’s Initiatives, Office of Governor Mike DeWine
Peter Voderberg - Department of Development; Chief, BroadbandOhio; Office of BroadbandOhio
Lydia Brodegard - Director of Special Education, Ohio Valley Educational Service
John Wooten – Manager, Virtual Health Technology, The Ohio State University Wexner Medical Center
Karen Jackson – Director, Virtual Health, The Ohio State University Wexner Medical Center

<table>
<thead>
<tr>
<th>Site</th>
<th>Contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Woodsfield Elementary School</td>
<td>Joshua Ischy, Principal</td>
</tr>
<tr>
<td></td>
<td>Shantel Zwick, Assistant Principal</td>
</tr>
<tr>
<td>Monroe Central High School</td>
<td>Joe Semple, Principal</td>
</tr>
<tr>
<td>Beallsville Schools</td>
<td>Casey Tolzda, Principal</td>
</tr>
</tbody>
</table>

November 6
Anna Miller - Department of Education; School-Based Health Coordinator; Office of Integrated Student Supports
Beth Ferguson - Department of Mental Health and Addiction Services; Office of Behavioral Health Policy
Lydia Brodegard - Director of Special Education, Ohio Valley Educational Service
John Wooten – Manager, Virtual Health Technology, The Ohio State University Wexner Medical Center
Karen Jackson – Director, Virtual Health, The Ohio State University Wexner Medical Center

<table>
<thead>
<tr>
<th>Site</th>
<th>Contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>River Elementary School</td>
<td>Eric James, Principal</td>
</tr>
<tr>
<td></td>
<td>Michele Grant, Assistant Principal</td>
</tr>
<tr>
<td>River High School</td>
<td>Ed Trifonoff, Principal</td>
</tr>
<tr>
<td></td>
<td>Rebekah McVey, Southeast Counselor</td>
</tr>
<tr>
<td>Powhatan Elementary School</td>
<td>-----</td>
</tr>
</tbody>
</table>
Appendix B
Policy & Procedure for Telehealth Practices in Switzerland of Ohio Local School District
Appendix B - Policy & Procedure for Telehealth Practices in Switzerland of Ohio Local School District

Parties involved:
-Switzerland of Ohio Local School District
-South East Healthcare

Locations served:
-Beallsville campus
-Monroe Central High School
-Powhatan Elementary
-River Elementary
-River High School
-Skyvue Elementary
-Swiss Hills Career Center
-Woodsfield Elementary

Process for services:
-Referral form to SE counselor
  -Referral sources:
    -building principal
    -GMN Case Manager
    -Prevention Specialist
    -Behavior Staff
    -School Counselors
    -School Nurses
    -Juvenile Court
    -parent/guardian

South East process once referral obtained:

Application of Telehealth Services
  1. Crisis situation
  2. Ongoing intervention

Identified personal at each building to assist in Telehealth:
*note, these individuals will meet criteria of non-Violence Crisis Intervention training and hold a valid certificate. Individuals will complete IT training with SOLSD IT department for equipment use. Individuals will be cleared to work with all students in crisis and on-going.

-Behavior Department Staff
- Kyle Burkhart, BCBA, Behavior Specialist - Beallsville campus, Powhatan Elementary, River Elementary, River High, Swiss Hills Career Center
- Dustin Fergeson, interim Behavior Specialist - Monroe Central High School, Skyvue Elementary, Swiss Hills Career Center, Woodsfield Elementary
- Chelsea Hogue, Behavior Therapist - Monroe Central High School, Skyvue Elementary, Swiss Hills Career Center, Woodsfield Elementary
- Nicole Kocher, Behavior Therapist - Powhatan Elementary

- Identified Personal at each building
  - Beallsville campus: Carol Clutter, Michele Wells
  - Monroe Central High School: Tanis Langsdorf
  - Powhatan Elementary: Caitlin Brown
  - River Elementary:
  - River High School: Amanda Mahoney
  - Skyvue Elementary:
  - Swiss Hills Career Center:
  - Woodsfield Elementary: Tammie Kernen
  *building principals will also be trained

Crisis situations:
- crisis team is notified, call goes to counselor per district policy.
- identified person(s) secures telehealth area and safety.
- follows the telehealth quick guide to connect to South East counselor
- if in crisis and deemed a safety concern, person should stay in the room with the student.

Ongoing intervention:
- South East counselor communicates scheduled student with school/contact person.
- identified person secures telehealth area and safety.
- no more than 5 minutes before scheduled session, student will be called or escorted to the telehealth area.
- identified person follows the telehealth quick guide to connect to South East counselor
- if not in crisis and safety is secured, person may wait outside the room if the room has a window so student can be in view
Appendix C
Quick Guide for Telehealth Session
Quick Guide for Telehealth Sessions

1. In this unique time, we are collaborating, being innovated, and meeting the needs of our students to the best of our abilities. Take a deep breath, you’ve got this!


3. Software Requirements
   a. OVESC staff members have access to Zoom. While this is not the only HIPPA approved platform, it does have scheduling feature and a secure connection. You can track your sessions via the schedule and other features available for zoom may make your session run smoothly.
   b. If using another platform, make sure you check the Telehealth Guidance for Service Providers.

4. Technology Checklist
   a. Computer, tablet, or phone for you.
   b. Ensure the student has a computer, tablet, or phone to use for your session. If they do not, look at other options for service delivery.
   c. External microphone – if your device does not have one integrated.
   d. External camera - if your device does not have one integrated.
   e. Headphones – if your device does not have adequate speaker quality or you want more privacy with your student.
   f. High speed internet connection
      i. Wi-Fi is compatible with most platforms. If you have a wired connection, connecting your device that way may increase the connection stability.

5. Room space
   a. Check your area for privacy. Place a sign on your door when telehealth session is in progress.
   b. Check your noise level and that around you. Noises may distract your student so refrain from background noise of a TV, music, other conversations in the room.
   c. Check visual distractions. Your background should be free of clutter or items that may grab the student’s attention.
   d. Lighting. Maintain consistent lighting in your area. Avoid a window directly behind you. Make sure your face is not shadowed on the device/camera.
e. **Clothing.** Make sure your clothing contrasts with the background and is not visually busy or distracting to your student. Keeping a solid color sweater/jacket for days your clothing may be busy is a good idea.

f. **Eye contact.** Make sure you display good eye contact with your student. This lets them know you are engaged and they have your attention. While you need to take notes at times, keep the conversation going and let them know what you are doing.

6. **Session prep**
   a. Let your student and parent/guardian know what you are working on that session. Just a quick, “this is what we are doing; this is what materials you may need” can help them be prepared and ready to learn along with you.
   b. Prep your lesson. If you will be doing screen sharing, using videos, whiteboard, etc, have all the links open on your computer so you can easily access them during your session.

7. **Billing**
   a. Remember when entering HBS billing to set the location for telehealth.
   b. Make sure you are using the correct codes for billing. HBS has loaded specific telehealth codes.

8. **Reflect**
   a. Take time to reflect on what worked, what did not, and what you want to accomplish next time. Remember you are making a difference to your student and his/her family!

---

Lydia Brodegard  
Director of Special Education  
Ohio Valley Educational Service Center  
[Lydia.brodegard@ovesc.org](mailto:Lydia.brodegard@ovesc.org)
Appendix D
Key Staff by Location
Appendix D – Key Staff

District Project Lead - Lydia Brodegard **, Director of Special Education, Ohio Valley Educational Service
District IT Project Lead - Tess Hill, Director of Information Technology
District IT Project Support - Corey Stollar, Information Technology Technician

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Casey Tolza, Principal+</td>
<td>Joe Semple**, Principal</td>
<td>Zac Housley+, Principal</td>
<td>Eric James*, Principal</td>
<td>Ed Trifonoff+, Principal</td>
<td>Chris Caldwell*, Principal</td>
<td>Dr. Matt Unger+, Director</td>
<td>Josh Ischy+, Principal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Telehealth Project Leader / Principal</th>
<th>Telehealth Clinical Champion / Behavior Therapist</th>
<th>Telehealth Administrative Leader / Principal</th>
</tr>
</thead>
<tbody>
<tr>
<td>April Parden, Assistant Principal</td>
<td>Lauren Craig*</td>
<td>April Parden, Assistant Principal</td>
</tr>
<tr>
<td>Joe Semple*, Principal</td>
<td>Chelsea Hogue**</td>
<td>Joe Semple**, Principal</td>
</tr>
<tr>
<td>Zac Housley+, Principal</td>
<td>Nicole Kocher*</td>
<td>Zac Housley+, Principal</td>
</tr>
<tr>
<td>Michele Grant*, Assistant Principal</td>
<td>Sarah Smith*</td>
<td>Michele Grant*, Assistant Principal</td>
</tr>
<tr>
<td>Ed Trifonoff+, Principal</td>
<td>Shelly Weese*</td>
<td>Ed Trifonoff+, Principal</td>
</tr>
<tr>
<td>Chris Caldwell*, Principal</td>
<td>Shelly Weese*</td>
<td>Chris Caldwell*, Principal</td>
</tr>
<tr>
<td>Dr. Matt Unger+, Director</td>
<td>Janna Poling*</td>
<td>Dr. Matt Unger+, Director</td>
</tr>
<tr>
<td>Shantel Zwick, Assistant Principal</td>
<td>Chelsea Hogue**</td>
<td>Shantel Zwick, Assistant Principal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Behavior Specialist</th>
<th>School Counselor</th>
<th>Southeast Counselor (Contracted by District)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kyle Burkhart**</td>
<td>Kellee Littlejohn^</td>
<td>Chanda Paczewski</td>
</tr>
<tr>
<td>Dustin Ferguson*</td>
<td>Jenna Rosnick^</td>
<td>Chanda Paczewski</td>
</tr>
<tr>
<td>(Interim)</td>
<td></td>
<td>Chanda Paczewski</td>
</tr>
<tr>
<td>Kyle Burkhart**</td>
<td></td>
<td>Chanda Paczewski</td>
</tr>
<tr>
<td>Kyle Burkhart**</td>
<td></td>
<td>Rebekah McVey</td>
</tr>
<tr>
<td>Kyle Burkhart**</td>
<td></td>
<td>Rebekah McVey</td>
</tr>
<tr>
<td>Kyle Burkhart**</td>
<td></td>
<td>Rebekah McVey</td>
</tr>
<tr>
<td>Dustin Ferguson*</td>
<td></td>
<td>Rebekah McVey</td>
</tr>
<tr>
<td>(Interim)</td>
<td></td>
<td>Rebekah McVey</td>
</tr>
<tr>
<td>Kyle Burkhart**</td>
<td></td>
<td>Chanda Paczewski</td>
</tr>
<tr>
<td>Dustin Ferguson*</td>
<td></td>
<td>Chanda Paczewski</td>
</tr>
<tr>
<td>(Interim)</td>
<td></td>
<td>Chanda Paczewski</td>
</tr>
<tr>
<td>Dustin Ferguson*</td>
<td></td>
<td>Chanda Paczewski</td>
</tr>
<tr>
<td>(Interim)</td>
<td></td>
<td>Chanda Paczewski</td>
</tr>
</tbody>
</table>

Referral sources:
- Building Principal
- Prevention Specialist [Sunessa Tollie^, Jennifer Stutzman ^, Samantha Knuchel^]
- Behavior Staff
- School Counselors
- School Nurses
- GMN Case Manager (outside agency)
  - Cindy Coss- Skyvue; Lisa Carpenter-WES; Kerry Hill-Powhatan; Jana Hutchison-River; Emily Smith-Beallsville
- Juvenile Court (outside agency)
- Parent/Guardian

CPI (Non-violence crisis intervention) trainers – Kyle Burkhart, Lydia Brodegard
* CPI certification current (Behavior Therapists, Behavior Specialists, other identified staff, some principals)
+ CPI certification expired (Some principals)
^ Trained in Mental Health First Aid (Prevention Specialists, School Counselors)
Red – telehealth zoom accounts being created
Appendix E
Equipment: Hardware
Appendix D - Telehealth Equipment: Hardware

