TIPS AND LEADS AND THREATS TO LIFE

FREQUENTLY ASKED QUESTIONS (FAQs)

Global Justice Information Sharing Initiative

This project was supported by Grant No. 2018-DP-BX-K021 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

Frequently Asked Questions
Threat to Life Initiative

DEFINITIONS

1. What is the definition of a "threat to life"?

For purposes of the Threat to Life Initiative, the term "*threat to life*" (TTL) is defined as "an emergency involving danger of death or serious physical injury to any person." See Electronic Communication Privacy Act (ECPA), Voluntary Disclosure of Customer Communications or Records, Title 18 U.S.C. §§ 2702 (b)(8) and (c)(4). TTL information should be viewed as a subset of tips and leads information. TTLs involve:

- A threat to kill or seriously injure others.
- A threat to kill or seriously injure oneself.

Such threats may be imminent or potential. Examples of TTLs include but are not limited to threat to public safety, crisis calls, active shooters, and threats to law enforcement.

2. What is the definition of "tips and leads information"?

"*Tips and leads information or data*" is defined, in part, as "generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident reports (SIR), suspicious activity reports (SAR), and/or field interview reports (FIR) information. However, threat to life (TTL) information and SAR information should be viewed as a subcategory of tip or lead data."[1]

3. What is the definition of "targeted violence"?

The FBI defines "*targeted violence*" as "an incident of violence where an assailant chooses a particular target prior to a violent attack."[2]

4. What is the definition of a "valid law enforcement purpose"?

"*Valid law enforcement purpose*" is defined as:

> A purpose for information/intelligence gathering, development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, protection of public or private structures and property, furthering officer safety (including situational awareness), and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties (P/CRCL) of Americans.[3]
>
> Similar terms may include "reasonable law enforcement purpose," "legitimate law enforcement purpose," and "authorized law enforcement activity."[4]

5. What is the definition of "personally identifiable information" (PII)?

A generally-accepted definition of "*personally identifiable information"* (PII) describes PII as "[i]nformation that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[5] This is the definition

used by the State and Major Urban Area Fusion Centers;[6] federal departments and agencies generally use a similar definition.

Law enforcement entities should be alert to the possibility that an applicable statute or regulation may provide a different definition for PII. For instance, for purposes of the Family Educational Rights and Privacy Act (FERPA), PII contained in "education records" refers to "identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information."[7]

PII is not a defined term in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. Although PII is similar to protected health information (PHI), these terms are not interchangeable.[8]

6. What is the definition of "privacy"?

The term "*privacy*" refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information (PII). Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); and to avoid being seen or overheard in particular contexts.[9]

7. **What is the definition of "civil liberties"?**

According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "*civil liberties*" refers to fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.[10]

8. What is the definition of "civil rights"?

The term "*civil rights*" refers to "those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or other [protected attributes]. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federally or state protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government."[11]

9. What is the definition of a "fusion center"?

A *fusion center* is "[a] collaborative effort of two or more federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." State and major urban area fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners.[12]

10. What is the definition of "need to know"?

As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.[13] This is known as "*need to know*."

11. What is the definition of "right to know"?

"*Right to know*" refers to a requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity or the roles and responsibilities of particular personnel in the course of their official duties.[14]

BEHAVIORAL THREAT ASSESSMENT MANAGEMENT

1. What is behavioral threat assessment management (BTAM)? What is the purpose of BTAM?[15]

School Safety: Gathering Tips and Addressing Threats

A 2021 study of student threat assessment programs in Virginia public K-12 schools recommends the following:

1. There should be a state training requirement for members of a school threat assessment team.

2. The state should improve its training model, placing greater emphasis on negative consequences of exclusionary discipline and recognizing that threat assessment is an alternative to zero-tolerance practices.

3. Schools should provide students, parents and staff an orientation to threat assessment practice and the needs for threat reporting.

4. Schools should provide evidence that they have an active threat assessment team.

5. School divisions should conduct an annual evaluation of the quality of each school's threat assessment practices.

6. Virginia law should provide that threat assessments be conducted for threats against others, and that suicide or self-harm assessments should be conducted for threats against self.