1. Recommended Cart Type and Required Functions

**Functional Requirements:**
- capability to hold 32-47" monitor with standard VESA mount
- adjustable shelf
- adjustable height
- locking wheels (ideally with short back legs to allow for positioning close to a wall)

**Installation recommendations**
- Use micro form factor mount from PC manufacturer to mount the PC on the back of the monitor
- conceal and secure all cabling
- mount surge protector to cart for a simple single power connection to wall when needed. Coiled cords work best.
Section 2. Recommended Cart or Wall Mount Height Guide

Section 3. Equipment specifications and examples

**Micro form factor PC**
Micro form factor Windows 10 PC (minimum specifications: Intel i5 processor, 8GB RAM, 128 GB SSD and Intel Iris Graphics, 1 Gbps Ethernet, integrated Wi-Fi (secondary connectivity))

**PTZ Camera**
Zoom Certified USB 3.0 Camera with Pan, Tilt, Zoom function. (minimum specifications: 1080p resolution at 30 fps, smooth motorized pan, tilt and zoom (Pan: ±90° | Tilt: ±35°/45° | 5-15x optical HD zoom), 90° field of view, Autofocus, Video mute/unmute LED indicator, Standard tripod thread)

**Microphone/Speaker array**
Zoom Certified Microphone array (minimum microphone specs: mute button with indicator, full duplex, noise cancellation, echo cancellation, automatic gain control, beamforming technology, range ≥ 4.5m, Frequency response: 90Hz – 16kHz, Sensitivity: >-27dB +/-1dB @ 1Pa) (minimum speaker specifications: Speaker volume 95dB SPL @1W)

*Some camera systems will feature integrated microphone arrays, making a separate array unnecessary. Integrated microphone arrays may be used as long as they meet minimum specifications.*
Appendix F
Equipment: Zoom Software
Video Communications for Telehealth

Increase quality of care and build engagement with modern video communications

**Improve patient outcomes**
Expedite hospital staff and specialist collaboration for patient care with real-time video communications.

**Maximize your resources**
Utilize resources and hardware you already have to expand your capabilities and telehealth offerings.

**Boost internal communications**
Foster collaboration and face-to-face meetings, trainings, and recruiting with participants in any location.

- HD video and audio provide exceptional clarity and quality for telehealth visits.
- Patients may be treated virtually from anywhere, from any device, ensuring timely medical care.
- Consistent high-quality video conferencing, even in low-bandwidth environments.
- Simple user management and single sign-on make video a seamless component of the telehealth experience.

"Other applications don’t allow for multiple members to join in a HIPAA enabled setting, but Zoom does. Now doctor, patient, and family members can be in the conversation."

Dr. Chris Gallagher, MD
Access Physicians

**Compliance and security**
Multi-layer security with AES-256 encryption

**Patient waiting room**
Providers can see who is waiting while maintaining patient privacy.

**Integrate seamlessly with Epic**
Launch a video visit directly from the Epic applications’ telehealth workflows.

**Accessibility for all participants**
Ensure that everyone can participate equitably with closed captioning and keyboard shortcuts.
Recording session review
Save your meetings for consultation and review (local desktop recording with signed BAA to enable HIPAA compliance for clinical application, or in the cloud for non-clinical applications).

Enhanced collaboration features
Collaborate with other doctors and specialists by annotating directly on the shared screen so that notations are visible to all attendees.

Medical device integrations
Examine and treat patients virtually with far-end camera control, EHR and medical device integrations, and in telehealth carts.

What does video-enabled patient care look like? Let’s take a look!

- Ensure timely internal communications between administrative and medical staff across the hospital.
- Telehealth consultations connect physicians, patients, and specialists for regular or urgent care.
- Progressive health education and preventative care for high-risk populations.
- Widespread, immediate coordination and real-time assessment for disaster response.
- Cost-effective continuing education and ongoing training for healthcare professionals.
- Provide virtual behavioral and mental health in 1-1 or group sessions that patients may join from their homes.

“Zoom provides us a secure connection – physician to physician, nurse to nurse, patient to social services.”

Rachel Dunagan
AV Technician
HIPAA Compliance

The Health Insurance Portability and Accountability Act and supplemental legislation collectively referred to as the HIPAA rules (HIPAA) lay out privacy and security standards that protect the confidentiality of protected health information (PHI). In terms of Unified Communication systems, the solution and security architecture must comply with the applicable standards, implementation specifications and requirements with respect to electronic PHI of a covered entity.

The general requirements of HIPAA Security Standards state that covered entities must:

1. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
4. Ensure compliance by its workforce.

How Zoom Enables HIPAA Compliance

In the course of providing services to healthcare customers, the Zoom Platform and Zoom Phone enable HIPAA compliance to covered entities. In provisioning and operating the Zoom HIPAA Services, Zoom complies with the provisions of the HIPAA Security Rule that are required and applicable to it in its capacity as a business associate.

Zoom is responsible for enforcing the administrative, technical and physical safeguards to prevent any unauthorized access to or disclosure of protected health information (PHI) in the Zoom environment.

The following table demonstrates how Zoom supports HIPAA compliance based on the HIPAA Security Rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule).
<table>
<thead>
<tr>
<th>HIPAA Standard</th>
<th>How Zoom Supports the Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control:</strong></td>
<td></td>
</tr>
<tr>
<td>• Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs.</td>
<td>• Data in motion is encrypted at the application layer using Advanced Encryption Standard (AES).</td>
</tr>
<tr>
<td>• Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.</td>
<td>• Multi-layered access control for owner, admin, and members.</td>
</tr>
<tr>
<td>• Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic health information during an emergency.</td>
<td>• Web and application access are protected by verified email address and password.</td>
</tr>
<tr>
<td>• Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.</td>
<td>• Meeting access is password protected by password or waiting room.</td>
</tr>
<tr>
<td>• Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.</td>
<td>• Meetings are not listed publicly by Zoom.</td>
</tr>
<tr>
<td></td>
<td>• Zoom leverages a redundant and distributed architecture to offer a high level of availability and redundancy.</td>
</tr>
<tr>
<td></td>
<td>• Organizations can select data center regions for data in motion to your account. This setting does not affect the data at rest storage location.</td>
</tr>
<tr>
<td></td>
<td>• Meeting host can easily remove attendees or terminate meeting sessions.</td>
</tr>
<tr>
<td></td>
<td>• Host can lock a meeting in progress.</td>
</tr>
<tr>
<td></td>
<td>• Meetings end automatically with timeouts.</td>
</tr>
<tr>
<td></td>
<td>• Privacy features allow you to control session attendee admittance with individual or group entry, waiting rooms, forced meeting test passcodes, and locked room functionality.</td>
</tr>
</tbody>
</table>
**Audit Controls:**
- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- Data in motion traverse Zoom’s secured and distributed infrastructure.
- Platform connections are logged for audio and quality-of-service purposes.
- Account admins have secured access to manage individual, group, or organization level management.

**Integrity:**
- Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
- Multilayer integration protection is designed to protect both data and service layers.
- Controls are in place to protect and encrypt meeting data.

**Integrity Mechanism:**
- Mechanism to authenticate electronic protected health information.
- Application executables are digitally signed.
- Implemented methods to corroborate that information has not been destroyed or altered.
- Data connections leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority.
- Web and application access are protected by verified email address and password.
**Person or Entity Authentication:**
- Verify that the person or entity seeking access is the one claimed.
- Web and application access are protected by verified email and password.
- Meeting host must log in to Zoom using a unique email address and account password.
- Access to desktop or window for screen sharing can be locked by host.
- Privacy features allow session attendee admittance with individual or group entry, waiting rooms, forced meeting passcodes, and locked room functionality.

**Transmission Security:**
- Protect electronic health information that is stored on the Zoom platform.
- Integrity controls: Ensure that protected health information is not improperly modified without detection.
- Data encryption protects against passive and active attacks on confidentiality.
- Data connections leverage TLS 1.2 encryption and PKI Certificates issued by a trusted commercial certificate authority.
- Zoom employs AES 256-GCM encryption for data to protect health information.

---

**Security and Encryption**

Healthcare organizations and account administrators need to have the tools and technology to ensure they’re meeting HIPAA standards. Here are just a few safeguards that enable you to ensure the security and privacy of protected health information (PHI).

- Data in motion is encrypted at the application layer using Advanced Encryption Standard (AES).
- Zoom Chat encryption allows for a secured communication where only the intended recipient can read the secured message. Privacy features allow you to control session attendee admittance with individual or group entry, waiting rooms, forced meeting passcodes, and locked room functionality.
Screen Sharing in Healthcare
Medical professionals and authorized healthcare partners can use Zoom to meet with patients and other healthcare professionals to screen-share health records and other resources. Screen sharing transmits encrypted screen capture mouse and keyboard strokes.

HIPAA Certification
Currently, the agencies that certify health technology – the Office of the National Coordinator for Health Information Technology and the National Institute of Standards and Technology – do “not assume the task of certifying software and off-the-shelf products” (p. 8352 of the Security Rule), nor accredit independent agencies to do HIPAA certifications. Additionally, the HITECH Act only provides for testing and certification of Electronic Health Records (EHR) programs and modules.

Thus, as Zoom is not an EHR software or module, our type of technology is not certifiable by these unregulated agencies. Saying this, Zoom’s HIPAA Attestation was performed by a third party that reviewed and affirmed that Zoom implements the controls needed to secure protected health information (PHI) according to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Breach Notification Rule, and the applicable parts of the Privacy Rule. The Attestation was conducted in compliance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) 18, AT-C sections 105 and 205.

Other Security Certification
SOC2:
The SOC 2 report provides third-party assurance that the design of Zoom, and our internal processes and controls, meet the strict audit requirements set forth by the American Institute of Certified Public Accountants (AICPA) standards for security, availability, confidentiality, and privacy. The SOC 2 report is the de facto assurance standard for cloud service providers.
Appendix G
Telemedicine, privacy, and information security in the age of COVID-19
Correspondence

Telemedicine, privacy, and information security in the age of COVID-19

Mohammad S. Jalali,1,2,3 Adam Landman,1,4,5 and William J. Gordon1,4,6

1Harvard Medical School, Boston, Massachusetts, USA, 2Institute for Technology Assessment, Massachusetts General Hospital, Boston, Massachusetts, USA, 3MIT Sloan School of Management, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA, 4Mass General Brigham, Somerville, Massachusetts, USA, 5Department of Emergency Medicine, Brigham and Women’s Hospital, Boston, Massachusetts, USA, and 6Division of General Internal Medicine and Primary Care, Brigham and Women’s Hospital, Boston, Massachusetts, USA

Corresponding Author: William J. Gordon, MD, MBI, BWH Hospitalist Service, PBB-B4-428, 75 Francis Street, Boston, MA 02115, USA (wjgordon@partners.org)

Received 18 November 2020; Editorial Decision 20 November 2020; Accepted 30 November 2020

The spread of COVID-19 has resulted in unprecedented circumstances that have necessitated a shift toward adopting infrastructure for telemedicine, due in large part to the inaccessibility of traditional care services and high exposure risks of in-person healthcare visits. With the increased strain and demand on traditional medical resources, telemedicine has emerged as an essential component of clinical care delivery and many healthcare organizations are reporting substantial increases in telemedicine use. For example, 1 medical center in New York City saw an increase in urgent care virtual visits from a pre-COVID-19 average of 102 daily to 802 post-COVID-19 expansion (March 2, 2020–April 14, 2020).1

Despite the numerous barriers to telemedicine, such as educating staff, cost, reimbursement, access to broadband, and patient digital literacy, telemedicine has flourished during the pandemic, forcing implementations that may have taken years without such a catalyst. As we continue this shift to telemedicine, new issues and risks unravel that need to be addressed, particularly in regard to information security and privacy, and ongoing work is needed to ensure that our technology infrastructure provides an environment for safe and effective care delivery.