7. The Virginia state school safety audit should restore the practice of collecting sufficient state-level data on all threat assessment cases so that the quality of implementation and equity of impact on student demographic groups can be examined.

For further information, refer to the National Institute of Justice https://nij.ojp.gov/topics/articles/school-safety-research-gathering-tips-and-addressing-threats?utm_campaign=justinfo&utm_medium=email&utm_source=govdelivery.

When utilized as part of a comprehensive violence prevention program, the behavioral threat assessment and management process (BTAM) is viewed as an effective tool for preventing targeted school violence.[16] This proactive approach to violence prevention was pioneered by the U.S. Secret Service (USSS) and has since been adapted to prevent the types of targeted violence that impact communities across the United States. USSS research indicates that school-based BTAM teams should be collaborative and multidisciplinary and should include, as appropriate, law enforcement, behavioral health, school administrators, teachers, and other professionals who are properly trained on how to conduct and manage behavioral threat assessments.[17] When a school establishes a BTAM program, it should clearly state that the primary objective of a school threat assessment is not to administer discipline, but rather to provide interventions and support to students in need.

The multidisciplinary nature of the BTAM team ensures that varying points of view will be represented, a wide range of expertise will be leveraged, and access to information and resources will be broad. Law enforcement and other members of the team may gather and assess information to identify individuals who may be experiencing distress and connect them with the resources and support they need. Some of these individuals may be engaging in behaviors that reasonably indicate a potential for violence and/or self-harm, in which case the BTAM team can identify intervention opportunities to redirect the individual toward more positive outcomes.[18] The BTAM process should be adopted and implemented as a matter of policy in jurisdictions that lack statutorily mandated BTAMs in schools.[19] For further information, refer to *Tips, Leads, and Threats to Life Promising Practices and Success Stories*.

Federal government agencies, including USSS's National Threat Assessment Center (NTAC) and DHS's National Threat Evaluation and Reporting (NTER) Program, the US Department of Education and the Department of Justice, Office Juvenile Justice and Delinquency Prevention have developed numerous resources. Many useful, up-to-date resources are available via the Readiness and Emergency Management for Schools Technical Assistance Center (REMS TA) website.[20]

2. What is behavioral health?

The term "behavioral health" refers to "the promotion of mental health, resilience and wellbeing; the treatment of mental and substance use disorders; and the support of those who experience and/or are in recovery from these conditions, along with their families and communities."[21] Behavioral health is a broad term that encompasses "mental health" and describes the connection between an individual's behaviors and his/her/their health and well-being.

3. Is there a difference between mental health and mental illness?

Yes. "Mental health" refers to an individual's "emotional, psychological, and social well-being. It affects how we think, feel, and act. It also helps determine how we handle stress [and]relate to others…. [*Footnote omitted*] Mental health is important at every stage of life, from childhood and adolescence through adulthood."[22] Every individual will experience struggles or challenges to his/her/their mental health or well-being over the course of a lifetime. These may include instances when a person is overwhelmed, stressed, or suffering a loss. If a person's responses to these situations persists over time and result in functional impairment (e.g., reduced functioning, inability to complete normal tasks), they may contribute to a mental illness diagnosis.

A mental illness is a health condition that can affect thinking, feeling, mood and/or behavior such as depression, anxiety disorder, or bipolar disorder. Mental illnesses can be diagnosed when signs and symptoms have persisted over time and led to functional impairment. A clinician completing a mental health assessment gathers biological, psychological, and social information to make a diagnosis, if appropriate.[23]

4. When or under what circumstances is a mental illness a risk factor for violence?

Mental illness is just one of many factors to consider when assessing whether an individual poses a risk to themselves or others. A diagnosis, standing alone, is ***not*** indicative of threatening behavior or elevated risk for threatening behavior.[24] In fact, studies have shown that "most individuals with serious mental illness are not dangerous, most acts of violence are committed by individuals who are not mentally ill, and people with mental illness are more likely to be victims than perpetrators of violent acts. Nonetheless, individuals with the ***most severe*** psychiatric diseases are at heightened risk for violent behavior when ***untreated*** for their symptoms, especially psychosis with paranoia or 'command hallucinations.'"[25]