In the US, the Department of Health and Human Services recently lifted several restrictions on communication apps, (eg, allowing the use of popular video conferencing applications, like Apple FaceTime, Facebook Messenger video chat, Google Hangouts, Zoom, and Skype) and increasing the range of services that are billable using telehealth.2 These actions reduced barriers that previously prevented the use of telemedicine services for individuals. Despite these advancements, the substantial information security and privacy concerns surrounding telemedicine cannot be overlooked. For example, Zoom, currently 1 of the most popular video conferencing platforms, has had a 10-fold increase in usage over just a few months including increased use in healthcare, leading to several important privacy considerations, such as intruders joining video conferences or inadequate encryption of communications, leading to the possibility of eavesdropping.

Additionally, governmental agencies have warned of increased risk of cyberattacks towards the healthcare sector and organizations doing research on COVID-19.3 Ransomware attacks—a type of cybersecurity threat that involves encrypting data and demanding payment in return for unencryption—have continued unabated during the pandemic, with many targeting hospitals.4 A recent ransomware attack in Germany led to a patient’s death, perhaps the first death in healthcare directly attributable to a cyberattack. Other recent ransomware attacks have included the Illinois Public Health website and a medical testing facility in the UK.3 Successful cyberattacks negatively impact hospital operations, delay access to clinical services, and lead to significant economic loss, all of which would be devastating to organizations already under extraordinary economic and clinical strain.

Protection against these threats to secure telemedicine platforms is complex, and requires a multi-disciplinary, multi-stakeholder approach. Awareness is an important first step, and can take the form of education, employee training, and simulated cyberattacks (eg, sending fake phishing emails and providing training for those who click) toward establishing a culture of security. Recent research in hospitals shows that among several personal characteristics and or-
ganizational conditions, employees’ workload had the strongest impact on the rate of clicking on phishing links. While extensive emailing of announcements may be needed to keep employees up to date during the pandemic, it could unnecessarily add to workload, putting them at higher risk of clicking on phishing emails. Moreover, best-practice security behaviors must be followed—encrypting data, keeping software updated, running antivirus software, using 2-factor authentication, and following local cybersecurity regulations or recommendations.

While healthcare organizations and ambulatory practices may initially need to use consumer video conferencing tools, they should transition to an enterprise (healthcare specific) video conferencing product. Enterprise grade software versions may include key security features such as encryption and may offer additional configuration settings that can be standardized for the entire organization, such as requiring a waiting room with every teleconference.

Overall, healthcare organizations need to enhance (if not revolutionize) their cybersecurity infrastructure by developing stronger prevention and detection protocols, both administrative and technological. Executives need to be willing to invest fully in cybersecurity throughout the organization. Emerging fields, such as artificial intelligence, the internet of things, and blockchain can also be employed as prevention and detection tools to combat cyber threats more effectively. To leverage these technologies, healthcare organizations need to partner with telemedicine and cybersecurity vendors to understand how to best implement and use their infrastructure and products.

While prevention and detection capabilities are essential, healthcare organizations should be prepared with well-defined response plans. Unfortunately, response plans are often ignored or they are not considered as prevention and detection strategies. Response plans that are tested and practiced are required to minimize the negative consequences of an incident and ensure the provision of safe, secure, and reliable health care operations.

Ultimately, while healthcare systems should allocate significant resources towards improving telemedicine capabilities, it is up to healthcare delivery organizations to ensure that these new capabilities are safe, secure, and protect patient privacy. Balancing the significant privacy and information security concerns with the enormous potential benefits of virtual care during this pandemic will remain a vital component to our continuously evolving response to COVID-19.

FUNDING
None.

REFERENCES
Appendix H – Regulatory Considerations

This communication is not intended to serve as legal advice and is offered for educational purposes only. The information provided should not be used as a substitute for independent legal advice and it is not intended to address every situation that could potentially arise. Please be aware that laws, regulations and technical standards change over time. As a result, it is important to verify and update any reference or information that is provided.

Best practices:

1) Obtain written informed consent from the parent or eligible student to provide a telemedicine visit and to share personally identifiable information (PII) and/or personal health information (PHI). See draft consent form from the School-based health care support toolkit.

2) Develop appropriate data sharing agreements with any necessary third parties for the project. See draft data sharing agreement from the School-based health care support toolkit.

Link to School-based health care support toolkit:

Family Educational Rights and Privacy Act (FERPA): A federal law that protects the privacy of students’ education records. An educational institution subject to FERPA may not disclose education records, or PII from education records, of a student without prior written consent of the parent or the eligible student, unless an exception applies. 20 U.S.C. §§ 1232g (b)(1) and (b)(2); 34 CFR §§ 99.30 and 99.31. Examples of exceptions include: disclosure to teachers and other school officials within the school if these school officials have a legitimate education interest in the records, or disclosure to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health and safety of the student or other individuals. Under FERPA if the PII from a student’s education records is disclosed non-consensually pursuant to the FERPA exception for health or safety emergency, the institution must record in the student’s record the basis for the disclosure and the parties to whom the information was disclosed. 34 CFR § 99.32(a)(5).

It is important to note the definition of “eligible student” as the right to provide consent, among other rights, are transferred from the parent to the eligible student (when the student reaches 18 years or attends a postsecondary institution at any age) 20 U.S.C. §1232g(d); 34 CFR §§ 99.3; and 99.5(a)(1).

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule: The HIPAA privacy rule requires covered entities to protect individuals’ health records and other PHI by requiring appropriate safeguards to protect privacy, and setting limits and conditions on the uses and disclosures that may be made of such information without patient authorization. Where the Privacy Rule applies, it permits covered entities to disclose PHI without patient authorization in situations such as disclosures for treatment, disclosures to family and others
involved in an individual’s care and for notification, disclosures to prevent a serious or imminent threat which includes permission of psychotherapy notes, which otherwise receive special protection. 45 CFR §164.508(a)(2).

FERPA and HIPAA can intersect for example when a school provides health care to students in the normal course of business and is considered a health care provider under HIPAA. If the school as a health care provider transmits PHI electronically in connection with a transaction HHS has adopted a transaction standard, then the school is considered a covered entity under HIPAA. However, if the school’s only health records are considered “education records” or “treatment records” under FERPA, HIPAA rules may not apply. The HIPAA Privacy Rule excludes from its coverage those records protected by FERPA. See Joint Guidance on the Application of HIPAA and FERPA to Student Health Records, December 2019.

Mental Health condition and/or substance abuse use disorder PHI/education records

Generally, HIPAA Privacy rules allows a covered entity to disclose PHI about a minor child to the child’s parent, when the disclosure is consistent with state law. FERPA generally permits the school to disclose PII from education records to the parent of a non-eligible student. HIPAA permits a health care provider to disclose PHI to family members of an adult patient without the patient’s consent, only if the provider perceives a serious and imminent threat to the health and safety of the patient or others and the family members are in a position to lessen the threat. Similarly under FERPA, an eligible student’s education and treatment records may be disclosed, without appropriate consent, only if the disclosure meets one of the exceptions to the FERPA general consent rule. See 20 U.S.C. §§ 1232g(b)(1), (b)(2), (b)(3), (b)(5), (b)(6), (h), (i), and (j); 34 CFR § 99.31.

Additionally, provisions related to 42 CFR Part 2 regulating the disclosure and re-disclosure of substance use disorder information and treatment by federally assisted Part 2 programs should be considered as Part 2 rules provide more stringent privacy protections than HIPAA and FERPA. 42 CFR Part 2 protects student substance abuse use disorder treatment records provided by school and community-based substance abuse use disorder treatment providers. Part 2 requires patient consent for treatment, payment, and healthcare operations. Part 2 permits disclosure of information to medical personnel under certain circumstances without consent during a medical emergency or in other limited situations. The Part 2 regulations at 42 CFR §2.51 specify that when a disclosure is made in connection with a medical emergency, the Part 2 program must document in the patient’s record the name and affiliation of the recipient of the information, the name of the individual making the disclosure, the date and time of the disclosure, and the nature of the emergency [42 CFR § 2.51(c)].

State law

ORC 5122.04 Outpatient services for minors without knowledge or consent of parent or guardian.
ORC 5164.95 Standards for payments for telehealth services. (Medicaid)

OAC 5160-1-18 Telehealth Emergency Rule, Medicaid rules related to telehealth services.

Data Sharing

The Ohio Department of Education has provided guidance on school based health care programs sharing data for program evaluation, if needed. With support from your legal and data teams it is recommended to develop appropriate data sharing agreements to outline the specific terms to share the data, state and federal regulations to govern the data, and technical details to ensure student privacy and data security.

Appendix I
2019 HIPAA FERPA Joint Guidance
Joint Guidance on the Application of the
Family Educational Rights and Privacy Act (FERPA)
And the Health Insurance Portability and
Accountability Act of 1996 (HIPAA)
To Student Health Records

December 2019 Update
(First Issued November 2008)
Contents

I. Introduction................................................................................................................... 3
II. Overview of FERPA ..................................................................................................... 3
III. Overview of HIPAA .................................................................................................. 5
IV. Where FERPA and HIPAA May Intersect ................................................................. 7
V. Frequently Asked Questions and Answers ............................................................... 7-25

Which Rule Applies?
1. Does the HIPAA Privacy Rule apply to an elementary or secondary school?
2. Does FERPA or HIPAA apply to student health records maintained by a health care provider acting for a FERPA-covered elementary or secondary school that is not employed by the school?
3. Does FERPA or HIPAA apply to records on students at health clinics or other health care facilities run by postsecondary institutions?
4. Does FERPA or HIPAA apply to records on students who are patients at a university hospital?
5. Does FERPA or HIPAA apply to the health records of an individual who is both a student and an employee of a university at which the person receives health care?
6. Are all student records maintained by a health clinic within a postsecondary institution considered “treatment records” under FERPA?
7. Can a postsecondary institution be a “hybrid entity” under the HIPAA Privacy Rule?

What Information Can Be Shared?
8. Where HIPAA applies, when an individual reaches the age of majority or becomes emancipated, who controls the protected health information (PHI) concerning health care services rendered while the individual was an unemancipated minor?
9. Where HIPAA applies, when can a health care provider share an adult child’s PHI with a parent if the adult child has not signed an authorization or asked the provider to send a copy of their records to the parent?
10. Where FERPA applies, when can a school disclose an eligible student’s personally identifiable information (PII) from education records to his or her parent if the eligible student has not provided written consent?
11. Does HIPAA allow a health care provider to disclose PHI about a minor child with a mental health condition and/or substance use disorder to the parents of the minor?
12. Does FERPA permit a school to disclose PII from the education records of a student, who is under the age of 18 years and is not attending a postsecondary institution, with a mental health condition and/or substance use disorder to the parents of the student?
13. What options do family members of an adult patient with mental illness have under HIPAA if they are concerned about the patient’s mental health and the patient refuses to agree to let a health care provider subject to HIPAA share information with the family?
14. What options do the parents of an eligible student with mental illness have under FERPA if they are concerned about the student’s mental health and the eligible student refuses to provide consent to permit a school subject to FERPA to share PII from education records with the family?

15. Does HIPAA allow a health care provider to disclose PHI about a student to a school nurse or physician?

16. Does FERPA allow a school official to disclose PII from a non-eligible student’s education records to a third-party health care provider without the written consent of the parent?

17. Does HIPAA allow a parent to access the medical records of his or her deceased child?

18. Does FERPA allow a parent to access the education records of his or her deceased child?

19. Under FERPA, may an eligible student’s treatment records be shared with parties other than treating professionals?

20. When does FERPA permit an eligible student’s treatment records to be disclosed to a third-party health care provider for treatment?

21. Under HIPAA, when can information be shared about someone who presents a serious danger to self or others?

22. Under FERPA, when can PII from a student’s education records be shared, without prior written consent, about someone who presents a serious danger to self or others?

23. Under FERPA, can an educational agency or institution disclose, without prior written consent, PII from a student’s education records, including health records, to the educational agency’s or institution’s law enforcement officials?