Situational factors, such as stressors a person is experiencing, can contribute to elevated risk. Not all negative behaviors can be attributed to mental illness. However, behaviors that may be concerning, regardless of whether they stem from a mental illness, include making threats towards others, escalating anger, unusual interest in weapons,[26] sadness, depression, isolation, drug use, changes in behavior or appearance, suicidal ideation, pronounced interest in violence, blaming others for problems, and grievances.[27] Another factor to consider is nonadherence to mental health treatment, including failure to take prescribed medication.[28]

5. What are the "duty to warn" and the "duty to protect"?

In most jurisdictions, mental health professionals have a legal obligation when they are treating a patient who makes a threat to another person or when they have some reason to believe the patient will harm that person.[29] This obligation may be characterized as a "duty to warn" (i.e., duty to warn an identified victim) or a "duty to protect" (i.e., a duty to take steps to protect the public from violence).[30] Depending on the applicable state statutory law or caselaw, mental health professionals may have the discretion or permission to break patient confidentiality and disclose relevant patient information to local law enforcement (aka "*Tarasoff* reporting") in order to prevent harm to others or to the patient.

State law addressing the scope and nature of this obligation varies from state to state.[31] Law enforcement personnel should therefore be specifically trained on the applicable state requirements addressing the duties of mental health professionals (e.g., whether the obligation in the jurisdiction is codified by statute, established by case law, or non-existent; to whom the law applies; whether it requires an identifiable victim, imminence or certainty; whether the harm must be serious physical harm or death, whether the duty to protect is permissive or mandatory in nature; what required steps must be taken by the professional pursuant to this duty). Additional training should focus on the legal requirements and standard operating procedures governing their response to *Tarasoff* reporting. Law enforcement agencies should also foster relationships with mental health professionals in the community and engage in an ongoing dialogue about the circumstances under which mental health professionals should report threatening behaviors. Law enforcement personnel may find it helpful to remind stakeholders that informed consent is frequently used by mental health professionals to permit *Tarasoff* reporting while mitigating the potential risk of liability.[32]

On a related issue, local law enforcement agencies should also understand the recommended steps they should take if they are notified by their fusion center or the Federal Bureau of Investigation (FBI) of imminent threats to a private citizen located in their jurisdiction or that an address in their jurisdiction has been named online by violent extremists.[33]

For further information, refer to *Tips, Leads, and Threats to Life Promising Practices and Success Stories*.

KEY RESOURCES RELATED TO MASS ATTACKS AND SCHOOL VIOLENCE

1. What resources are available to school resource officers (SROs) and local law enforcement agencies when dealing with an individual who has engaged in concerning behavior(s)?

Local law enforcement may identify an individual in the community who has displayed concerning but not yet criminal behaviors. In these cases, law enforcement professionals should use a multidisciplinary, community-based approach to intervention, ideally as part of a school-based BTAM team. Available resources will vary by location, but law enforcement agencies should be prepared to collaborate with mental health professionals, crisis intervention teams, social services, workplaces, schools, houses of worship, and

other community systems that can provide resources and support for individuals who may pose a risk of harm to self or others, but whose behavior has not reached the level of criminality.[34]

2. What resources has the United States Secret Service developed to address mass attacks and school violence?

The U.S. Secret Service (USSS) National Threat Assessment Center (NTAC) produces operationally relevant research products intended to inform the threat assessment processes of those tasked with public safety. Each year, the NTAC publishes ***Mass Attacks in Public Spaces***, a research series examining targeted attacks that are carried out in public or semi-public spaces and result in harm to three or more people, including attacks in workplaces, public gatherings, houses of worship, and other community locations. The NTAC has also maintained a particular focus on the prevention of targeted school violence. In 2019, the NTAC published *Protecting America's Schools: A U.S. Secret Service Analysis of Targeted School Violence*, which examined 41 attacks perpetrated by current or recently former students at K-12 schools from 2008 to 2017. In 2021, the NTAC's *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools* examined 67 averted school attack plots in which current or recently former students at K-12 schools took steps to advance an attack plan that intended to cause harm but were ultimately stopped. NTAC provides specific operational guidance for schools on how to develop targeted violence prevention programs, in *Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence*. All of these products and more can be accessed at www.secretservice.gov/protection/ntac.

3. What resources has the Federal Bureau of Investigation developed to address mass attacks and school violence?

The Federal Bureau of Investigation has developed resources to address mass attacks and school violence. National Center for the Analysis of Violent Crime (NCAVC) presents a systematic procedure for threat assessment and intervention. The model is designed for use by educators, mental health professionals, and law enforcement agencies. Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks, published in 2017 by the FBI Behavioral Analysis Unit (BAU), NCAVC provides a practical guide on assessing and managing the threat of targeted violence[35] while providing concrete strategies to help communities prevent targeted violence incidents. A Study of the Pre-Attack Behaviors of Active Shooters in the United States Between 2000 and 2013, published by the FBI BAU in 2018, covers active shooter incidents in the United States between 2000 and 2013, and examines specific behaviors that may precede an attack and be useful in identifying, assessing, and managing those who may be on a pathway to violence. Finally, Active Shooter Incidents in the United States in 2020 is a joint product among the FBI's Office of Partner Engagement, Criminal Investigative Division, CIRG, and the Advanced Law Enforcement Rapid Response Training (ALERRT) Center at Texas State University. Published on July 1, 2021, this report details the FBI's designation of 40 shootings in 2020 as active shooter incidents. The FBI defines an active shooter as one or more individuals actively engaged in killing or attempting to kill people in a populated area.

The FBI's Behavioral Threat Assessment Center (BTAC), Behavioral Analysis Unit 1 (BAU-1), Critical Incident Response Group (CIRG), has developed several resource documents that may be useful to practitioners of threat assessment and threat management processes, to include the following: (1) **Data Collection** provides a general list of behavior-related information sets which, if gathered, may be helpful in completing methodical behavioral threat assessments. The product is not intended to be all-inclusive, and portions of it may not be applicable in all situations; (2) **Legal Language Support** offers research to augment testimonials, particularly affidavits in support of search warrants, to demonstrate a more complete

picture of the situation and/or threat posed by a specific person of concern; (3) **Pre-Consultation Guide** offers guidance to help gather information in preparation for a case referral or presentation to a threat assessment team; (4) **Threat Triage and Data Collection** provides triage factors to assist with the initial triage of a threat and to guide appropriate data collection in support of an assessment; and (5) **Warning Signs and Tripwires** offers a general list of targeted violence tripwires and warning signs of which law enforcement should be aware. The list is not necessarily exclusive, and other behaviors of concern may be observable to investigators. For additional information, practitioners should contact their local FBI field office BAU coordinators and/or threat management coordinators.

4. **What is the mission of the Department of Homeland Security National Threat Evaluation Reporting (NTER) and what resources has it developed?**

   The National Threat Evaluation and Reporting (NTER) Program's mission is to strengthen information sharing and enhance Homeland Security partners' ability to identify and prevent targeted violence and mass attacks, regardless of ideology.

   The NTER Program recently launched its forward-facing website. Please visit the NTER website for the latest NTER information.

   The DHS Violence Prevention Resource Guide, published in August 2021, highlights available DHS resources and funding opportunities in the violence prevention space.

5. **Are there any joint products developed by federal partners addressing school emergency operation plans and incorporating lessons learned by incidents of school violence?**

   The Report on Indicators of School Crime and Safety, a joint effort by the National Center for Education Statistics and the Bureau of Justice Statistics, highlights key findings on 22 school crime and safety indicators. While some indicators overlap with risk factors and warning behaviors in threat assessment, such as bullying and carrying a weapon, other indicators portray some unfavorable school conditions, such as gangs, hate-related speech, availability of illegal drugs, and student perceptions of safety. These school environmental indicators may need further examination to determine their impact on an individual's propensity to commit violence.