24. Does HIPAA permit a covered entity to disclose PHI to a Protection and Advocacy system where the disclosure is required by law?

25. Does FERPA permit an educational agency or institution to disclose PII from a student’s education records to a Protection and Advocacy system?

26. Does HIPAA permit a school-based health care provider to report a student to the National Criminal Background Check System (NICS)?

27. Does FERPA permit an educational agency or institution to disclose, without prior written consent, PII from a student’s education records to the NICS?

VI. Conclusion ........................................................................................................................................25
I. Introduction

The purpose of this guidance is to explain the relationship between the Family Educational Rights and Privacy Act (FERPA) statute and implementing regulations and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. This document updates and expands on prior guidance to help address potential confusion on the part of school administrators, health care professionals, and others on how FERPA and HIPAA apply to records maintained on students. It also addresses certain disclosures that are allowed without the written consent of the parent or eligible student under FERPA or without authorization under the HIPAA Privacy Rule, especially those related to emergency health or safety situations. While this guidance seeks to answer many questions that school officials, parents, and others may have about the intersection of these Federal laws, ongoing discussions may raise additional questions. Contact information for submitting additional questions or suggestions for purposes of informing future guidance is provided at the end of this document. The U.S. Departments of Education and Health and Human Services are committed to a continuing dialogue on these important matters affecting the safety and security of our nation’s schools, students, and communities.

Note: This guidance does not have the force and effect of law and is not meant to bind the public in any way. Instead, it is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

II. Overview of FERPA

FERPA (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of students’ “education records.” FERPA affords parents certain rights with respect to their children’s education records maintained by educational agencies and institutions and their agents to which FERPA applies. These include the right to access their children’s education records, the right to seek to have these records amended, and the right to provide consent for the disclosure of personally identifiable information (PII) from these records, unless an exception to consent applies. See 34 CFR Part 99, Subparts B, C, and D. These rights transfer to the student when the student reaches the age of 18 years or attends a postsecondary institution at any age, thereby becoming an “eligible student” under FERPA. 20 U.S.C. §1232g(d); 34 CFR §§ 99.3 (definition of “eligible student”) and 99.5(a)(1).

FERPA applies to educational agencies and institutions that receive Federal funds under any program administered by the U.S. Department of Education. 20 U.S.C. §§ 1221(c)(1) and 1232g(a)(3); 34 CFR § 99.1(a). If an educational agency or institution receives Federal funds under one or more of these programs, FERPA applies to the recipient as a whole, including each of its components, such as a department within a university. 34 CFR § 99.1(d). The term “educational agency or institution” generally refers to public elementary and secondary schools, school districts, and postsecondary institutions, including medical and other professional schools. Private and religious schools at the elementary and secondary levels generally do not receive funds from the U.S. Department of Education and are, therefore, not subject to FERPA.

An educational agency or institution subject to FERPA may not disclose the education records, or PII from education records, of a student without the prior written consent of a parent or the
student if the student is an “eligible student,” unless an exception applies. 20 U.S.C. §§ 1232g (b)(1) and (b)(2); 34 CFR §§ 99.30 and 99.31. FERPA contains several exceptions to the general consent requirement which are set forth in 20 U.S.C. §§ 1232g(b)(1), (b)(2), (b)(3), (b)(5), (b)(6), (h), (i), and (j), and 34 CFR § 99.31. For example, educational agencies and institutions can disclose PII from a student’s education records, including health and medical information, to teachers and other school officials within the school, without prior written consent, if these school officials have been determined to have “legitimate educational interests” in the education records, pursuant to criteria set forth in the school’s annual notification of FERPA rights. 20 U.S.C. § 1232g(b)(1)(A); 34 CFR §§ 99.7(a)(3)(iii) and 99.31(a)(1)(i)(A). Educational agencies and institutions can also disclose PII from a student’s education records, without prior written consent, to appropriate parties in connection with an emergency, if these parties’ knowledge of the information is necessary to protect the health or safety of the student or other individuals. 20 U.S.C. § 1232g(b)(1)(I); 34 CFR §§ 99.31(a)(10) and 99.36.

The term “education records” is defined to mean, with certain exceptions, those records that are: (1) directly related to a student, and (2) maintained by an educational agency or institution or by a party acting for the agency or institution. 20 U.S.C. § 1232g(a)(4)(A); 34 CFR § 99.3 (definition of “education records”). For instance, a student’s health records, including immunization records, maintained by an educational agency or institution (such as by an elementary or secondary school nurse) would generally constitute education records subject to FERPA.

Records that educational agencies and institutions maintain on children with disabilities, including records of children referred under the Individuals with Disabilities Education Act (IDEA), are also covered as education records under both FERPA and IDEA. IDEA includes confidentiality provisions that are similar to, but broader than, FERPA to protect the privacy of PII in the early intervention or education records of children referred to the IDEA. See 20 U.S.C. §1417(c) and for children ages 3 through 21 the IDEA Part B regulations at 34 CFR §§ 300.610-300.626 and for children with disabilities under the age of three the IDEA Part C regulations at 34 CFR §§ 303.400 – 303.416. The IDEA Part B and C confidentiality provisions contain informed parent consent and notice provisions that are separate from FERPA and permit disclosure of PII without parent consent to officials of participating agencies (as defined separately within the IDEA Part B and C regulations). The IDEA regulations contain additional exceptions and generally incorporate the FERPA exceptions to the prior consent requirements. For a comparison of the FERPA and IDEA confidentiality provisions, please refer to Department technical assistance guidance entitled, “IDEA and FERPA Confidentiality Provisions” available at: https://studentprivacy.ed.gov/resources/ferpaidea-cross-walk.

Under FERPA, “treatment records,” as they are commonly called, are excluded from the definition of “education records.” Treatment records are:

- records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the
student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student’s choice.

20 U.S.C. § 1232g(a)(4)(B)(iv); 34 CFR § 99.3 (definition of “education records”). Assuming certain conditions are satisfied, treatment records may include, for instance, a student’s health or medical records that a college’s psychologist maintains solely in connection with providing treatment to the student. An educational agency or institution may only disclose an eligible student’s treatment records to individuals who are providing treatment to the student (including health care professionals who are not part of, nor acting on behalf of, the educational agency or institution (e.g., third-party health care providers)), and a physician or other appropriate professional of the student’s choice. Id. For all other disclosures of an eligible student’s treatment records, an educational agency or institution must obtain the student’s prior written consent or satisfy one of the exceptions to FERPA’s general written consent requirement, as the records would no longer qualify as “treatment records” (and thereby be excluded from the definition of “education records”) and, instead, become subject to all other FERPA requirements. FERPA’s implementing regulations and other helpful information about FERPA can be found at: https://studentprivacy.ed.gov/resources/family-educational-rights-and-privacy-act-regulations-ferpa.

III. Overview of HIPAA

Congress enacted HIPAA in 1996 to, among other things, improve the efficiency and effectiveness of the health care system through the establishment of national standards and requirements for electronic health care transactions and to protect the privacy and security of individually identifiable health information. Collectively, these are known as the HIPAA Administrative Simplification provisions, and the U.S. Department of Health and Human Services has issued a suite of rules, including the Privacy Rule, to implement these provisions. Entities subject to the HIPAA Administrative Simplification Rules (known as the HIPAA Rules) (see 45 CFR Parts 160, 162, and 164), called “covered entities,” are health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with covered transactions. See 45 CFR § 160.103. “Health care providers” include institutional providers of health or medical services, such as hospitals, as well as non-institutional providers, such as physicians, dentists, and other practitioners, along with any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. Covered transactions are those for which the U.S. Department of Health and Human Services has adopted a standard, such as health care claims submitted to a health plan. See 45 CFR § 160.103 (definitions of “health care provider” and “transaction”) and 45 CFR Part 162, Subparts K–R. Once a health care provider becomes a covered entity, the HIPAA Privacy Rule applies to the individually identifiable health information held by, or on behalf of, the health care provider as a health care provider.

The HIPAA Privacy Rule requires covered entities to protect individuals’ health records and other personal health information the entities maintain or transmit, known as protected health information (PHI), by requiring appropriate safeguards to protect privacy, and setting limits and conditions on the uses and disclosures that may be made of such information without patient
authorization. The rule also gives patients certain rights with respect to their health information, including rights to examine and obtain a copy of their health records, and to request corrections (amendments).

**HIPAA Disclosures that are Relevant in Emergency Situations**

Where the HIPAA Privacy Rule applies, it permits covered entities to disclose PHI without patient authorization in certain circumstances, including emergency or other situations. Examples of such permitted disclosures include:

- **Disclosures for Treatment**: Covered entities may disclose, without a patient’s authorization, PHI about the patient as necessary to treat the patient or to treat another person (who might be, for example, affected by the same emergency situation). Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment. See 45 CFR §§ 164.502(a)(1)(ii), 164.506(c), and the definition of “treatment” at § 164.501.

- **Disclosures to Family, Friends, and Others Involved in an Individual’s Care and for Notification**: Covered entities are permitted to share PHI with family members (or other caregivers) that is directly relevant to the involvement of a family member in the patient’s health care or payment for care if, when given the opportunity, the patient does not object to the disclosure. A covered entity also may share this information with such a family member when the patient is not present—or when it is impracticable, because of emergency circumstances or the patient’s incapacity, for the covered entity to ask the patient about sharing information with a family member—if it determines, in the exercise of professional judgment, that doing so would be in the best interest of the patient. See 45 CFR § 164.510(b).

  A covered entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient’s care, of the patient’s location, general condition, or death. This may include situations where it is necessary to notify family members and others, the police, the press, or the public at large. See 45 CFR § 164.510(b).

- **Disclosures to Prevent a Serious and Imminent Threat**: Health care providers may share PHI with anyone as necessary to prevent or lessen a serious and imminent threat to the health or safety of the individual, another person, or the public – consistent with applicable law (such as State statutes, regulations, or case law) and the provider’s standards of ethical conduct. This permission includes the sharing of psychotherapy notes, which otherwise receive special protection under the Privacy Rule. See 45 CFR § 164.508(a)(2). Thus, without a patient’s authorization or agreement, health care providers may disclose a patient’s health information to anyone who is in a position to prevent or lessen the threatened harm, including family, friends, caregivers, and law enforcement. The HIPAA Privacy Rule expressly presumes the good faith of health care providers in
their determination of the nature and severity of the threat to health or safety and the need to disclose information. See 45 CFR § 164.512(j).

Additional information about how HIPAA permits uses and disclosures for emergency preparedness, planning, and response, is available on OCR’s website at https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html.

IV. Where FERPA and HIPAA May Intersect

In a few limited circumstances, an educational agency or institution subject to FERPA can also be subject to HIPAA. For instance, a school that provides health care to students in the normal course of business, such as through its health clinic, is also a “health care provider” under HIPAA. If a school that is a “health care provider” transmits any PHI electronically in connection with a transaction for which HHS has adopted a transaction standard, it is then a covered entity under HIPAA. As a covered entity, the school’s health care transactions must comply with the HIPAA Transactions and Code Sets Rule (or Transactions Rule).

However, many schools that meet the definition of a HIPAA covered entity do not have to comply with the requirements of the HIPAA Rules because the school’s only health records are considered “education records” or “treatment records” under FERPA. See 45 CFR § 160.103 (definition of “protected health information” ¶¶ (2)(i), (ii)). The HIPAA Privacy Rule specifically excludes from its coverage those records that are protected by FERPA by excluding such records from the definition of “protected health information.”

V. Frequently Asked Questions and Answers

Which Rule Applies?

1. Does the HIPAA Privacy Rule apply to an elementary or secondary school?

Generally, no. In most cases, the HIPAA Privacy Rule does not apply to an elementary or secondary school because the school either: (1) is not a HIPAA covered entity or (2) is a HIPAA covered entity but maintains health information only on students in records that are “education records” under FERPA and, therefore, not PHI covered by the HIPAA Privacy Rule. In some circumstances a private school would be required to comply with the HIPAA Privacy Rule when it is a HIPAA covered entity and not subject to FERPA because it does not receive funds from the U.S. Department of Education. Elementary or secondary schools would fall into one of the following categories:

- **The school is not a HIPAA covered entity.** The HIPAA Privacy Rule only applies to health plans, health care clearinghouses, and those health care providers that transmit health information electronically in connection with certain administrative and financial transactions (“covered transactions”). See 45 CFR § 160.102. Covered transactions are those for which the U.S. Department of Health and Human Services has adopted a standard, such as health care claims submitted to a health plan. See the definition of
“transaction” at 45 CFR § 160.103 and 45 CFR Part 162, Subparts K–R. Thus, even though a school employs school nurses, physicians, psychologists, or other health care providers, the school is not generally a HIPAA covered entity because the providers do not engage in any of the covered transactions, such as billing a health plan electronically for their services. It is expected that most elementary and secondary schools fall into this category.

- **The school is a HIPAA covered entity but does not have PHI.** Even if a school is a covered entity and must comply with the HIPAA Transactions and Code Sets Rules, the school would not be required to comply with the HIPAA Privacy Rule if it only maintains health information in FERPA “education records.” For example, a public high school might employ a health care provider that bills Medicaid electronically for services provided to a student under the IDEA. The school is a HIPAA covered entity because it engages in one of the covered transactions electronically, and therefore, would be subject to the HIPAA transaction standard requirements. However, if the school provider maintains health information only in “education records” under FERPA, the school is not required to comply with the HIPAA Privacy Rule because the Privacy Rule explicitly excludes FERPA “education records.” See 45 CFR § 160.103 (definition of “protected health information,” ¶¶ (2)(i), (ii)). Importantly, although the HIPAA Privacy Rule does not apply, FERPA’s and IDEA’s privacy requirements do apply, including the requirement to obtain prior written parent or eligible student consent (under 20 U.S.C. §§ 1232g(b)(1) and (b)(2) and 34 CFR §§ 99.30, 300.9 and 300.622) to disclose to Medicaid billing information about a service provided to a student.

- **The school is a HIPAA covered entity and is not subject to FERPA.** Schools that are covered entities and are not subject to FERPA must comply with both the HIPAA transaction requirements and the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules regarding any individually identifiable health information the school has about students and others to whom it provides health care. For example, if a private elementary or secondary school not subject to FERPA employs a physician who bills a health plan electronically for the care provided to students (making the school a HIPAA covered entity), the school must comply with the HIPAA Rules regarding the individually identifiable health information of its patients.

- **Certain private school placements.** Where a student is placed in a private school for the provision of Individualized Education Program (IEP) services on behalf of a school or school district subject to FERPA, the education records of the privately placed student maintained by the private school are subject both to FERPA and to the confidentiality requirements under the IDEA, which incorporate the provisions of FERPA, and not the HIPAA Privacy Rule. The U.S. Department of Education is in the process of preparing a Notice of Proposed Rulemaking to amend the FERPA regulations to add this provision and will provide an opportunity for the public to comment on this proposed amendment.

2. Does FERPA or HIPAA apply to student health records maintained by a health care provider acting for a FERPA-covered elementary or secondary school that is not employed by the school?
Health records that directly relate to students and are maintained by a health care provider, such as a third party contractor, acting for a FERPA-covered elementary or secondary school, would qualify as education records subject to FERPA regardless of whether the health care provider is employed by the school.

Conversely, student health records that are maintained by a health care provider that provides services directly to students and that is not acting for a FERPA-covered educational agency or institution do not constitute FERPA-protected education records. For example, the records created and maintained by a public health nurse who provides immunizations to students on a FERPA-covered elementary or secondary school’s grounds, but who is not acting for the school, would not qualify as “education records” under FERPA. (Note: If the school wishes to disclose PII from student education records that it maintains to the public health nurse, the school would have to comply with FERPA and obtain prior written parent or eligible student consent or satisfy an exception to FERPA’s general consent requirement.)

HIPAA would apply to student records maintained by a health care provider that are not subject to FERPA only if the provider transmits any PHI electronically in connection with a transaction for which HHS has adopted a transaction standard, e.g., health care claims, and the records contain PHI.

3. Does FERPA or HIPAA apply to records on students at health clinics or other health care facilities run by postsecondary institutions?

FERPA applies to most public and private postsecondary institutions and, thus, to the records on students maintained by the campus health clinics and other health care facilities operated by such institutions. These records will be either education records or treatment records under FERPA, both of which are excluded from coverage under the HIPAA Rules, even if the school is a HIPAA covered entity. See 45 CFR § 160.103 (definition of “protected health information,” ¶¶ (2)(i), (ii)).

While the health records of students maintained by postsecondary institutions may be subject to FERPA, if the institution is a HIPAA covered entity and provides health care to nonstudents, the individually identifiable health information of the nonstudent patients is subject to the HIPAA Rules. Thus, for example, postsecondary institutions that are subject to both HIPAA and FERPA and that operate clinics or other health care facilities open to staff, the public, or both (including family members of students) are required to comply with FERPA with respect to the health records (i.e., “education records” or “treatment records”) of their student patients, and with the HIPAA Rules with respect to the health records (i.e., PHI) of their nonstudent patients.

4. Does FERPA or HIPAA apply to records on students who are patients at a university hospital?

Patient records maintained by a hospital affiliated with a university that is subject to FERPA are not typically “education records” or “treatment records” under FERPA because university
hospitals generally do not provide health care services to students for the university. Rather, these university hospitals generally provide such services without regard to the person’s status as a student and not on behalf of a university. Assuming the hospital is a HIPAA covered entity, these records are subject to all of the HIPAA Rules, including the HIPAA Privacy Rule. However, in a situation where a hospital does run the student health clinic on behalf of a university, records that the clinic maintains on students would be subject to FERPA, either as “education records” or “treatment records,” and not subject to the HIPAA Rules.

5. Does FERPA or HIPAA apply to the health records of an individual who is both a student and an employee of a university at which the person receives health care?

Health records that directly relate to an individual who is both a student and an employee of a university and that are maintained by the university at which the individual receives health care would be considered “education records” or “treatment records” protected under FERPA; thus, such records would be excluded from coverage under the HIPAA Rules. FERPA defines “education records” as, with certain exceptions, records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution. 20 U.S.C. § 1232g(a)(4)(A); 34 CFR § 99.3 (definition of “education records”). One of the exceptions to this definition of education records excludes certain records relating to employees of the educational agency or institution. To fall within this exclusion, such records must, among other things, relate exclusively to the individual in his or her capacity as an employee. See 20 U.S.C. § 1232g(a)(4)(B)(iii); 34 CFR § 99.3 (definition of “education records”). (Of note, this exclusion also does not apply to records relating to individuals in attendance at the educational agency or institution who are employed as a result of their status as students. 20 U.S.C. § 1232g(a)(4)(B)(iii); 34 CFR § 99.3 (definition of “education records,” ¶ (b)(3)(ii)).) The health records that are maintained by a university as part of its provision of health care to a student who is also an employee of a university would not constitute employment records because the health records would not relate exclusively to the individual in his or her capacity as an employee but also would relate to the individual in his or her capacity as a student. Thus, such records would be covered as education records by FERPA and thus would not be covered by the HIPAA Rules.

6. Are all student records maintained by a health clinic within a postsecondary institution considered “treatment records” under FERPA?

No. Not all records on eligible students that are maintained by a college- or university-run health clinic are treatment records under FERPA because, among other things, many such records are not made, maintained, or used only in connection with the treatment of the students. For example, billing records that a college- or university-run health clinic maintains on a student are not solely made, maintained, and used in connection with the treatment of the student and, therefore, would constitute “education records,” not “treatment records,” under FERPA, the disclosure of which would require prior written consent from the eligible student unless an exception applies. In addition, records relating to the treatment of a student that the college- or university-run health clinic maintains and discloses to persons other than those providing
treatment to the student, or physicians or other appropriate professionals of the student’s choice, are “education records,” not “treatment records,” under FERPA.

7. Can a postsecondary institution be a “hybrid entity” under the HIPAA Privacy Rule?

Yes. A postsecondary institution that is a HIPAA covered entity may have health information to which the Privacy Rule may apply not only in the health records of nonstudents in the health clinic, but also in records maintained by other components of the institution, such as a law enforcement unit or research department, where such records are not education records or treatment records under FERPA. In such cases, the institution, as a HIPAA covered entity, has the option of becoming a “hybrid entity” and, thus, have the HIPAA Privacy Rule apply only to its health care unit. The school can achieve hybrid entity status by designating the health unit as its “health care component.” As a hybrid entity, any individually identifiable health information maintained by other components of the university (i.e., outside of the health care component), such as a law enforcement unit, or a research department, would not be subject to the HIPAA Privacy Rule, notwithstanding that these components of the institution might maintain records that are not “education records” or “treatment records” under FERPA.

To become a hybrid entity, the covered entity must designate and include in its health care component(s) all components that would meet the definition of a covered entity (or business associate) if they were separate legal entities. However, the hybrid entity is not permitted to include in its health care component other types of components that do not perform the covered functions of the covered entity or components that do not perform support activities for the components performing covered functions. That is, components that do not perform health plan, health care provider, or health care clearinghouse functions, and components that do not perform activities in support of these functions (as would a business associate of a separate legal entity) may not be included in a health care component(s). Within the hybrid entity, most of the HIPAA Privacy Rule requirements apply only to the health care component(s), although the hybrid entity retains certain oversight, compliance, and enforcement obligations. See 45 CFR § 164.105 of the Privacy Rule for more information. See also https://www.hhs.gov/hipaa/professionals/faq/522/can-a-postsecondary-institution-be-a-hybrid-entity-under-hipaa/index.html for additional information about hybrid entities under the HIPAA Privacy Rule.

What information can be shared?

8. Where HIPAA applies, when an individual reaches the age of majority or becomes emancipated, who controls the PHI concerning health care services rendered while the individual was an unemancipated minor?

The individual who is the subject of the PHI can exercise, with limited exceptions, all rights granted by the HIPAA Privacy Rule with respect to all PHI about him or her, including information obtained while the individual was an unemancipated minor, consistent with State or other law. Generally, State laws provide that parents are the personal representatives of minor children until such time as the child reaches the age of majority or becomes emancipated. Parents of adult children or emancipated minors generally are not treated as personal representatives and, therefore, cannot exercise the rights of their children under HIPAA. Of
course, any individual can designate a personal representative – which may include a parent – who can exercise rights on his or her behalf.

For example, if parents wanted to provide a specialist with an adult child’s medical records from the family doctor, HIPAA would govern whether the parent could obtain said records from the family doctor. Under the HIPAA Privacy Rule, the parent could provide the doctor with a HIPAA authorization signed by the adult child, or have the adult child exercise the HIPAA right of access to direct the family doctor to send the records to the parent.

9. Where HIPAA applies, when can a health care provider share an adult child’s PHI with a parent if the adult child has not signed an authorization or asked the provider to send a copy of their records to the parent?

HIPAA allows health care professionals to disclose some health information without a patient’s authorization or agreement under certain circumstances, as described below.

- **Caregivers.** When the patient hasn’t objected, and the provider shares health information with a caregiver that is directly related to the caregiver’s involvement in the patient’s health care or payment of care. 45 CFR § 164.510(b).

  For example, an adult child’s family physician conducts a depression screening and believes the adult child shows positive markers for depression. The family physician, adult child, and parent have discussed the potential diagnosis in the past, and the patient did not object to the parent’s presence or participation. The family physician may take into account the parents’ history of involvement in determining that it is in the adult child’s best interests to contact the parents with whom the adult child lives to discuss medical strategies at home.

- **Personal representatives.** A parent who serves as the personal representative of the adult child, or who holds a health care power of attorney or other legal appointment granting control of medical information for the adult child, generally has the right to access the child’s records. 45 CFR § 164.502(g), 45 CFR § 164.524. An exception applies where the covered health care provider has a reasonable belief, based on professional judgment, that the adult child is subject to domestic violence, abuse or neglect by the personal representative, or doing so would otherwise endanger the child. 45 CFR § 164.502(g)(5). The covered health care provider must verify the personal representative’s authority to act on behalf of the adult child before disclosing information. 45 CFR § 164.514(h)(1).

  For example, a parent holds a health care power of attorney for an adult child with serious mental illness. The parent can exercise the HIPAA right of access to obtain the adult child’s records, so long as the health care provider first verifies the parent’s authority (e.g., by viewing a copy of the health care power of attorney documentation).

- **Facility Directories.** Sharing facility directory information about an adult child (i.e., name, location in the facility, and general condition) with a parent or other person who
identifies the adult child by name, if the provider determines that doing so is in the best interests of a patient who is incapacitated or there is an emergency treatment circumstance, provided that the disclosure is consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider. 45 CFR § 164.510(a).

For example, a parent calls the local hospital looking for an adult child who is missing. Hospital staff may inform the parent that the adult child is in serious condition in the intensive care unit if the staff are not aware of any objection the child may have to this disclosure. The level of the parent’s involvement in the adult child’s care does not affect the hospital staff’s ability to disclose this information.

- **Health or Safety Threats.** Informing parents or others in a position to prevent or lessen a serious and imminent threat to the health or safety of the individual, another person, or public, consistent with applicable law and the provider’s standards of ethical conduct. 45 CFR § 164.512(j).

For example, a young man who has reached the age of majority storms out of his therapist’s office stating, “I know where my parents keep their guns.” The therapist believes that the young man is on his way home and may try to use a weapon kept by the parents at home. The therapist may contact the parents, police, or others in a position to help, to warn them that the young man is on the way home and may take a weapon.

10. Where FERPA applies, when can a school disclose an eligible student’s PII from education records to his or her parent if the eligible student has not provided written consent?

Although FERPA provides that the parents’ rights afforded by FERPA transfer to the “eligible student,” FERPA permits an educational agency or institution to share, without applicable prior written consent, PII from the eligible student’s education records with his or her parents under certain circumstances. For example:

- Schools may release PII from an eligible student’s education records to his or her parents, without the consent of the eligible student, if the student is claimed as a dependent for tax purposes under section 152 of the Internal Revenue Code. 20 U.S.C. § 1232g(b)(1)(H); 34 CFR § 99.31(a)(8).

- FERPA permits schools to disclose PII from an eligible student’s education records to his or her parents, without the consent of the eligible student, in connection with a health or safety emergency if the parents’ knowledge of the records is necessary to protect the health or safety of the student or other persons. 20 U.S.C. § 1232g(b)(1)(I); 34 CFR §§ 99.31(a)(10) and 99.36.

- FERPA permits a college or university to inform parents of students under the age of 21 (at the time of disclosure) that the student has violated any law or policy concerning the use or possession of alcohol or a controlled substance if the institution determines that the
student committed a disciplinary violation with respect to that use or possession. 20 U.S.C. § 1232g(i); 34 CFR § 99.31(a)(15).

- Nothing in FERPA prohibits a school official from sharing information with parents that is based on that official’s personal knowledge or observation and that is not based on information contained in an education record. Therefore, FERPA would not prohibit a teacher or other school official from letting a parent know of their concern about the parent’s child that is based on their personal knowledge or observation.

11. Does HIPAA allow a health care provider to disclose PHI about a minor child with a mental health condition and/or substance use disorder to the parents of the minor?

The HIPAA Privacy Rule generally allows a covered entity to disclose PHI about a minor child to the child’s parent, as the minor child’s personal representative, when the disclosure is not inconsistent with State or other law.¹

In some cases, such as when a minor may receive treatment without a parent’s consent under applicable law, the parents are not treated as the minor’s personal representative. See 45 CFR § 164.502(g)(3). In such cases where the parent is not the personal representative of the minor, other HIPAA Privacy Rule provisions may allow the disclosure of PHI about the minor to the parent.

For example, if a provider believes a minor presents a serious danger to self or others, the HIPAA Privacy Rule permits a covered entity to disclose PHI to a parent or other person(s) if the covered entity has a good faith belief that: (1) the disclosure is necessary to prevent or lessen the serious and imminent threat and (2) the parent or other person(s) is reasonably able to prevent or lessen the threat. The disclosure also must be consistent with applicable law and standards of ethical conduct. See 45 CFR § 164.512(j)(1)(i); see also provisions related to 42 CFR Part 2 regulating the disclosure and re-disclosure of substance-use disorder information by Part 2 programs.

For example, a minor makes statements to his physician that he plans to harm himself or others. The HIPAA Privacy Rule permits the physician, including a mental health provider, to contact a parent (or anyone) who the health care provider has a reasonable belief is in a position to lessen or prevent the harm.

12. Does FERPA permit a school to disclose PII from the education records of a student, who is under the age of 18 years and is not attending a postsecondary institution, with a mental health condition and/or substance use disorder to the parents of the student?

Yes. FERPA permits schools to disclose PII from education records to the parent of a student

¹ For more detailed information, see 45 CFR § 164.502(g) and the fact sheets regarding personal representatives at:
- https://www.hhs.gov/sites/default/files/when-your-child.pdf
- https://www.hhs.gov/sites/default/files/am-i-mychilds.pdf
who is not an eligible student. See 34 CFR § 99.31(a)(12). Further, under FERPA, a school must generally provide a parent of a student who is not an eligible student with an opportunity to inspect and review his or her child’s education records within 45 days of the receipt of a request. 20 U.S.C. § 1232g(a)(1)(A); 34 CFR § 99.10(b). While required to provide a parent of a student who is not an eligible student with access to their child’s education records, a school is not generally required by FERPA to provide copies of education records. See 20 U.S.C. § 1232g(a)(1)(A); 34 CFR § 99.10. One of the exceptions in which a school may be required to provide a copy of the education records requested is in the context of a request for access to education records from a parent or student who is not an eligible student where the circumstances would effectively prevent the parent from exercising his or her right to inspect and review education records; in this context, the school would be required to either provide the parent with a copy of the education records requested or make other arrangements that would allow for the parent to inspect and view the requested records. 34 CFR § 99.10 (d). An example of circumstances effectively preventing a parent from inspecting or reviewing education records is where the parent does not live within commuting distance of the school.

13. What options do family members of an adult patient with mental illness have under HIPAA if they are concerned about the patient’s mental health and the patient refuses to agree to let a health care provider subject to HIPAA 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 decision-making 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. See 45 CFR § 164.512(j). Otherwise, under HIPAA, the provider must respect the wishes of the adult patient who objects to the disclosure.

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. A provider can factor that information into the patient’s care, and should the patient later request access to the health record, any such information disclosed under a promise of confidentiality (such as that shared by a concerned family member with the provider), may be withheld from the patient if the disclosure would be reasonably likely to reveal the source of the information. See 45 CFR § 164.524(a)(2)(v). This exception to the patient’s right to access their PHI allows loved ones to disclose relevant health or safety information with providers without fear of disrupting their relationship with the patient.

14. What options do the parents of an eligible student with mental illness have under FERPA if they are concerned about the student’s mental health and the eligible student refuses to provide consent to permit a school subject to FERPA to share PII from education records with the family?

Under FERPA, an eligible student’s education records and treatment records (which constitute education records if made, maintained, or used for any purpose other than the eligible student’s treatment) may be disclosed, without appropriate consent, if the disclosure meets one of the
exceptions to FERPA’s general consent rule. See 20 U.S.C. §§ 1232g(b)(1), (b)(2), (b)(3), (b)(5), (b)(6), (h), (i), and (j); 34 CFR § 99.31. For example, a university physician treating an eligible student might determine that the student’s treatment records should be disclosed to the student’s parents. This disclosure may be made, without consent of the eligible student, if the eligible student is claimed as a dependent under section 152 of the Internal Revenue Code of 1986. 20 U.S.C. § 1232g(b)(1)(H); 34 CFR § 99.31(a)(8). If the eligible student is not claimed as a dependent, the disclosure may be made to the parents if the conditions of any other exception to FERPA’s general requirement of consent are met, such as if the disclosure is in connection with a health or safety emergency and the parents’ knowledge of the records is necessary to protect the health or safety of the eligible student or other persons. 20 U.S.C. § 1232g(b)(1)(I); 34 CFR §§ 99.31(a)(10) and 99.36.

If the exceptions to FERPA’s general consent requirement do not apply and the eligible student refuses to provide written consent for the disclosure, then FERPA would prohibit the school from making the disclosure. However, FERPA would not prevent school officials from listening to the concerns of family members or other care givers, nor preclude a school official from sharing personal observations of the student not based on information contained in the student’s education record.

15. Does HIPAA allow a health care provider to disclose PHI about a student to a school nurse or physician?

Yes. The HIPAA Privacy Rule allows covered health care providers to disclose PHI about students to school nurses, physicians, or other health care providers for several purposes, without the authorization of the student or student’s parent.

HIPAA permits covered entities to disclose PHI for treatment purposes, without the authorization of the student or student’s parent. For example, a student’s primary care physician may discuss the student’s medication and other health care needs with a school nurse who will administer the student’s medication and provide care to the student while the student is at school.

The HIPAA Privacy Rule also permits a covered entity to disclose PHI to a person(s) if the covered entity has a good faith belief that: (1) the disclosure is necessary to prevent or lessen a serious and imminent threat and (2) the parent or other person(s) is reasonably able to prevent or lessen the threat. The disclosure also must be consistent with applicable law and standards of ethical conduct. See 45 CFR § 164.512(j)(1)(i).

For example, a parent tells their child’s therapist they are worried because the child threatened to kill a teacher and has access to a weapon. HIPAA permits the therapist to contact school officials if, based on a credible representation by the parent, the therapist believes the disclosure to school officials is necessary to prevent or lessen a serious and imminent threat to the teacher.

16. Does FERPA allow a school official to disclose PII from a non-eligible student’s education records to a third-party health care provider without the written consent of the parent?
In a couple of cases, yes. First, under FERPA, a school nurse or other school official may disclose PII from a non-eligible student’s education records to the student’s family physician, without the written consent of the parent, where a health or safety emergency exists and the physician’s knowledge of the records is necessary to protect the health or safety of the student or other persons. 20 U.S.C. § 1232g(b)(1)(I); 34 CFR §§ 99.31(a)(10) and 99.36. Additionally, FERPA would permit a school official to verify information that is contained in a record created by a third party with that third party, such as verifying a physician’s note excusing a student’s absence with that physician, as long as other PII from the student’s education records is not disclosed without written consent. See 34 CFR § 99.3 (definition of “disclosure”). This is because the definition of “disclosure” permits a targeted release of information back to the stated source for verification purposes. See id.

17. Does HIPAA allow a parent to access the medical records of his or her deceased child?

HIPAA defers to applicable State laws regarding who qualifies as an individual’s personal representative, and thus who can obtain and make decisions about sharing the individual’s health information upon the individual’s death, when the individual dies without designating a legal personal representative. See 45 CFR § 164.502(g)(4). The parent of a deceased minor child generally is the child’s personal representative.

When a child has reached the age of majority (under State law) before death and has designated a personal representative who is not a parent, a covered entity must obtain authorization from the personal representative before disclosing records to the parent.

18. Does FERPA allow a parent to access the education records of his or her deceased child?

Consistent with common law principles, the U.S. Department of Education interprets the FERPA rights of eligible students to lapse or expire upon the death of the eligible student. Therefore, FERPA would not protect the education records of a deceased eligible student, and an educational agency or institution may disclose such records at its discretion or consistent with State law. However, at the elementary and secondary level, FERPA rights do not lapse or expire upon the death of a non-eligible student because FERPA provides specifically that the rights it affords rest with the parents of students until that student reaches 18 years of age or attends a postsecondary institution. Once the parents are deceased, the records are no longer protected by FERPA.

19. Under FERPA, may an eligible student’s treatment records be shared with parties other than treating professionals?

Under FERPA, treatment records, by definition, are only available to professionals and paraprofessionals providing treatment to the student, or to physicians or other appropriate professionals of the student’s choice. If an educational agency or institution that maintains a student’s treatment records uses or discloses these records for other purposes or to other parties, they are no longer “treatment records,” and become subject to the FERPA requirements concerning “education records.” (As previously explained, any disclosure of “education records”
requires prior written consent of a parent or eligible student or must satisfy one of the exceptions to FERPA’s general consent requirement. See 20 U.S.C. §§1232g(b)(1), (b)(2), (b)(3), (b)(5), (b)(6), (h), (i), and (j); 34 CFR §§ 99.30 and 99.31.)

For example, in order for a physician at a university-operated health clinic treating an eligible student to disclose the student’s treatment records to the student’s parents, the physician would need to either obtain the eligible student’s prior written consent or satisfy one of the exceptions to FERPA’s general consent requirement. Under one such exception, the physician could non-consensually disclose the records to the parents if the eligible student qualified as the parents’ dependent, under section 152 of the Internal Revenue Code of 1986, for Federal income tax purposes. See 20 U.S.C. § 1232g(b)(1)(H); 34 CFR § 99.31(a)(8). The disclosure could also be made, without prior written consent, to parents, as well as other appropriate parties, in connection with a health or safety emergency if the parents’, or other parties’, respective, knowledge of the records was necessary to protect the health or safety of the student or other persons. See 20 U.S.C. § 1232g(b)(1)(I); 34 CFR §§ 99.31(a)(10) and 99.36.

**20. When does FERPA permit an eligible student’s treatment records to be disclosed to a third-party health care provider for treatment?**

An eligible student’s treatment records may be disclosed to individuals who are providing treatment to the student, including health care professionals who are not part of nor acting on behalf of an educational institution (i.e., third-party health care provider), as long as the information is being disclosed only for the purpose of providing treatment to the student. See 20 U.S.C. § 1232g(a)(4)(B)(iv); 34 CFR § 99.3 (definition of “education records,” ¶ (b)(4)(iii)). In addition, an eligible student’s treatment records may be disclosed to a third-party physician or other appropriate professional of the student’s choice. See 20 U.S.C. § 1232g(a)(4)(B)(iv). In either of these situations, if the treatment records are disclosed to a third-party health care provider that is a HIPAA covered entity, the records would become subject to the HIPAA Privacy Rule. The treatment records maintained by the educational institution would continue to be treatment records under FERPA, so long as the records remain unavailable to anyone other than persons providing the eligible student with treatment, or a physician or other appropriate professional of the student’s choice.

If the disclosure is for purposes other than treatment, an eligible student’s treatment record only may be disclosed to a third party as an “education record,” that is, with the prior written consent of the eligible student or if one of the exceptions to FERPA’s general consent requirement is met. For example, if a university is served with a court order requiring the disclosure of the mental health records of a student maintained as treatment records at the campus clinic, FERPA would permit the university to disclose the records to comply with the court order in accordance with the provisions of 20 U.S.C. §§ 1232g(b)(2), and (j) and 34 CFR § 99.31(a)(9). Although FERPA would generally require the university to make a reasonable effort to notify the eligible student in advance of compliance with such a court order so that the eligible student may seek protective action, the university may also wish to take additional measures to protect the privacy of student mental health records, such as obtaining a protective order or filing the records under seal. The university also should determine if the disclosure would comply with all other applicable laws, including any applicable State laws protecting the confidentiality of the mental
health records. Thereafter, these mental health records that the university disclosed for non-treatment purposes would no longer be excluded from the definition of “education records” and, instead, become subject to all other FERPA requirements as “education records” under FERPA.

21. Under HIPAA, when can information be shared about someone who presents a serious danger to self or others?

The HIPAA Privacy Rule permits a covered entity to disclose PHI, including psychotherapy notes, when the covered entity has a good faith belief that the disclosure: (1) is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others and (2) is to a person(s) reasonably able to prevent or lessen the threat. This may include, depending on the circumstances, disclosure to law enforcement, family members, the target of the threat, or others whom the covered entity has a good faith belief can mitigate the threat. The disclosure also must be consistent with applicable law and standards of ethical conduct. See 45 CFR § 164.512(j)(1)(i).

For example, consistent with other laws and ethical standards, a mental health provider whose teenage patient has made a credible threat to inflict serious and imminent bodily harm on one or more fellow students may alert law enforcement, a parent or other family member, school administrators or campus police, or others the provider believes may be able to prevent or lessen the chance of harm. In such cases, the covered entity is presumed to have acted in good faith where its belief is based upon the covered entity’s actual knowledge (i.e., based on the covered entity’s own interaction with the patient) or in reliance on a credible representation by a person with apparent knowledge or authority (i.e., based on a credible report from a family member or other person). See 45 CFR § 164.512(j)(4).

For threats or concerns that do not rise to the level of “serious and imminent,” other HIPAA Privacy Rule provisions may apply to permit the disclosure of PHI. For example, covered entities generally may disclose PHI about a minor child to the minor’s personal representative (e.g., a parent or legal guardian), consistent with State or other laws. See 45 CFR § 164.502(b).

22. Under FERPA, when can PII from a student’s education records be shared, without prior written consent, about someone who presents a serious danger to self or others?

FERPA provides that PII from a student’s education records, including student health records, may be disclosed by educational agencies and institutions to appropriate parties in connection with a health or safety emergency, without the consent of the parent or eligible student, if knowledge of the information is necessary to protect the health or safety of the student or other individuals. 20 U.S.C. § 1232g(b)(1)(I); 34 CFR §§ 99.31(a)(10) and 99.36.

For example, if an eligible student storms out of a teacher’s office stating that, “I know where my parents keep their guns, and someone is going to pay” and the teacher believes that the student is on his way home to and may try to use the weapons, FERPA’s health or safety exception would permit the teacher to contact the parents, police, or others in a position to help, to warn them that the student is on the way home and threatened to use a weapon against others.
Educational agencies and institutions are responsible for making the determination as to whether a health or safety emergency exists. See 34 CFR § 99.36(c). Pursuant to § 99.36(c) of the FERPA regulations, in determining whether it may rely on FERPA’s health or safety emergency exception:

an educational agency or institution may take into account the totality of the circumstances pertaining to a threat to the health or safety of a student of other individuals. If the educational agency or institution determines that there is an articulable and significant threat to the health or safety of the student or other individuals, it may disclose information from education records to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals. If, based on the information available at the time of the determination, there is a rational basis for the determination, the [U.S. Department of Education] will not substitute its judgment for that of the educational agency or institution in evaluating the circumstances and making its determination.

(Emphasis added.) See also 73 Fed. Reg. 74,806, 74,837 (Dec. 9, 2008) (explaining that the U.S. Department of Education amended FERPA’s health or safety emergency exception to add subsection (c) in order to “provide[ ] greater flexibility and deference to school administrators so they can bring appropriate resources to bear on a circumstance that threatens the health or safety of individuals.”).

The U.S. Department of Education discussed the health or safety emergency exception to FERPA’s general consent requirement in some detail in the preamble to the 2008 Federal Register notice implementing changes to the FERPA regulations, 73 Fed. Reg. 74,806, 74,836-74,839 (Dec. 9, 2008), and in guidance entitled “Addressing Emergencies on Campus,” issued in June 2011. In the preamble, the U.S. Department of Education explained that:

the phrase “articulable and significant threat” means that if a school official can explain why, based on all the information then available, the official reasonably believes that a student poses a significant threat, such as a threat of substantial bodily harm, to any person, including the student, the school official may disclose education records to any person whose knowledge of information from those records will assist in protecting a person from that threat.

73 Fed. Reg. at 74,838. The U.S. Department of Education also stated that:

to be “in connection with an emergency” means to be related to the threat of an actual, impending, or imminent emergency, such as a terrorist attack, a natural disaster, a campus shooting, or the outbreak of an epidemic. An emergency could also be a situation in which a student gives sufficient, cumulative warning signs that lead an educational agency or institution to believe the student may harm himself or others at any moment. It does not mean the threat of a possible or eventual emergency for which the likelihood of occurrence is unknown, such as would be addressed in emergency preparedness activities.
Further, in the June 2011 guidance, the U.S. Department of Education explained the following:

In some situations, a school official may determine that it is necessary to disclose [PII] from a student’s education records to appropriate parties in order to address a health or safety emergency . . . This exception to FERPA’s general consent requirement is limited to the period of the emergency and generally does not allow for a blanket release of [PII] from a student’s education records. Typically, law enforcement officials, public health officials, trained medical personnel, and parents (including parents of an eligible student) are the types of appropriate parties to whom information may be disclosed under this FERPA exception. Disclosures for health or safety emergency reasons do not include disclosures to address emergencies for which the likelihood of occurrence is unknown, such as would be the case in emergency preparedness activities.


Finally, where an educational agency or institution non-consensually discloses PII from a student’s education records pursuant to FERPA’s health or safety emergency exception, within a reasonable period of time after the disclosure, the educational agency or institution must record in the student’s education records the articulable and significant threat to the health or safety of the student or other individual(s) that formed the basis for the disclosure, and the parties to whom the information was disclosed. 34 CFR § 99.32(a)(5).

23. Under FERPA, can an educational agency or institution disclose, without prior written consent, PII from a student’s education records, including health records, to the educational agency’s or institution’s law enforcement officials?

Yes, if certain conditions are met. By way of background, many schools have their own law enforcement units to monitor safety and security and enforce any local, State, or Federal law or refer such enforcement matters to appropriate authorities. Those schools that do not have specific law enforcement units may designate a particular office or school official to be responsible for monitoring safety and security and referring potential or alleged violations of law to local authorities. Some smaller school districts and colleges employ off-duty police or sheriff’s department officers to serve as school security officers.

If a law enforcement official is an employee of an educational agency or institution and meets the criteria specified in the school’s annual notification of FERPA rights to parents and eligible students for being a “school official” who has been determined to have a “legitimate educational interest” in the education records, then the law enforcement unit official may be considered a school official to whom PII from students’ education records may be disclosed, without prior written consent of a parent or eligible student. See 20 U.S.C. § 1232g(b)(1)(A); 34 CFR §§ 99.7(a)(3)(iii) and 99.31(a)(1)(i)(A). Educational agencies and institutions may also consider law enforcement unit officials, such as off-duty police or sheriffs’ department officers and School Resource Officers (SROs) who are not employees of the educational agency or institution, to be
“school officials,” to whom PII from student’s education records may be disclosed, without appropriate consent, if the law enforcement unit officials:

1. Perform an institutional service or function for which the educational agencies or institutions would otherwise use employees (for, e.g., to ensure school safety and security);
2. Are under the “direct control” of the educational agencies or institutions with respect to the use and maintenance of the education records (for, e.g., through a memorandum of understanding (MOU) that establishes data use restrictions and data protection requirements);
3. Are subject to FERPA’s use and re-disclosure requirements in 34 CFR § 99.33, which provides that the PII from education records may be used only for the purposes for which the disclosure was made (for, e.g., to promote school safety and the physical security of students), and which limits the re-disclosure of PII from education records; and,
4. Meet the criteria specified in the educational agencies’ or institutions’ annual notification of FERPA rights for being “school officials” who have been determined to have “legitimate educational interests” in the education records.

See 20 U.S.C. § 1232g(b)(1)(A); 34 CFR §§ 99.7(a)(3)(iii) and 99.31(a)(1)(i)(A) and (B)(1)-(3).

In situations where the law enforcement official is not a school official with a legitimate educational interest, the school may only disclose a student’s education records, including health records, to that official with the prior, written consent of the parent or eligible student, unless an exception applies. One such exception that could apply is FERPA’s health or safety emergency exception (discussed in greater detail in Question 21 above). Under this FERPA exception, a student’s education records, including health records, may be disclosed, without the prior written consent of a parent or eligible student, to appropriate parties in connection with an emergency, if knowledge of the information is necessary to protect the health or safety of the student or other individuals. See 20 U.S.C. § 1232g(b)(1)(I); 34 CFR §§ 99.31(a)(10) and 99.36.


24. Does HIPAA permit an educational agency or institution to disclose PHI to a Protection and Advocacy system where the disclosure is required by law?

Yes. Protection and Advocacy (P&A) systems are designated by the governor of each State and territory to protect and advocate for the rights of individuals with disabilities, including by investigating incidents of abuse or neglect. Each P&A system administers multiple P&A programs authorized by Congress through legislation such as the Developmental Disabilities Assistance and Bill of Rights Act (DD Act) (for individuals with developmental disabilities), the
Protection and Advocacy for Individuals with Mental Illness Act (PAIMI Act) (for individuals with mental illness), and section 509 of the Rehabilitation Act of 1973 (Rehabilitation Act) (for certain individuals with disabilities who, for example, are not eligible for P&A services under the DD Act or PAIMI Act). These statutes and their implementing regulations require that access to records be provided to P&A systems under certain circumstances. See DD Act at 42 U.S.C. § 15043(a)(2)(I) and (J), 45 CFR § 1386.22; PAIMI Act at 42 U.S.C. § 10805(a)(4), 42 CFR § 51.41; and the Rehabilitation Act at 29 U.S.C. § 794e(f)(2), 34 CFR § 381.10(a)(2).

The Privacy Rule permits a covered entity to disclose PHI without an individual’s authorization to a P&A system to the extent that such disclosure is required by law and the disclosure complies with the requirements of that law. See 45 CFR § 164.512(a). Thus, a covered entity may disclose PHI to the P&A system, as required by the DD Act, PAIMI Act, or section 509 of the Rehabilitation Act, as well as any other Federal statute authorizing a P&A program, when the P&A system requests access to such records in carrying out its protection and advocacy functions under these Acts. Similarly, covered entities may disclose PHI to the P&A system where another Federal, State, or other law mandates such disclosures, consistent with the requirements in such law.

Where disclosures are required by law, the Privacy Rule’s minimum necessary standard does not apply; instead, the law requiring the disclosure will establish the limits on what should be disclosed. Moreover, with respect to disclosures required by law, a covered entity cannot use the Privacy Rule as a reason not to comply with its other legal obligations.

25. Does FERPA permit an educational agency or institution to disclose PII from a student’s education records to a Protection and Advocacy system?

Yes, in certain circumstances. For instance, an educational agency or institution may disclose PII from a student’s education records to a P&A system, where a parent of a student under 18 and not in attendance at an institution of postsecondary education, or an eligible student, provides prior written consent to disclose such PII to the P&A system. Additionally, as we previously stated in an amici curiae brief jointly filed by the U.S. Departments of Education and Health and Human Services before the U.S. Court of Appeals for the Second Circuit, there are also circumstances in which an educational agency or institution may disclose such PII to the P&A system without obtaining such prior written consent, such as in connection with an emergency under FERPA’s health or safety exception (set forth in 20 U.S.C. § 1232g(b)(1)(I) and 34 CFR §§ 99.31(a)(10) and 99.36), if the P&A system’s knowledge of the PII is necessary to protect the health or safety of the student or other individuals. We noted that “the facts supporting a P&A’s determination that a mentally ill student’s health or safety is in serious jeopardy, see 42 U.S.C. § 10805(a)(4)(C), for example, might also support a school’s determination that an ‘emergency’ existed in which disclosure of [PII from education records] was ‘necessary to protect the health or safety of the student or other persons.’” 20 U.S.C. § 1232g(b)(1)(L).” Id. at 15-16. However, we also recognized that a P&A system’s request for name and contact information might not always satisfy a FERPA exception to the general requirement of consent and that, in those instances where the DD Act, the PAIMI Act, or section 509 of the
Rehabilitation Act conflict with FERPA, “FERPA does not bar a P&A from obtaining access to the name of and contact information for a parent, guardian, or other legal representative of a minor student with a disability or mental illness where the P&A's probable cause determination satisfies the requirements for access to records under the PAIMI Act and the DD Act.” \textit{Id.} at 15-16. We concluded that where the statutes are in conflict, “the specific access provisions of the PAIMI Act and the DD Act (and [section 509 of the Rehabilitation Act] by incorporation) are properly understood as a limited override of FERPA's generally applicable non-disclosure requirements.” \textit{Id.} at 15. We viewed a P&A system’s access to such PII from education records as generally being consistent with Congress’ intent relating to student privacy in part because a P&A system “is required to maintain the confidentiality of any student records it receives, see 42 U.S.C. § 10806(a) …,” such that we saw little risk of the public disclosure of the information that FERPA is intended to prevent. \textit{Id.} at 19-20.

26. \textbf{Does HIPAA permit a school-based health care provider to report a student to the National Instant Criminal Background Check System (NICS)?}

Most likely no. Although HIPAA allows limited disclosures to the National Instant Criminal Background Check System (NICS) by a designated set of covered entities, this permission most likely would not apply to covered entities that operate in the school context.

NICS is maintained by the Federal Bureau of Investigation (FBI) to conduct background checks on persons who may be disqualified from possessing or receiving firearms based on State law or Federal prohibited categories, including those who have been “involuntarily committed to a mental institution” or “adjudicated as a mental defective” (e.g., found incompetent to stand trial). See 27 CFR § 478.11.

HIPAA’s permission to disclose to NICS applies only to covered entities that are: (1) An entity designated by a State to report, or which collects information for purposes of reporting, on behalf of a State, to the NICS; or (2) A court, board, commission, or other lawful authority that makes a commitment or adjudication that causes an individual to become subject to disqualification as described above. For these covered entities, the Privacy Rule allows disclosure of only the limited demographic and certain other information needed for purposes of reporting to NICS and expressly prohibits the disclosure of diagnostic or clinical information for such purposes. See 45 CFR § 164.512(k)(7).

It is unlikely that a school health provider is a HIPAA covered entity designated by a State to report to NICS or given the authority to order a student’s involuntary commitment, but if it is, such a provider could make limited disclosures concerning a student to NICS.

More information can be found online at OCR’s NICS page.

27. \textbf{Does FERPA permit an educational agency or institution to disclose, without prior written consent, PII from a student’s education records to the NICS?}

FERPA permits records of a law enforcement unit of an educational agency or institution, subject to the provisions of 34 CFR § 99.8, to be reported to NICS without obtaining the prior written consent of parents or eligible students because such records are not covered as “education records” under FERPA. Among the exclusions from the definition of “education records” – and
thus from the privacy protections of FERPA – are records of a law enforcement unit of an educational agency or institution. 20 U.S.C. 1232g(a)(4)(B)(ii); 34 CFR § 99.3 (definition of “education records,” subsection (b)(2)). These records must be: (1) created by a law enforcement unit; (2) created for a law enforcement purpose; and (3) maintained by the law enforcement unit. 20 U.S.C. 1232g(a)(4)(B)(ii); 34 CFR § 99.8(b)(1). Law enforcement unit records do not include the following: (1) records created by a law enforcement unit for a law enforcement purpose that are maintained by a component of the educational agency or institution other than the law enforcement unit; or (2) records created and maintained by a law enforcement unit exclusively for a non-law enforcement purpose, such as a disciplinary action or proceeding conducted by the educational agency or institution. 34 CFR § 99.8(b)(2). Under FERPA, “law enforcement unit” means any individual, office, department, division, or other component of an educational agency or institution, such as a unit of commissioned police officers or noncommissioned security guards, that is officially authorized or designated by that agency or institution to (1) enforce any local, State, or Federal law, or refer to appropriate authorities a matter for enforcement of any local, State, or Federal law against any individual or organization other than the agency or institution itself; or (2) maintain the physical security and safety of the agency or institution. 34 CFR § 99.8(a)(1). Therefore, subject to State or local law, educational agencies and institutions may disclose records of a law enforcement unit, as set forth in 34 CFR § 99.8, to anyone, including NICS, without consent from parents or eligible students.

V. Conclusion

While the educational agency or institution has the responsibility to make the initial, case-by-case determination of whether a disclosure meets the requirements of FERPA, the U.S. Department of Education’s Student Privacy Policy Office is available to offer technical assistance to school officials in making such determinations.

For quick, informal responses to routine questions about FERPA, school officials may e-mail the Department at FERPA@ed.gov. For more formal technical assistance on the information provided in this guidance in particular or FERPA in general, please contact the Student Privacy Policy Office at the following address:

Student Privacy Policy Office
U.S. Department of Education
400 Maryland Ave. S.W.
Washington, D.C. 20202-8520

You may also find additional information and guidance on the Department’s website at: https://studentprivacy.ed.gov.

For more information on the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, please visit the U.S. Department of Health and Human Services’ HIPAA Privacy Rule Web site at: http://www.hhs.gov/ocr/hipaa/. The Web site offers a wide range of helpful information about the HIPAA Privacy Rule, including the full text of the Privacy Rule, a HIPAA Privacy Rule summary, over 400 frequently asked questions, and both consumer and covered
entity fact sheets. Information on the other HIPAA Administrative Simplification Rules is available at: http://www.cms.hhs.gov/HIPAAGenInfo/.

In addition, if you would like to submit additional questions not covered by this guidance document or suggestions for purposes of informing future guidance, please send an e-mail to OCRPrivacy@hhs.gov and FERPA@ed.gov.
Appendix J
Draft Protocol
Appendix J – Draft Protocol

Telebehavioral health services shall consist of district-approved counselors using approved synchronous audio video technology to provide behavioral health services in crisis situations or for ongoing intervention to District students or staff. District policies for providing behavioral health services are followed.

District Telepresenter (staff assisting with telebehavioral health services) shall meet the following criteria:
1. Completion of Non-Violence Crisis Intervention training and hold a valid CPI certificate or other have completed other approved training
2. Have HIPAA compliant telehealth platform access
3. Have ready access to counselor
4. Demonstrate competency in telehealth technology and clinical protocol
5. Be cleared to work with all students in crisis and on-going

Counselors providing telebehavioral health services shall meet the following criteria:
1. Contracted to provide counseling services in District
2. Have secure phone and laptop and HIPAA compliant telehealth platform access
3. Have ready access to District Telepresenter
4. Demonstrate competency in telehealth technology and clinical protocol

Telebehavioral Health Processes

<table>
<thead>
<tr>
<th></th>
<th>Crisis Situation</th>
<th>Ongoing Intervention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>The Crisis Team is notified of situation and the Counselor is called per District policy.</td>
<td>The Counselor notifies school contact person of scheduled telebehavioral health session for student</td>
</tr>
<tr>
<td>Preparation</td>
<td>The Crisis Team escorts the student to the telehealth area.</td>
<td>No more than five minutes before the scheduled session, the student will be called or escorted to the telehealth room</td>
</tr>
<tr>
<td>Provision</td>
<td>A crisis team member who is also the telepresenter introduces the student to the Counselor and stays with the student (at the Counselor’s discretion, the telepresenter may remain outside the room but with the ability to view the student at all times).</td>
<td>The Counselor validates the student’s identity. The telepresenter may remain outside the room with the ability to view the student as needed.</td>
</tr>
<tr>
<td>Documentation</td>
<td>The Counselor and District telepresenter communicates via secure text or monitored email, as needed during the session. If there are audio video technical issues, the behavioral health session will be completed via phone.</td>
<td>Documentation includes consent for telebehavioral services and that the session was conducted via HIPAA approved platform. Records are maintained according to District policy</td>
</tr>
<tr>
<td>Follow up</td>
<td>The school, student and parent/caregiver shall be advised of recommended follow up. The telehealth technology is turned off by the telepresenter. Mobile endpoints are returned to the designated storage area and plugged in.</td>
<td></td>
</tr>
</tbody>
</table>