   In 2013, the U.S. Departments of Education (ED); Justice (DOJ) led by the Federal Bureau of Investigation (FBI); Homeland Security (DHS), led by the Federal Emergency Management Agency (FEMA); and Health and Human Services (HHS), released the *Guide for Developing High-Quality School Emergency Operations Plans (School Guide)*. In 2019, the agencies issued a companion guide entitled, *The Role of Districts in Developing High-Quality School Emergency Operations Plans (District Guide)*. These documents align with and build upon years of school safety work to enhance planning. The *School Guide* and the *District Guide* incorporate lessons learned from incidents and respond to the needs and concerns voiced by stakeholders following recent emergencies. All practitioners with school safety responsibilities (education officials, first responders, planners, elected leadership) are encouraged to use the *School Guide* and the *District Guide* to collaborate as well as create or revise and update existing plans and to align their emergency planning practices with those at the national, state, and local levels.

   To assist local school districts in developing high-quality school emergency operations plans by implementing the *School Guide*'s contents, the Readiness and Emergency Management for Schools (REMS) Technical Assistance Center has developed several resources and training opportunities to make the

guidance easier to learn, understand, and implement. For further information, refer to https://rems.ed.gov/docs/SchoolEOPDevelopment_Resources_508C.pdf.

PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

1. What are the core privacy, civil rights, and civil liberties (P/CRCL) principles that guide the collection, analysis, and dissemination of personally identifiable information (PII)?

Law enforcement entities should have a written P/CRCL policy that articulates how they handle personally identifiable information (PII) and other sensitive information they seek, receive, or use. Civil rights and civil liberties protections should be clearly explained in the P/CRCL policy.[36] The collection, triage, analysis, dissemination, and feedback related to threats to life (TTLs) must adhere to applicable privacy, civil rights, and civil liberties laws, regulations, and policies.[37] For further information about success stories, refer to *Tips, Leads, and Threats to Life Promising Practices and Success Stories*.

2. What are the legal standards for gathering or collecting personally identifiable information (PII)?

Law enforcement can gather or collect PII about individuals ***only*** if they have a valid law enforcement purpose.[38] Valid law enforcement purpose is contextual and differs depending on the type of and uses for the information or intelligence. Examples of valid law enforcement purpose include (but are not limited to):

- A fusion center analyst who reviews, vets, and shares with the responsible local law enforcement agency a report of an individual who is threatening to "kill himself tomorrow."
- An investigator who queries a criminal intelligence system based on her need to know and her agency's right to know the information in the performance of a law enforcement activity.[39]
- An analyst or intake examiner who triages a tip to determine whether a person's behavior or speech poses a concern for significant and imminent violence.[40]

Law enforcement personnel must ensure that the applicable threshold (e.g., reasonably indicative, reasonable suspicion) is met for the particular use of the information or intelligence. For example, a criminal intelligence information (CII) record submitted by a law enforcement officer to a criminal intelligence system subject to 28 C.F.R. Part 23 must meet the "reasonable suspicion" standard (along with the other CII submission criteria) set forth in the regulation.[41] Similarly, a terrorism-related suspicious activity report (SAR)[42] shared by an intelligence analyst in the eGuardian SAR Data Repository should be based on the "reasonably indicative" determination.[43] The applicable thresholds should be set forth in the entity's P/CRCL policy.

Open source information search results containing PII about the subject/victim/witness of a threats to life (TTLs) report can be collected, maintained, and shared if the results are relevant to assisting law enforcement in identifying criminal activity, avoiding self-harm, or furthering officer safety.[44] The entity may conduct threat assessments regarding the threat. As with any information shared, sweeping generalizations and reliance on nonfactual information and opinion should be avoided.

3. What are the basic restrictions for addressing law enforcement activities and the First Amendment?

Gathering information to enforce the criminal law (e.g., threats to others) or to protect individuals from self-harm may come from tip or lead information, visual observation, or other circumstances indicating the possibility that criminal activity has occurred, is occurring, or is being planned. The TTL may be predicated on one of the unprotected categories of speech[45] but it cannot be based solely on speech protected by the First Amendment.[46]

Law enforcement shall not investigate, collect, or maintain information on individuals solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by

the Constitution or laws of the United States. A government entity may collect information about First Amendment activity only when valid and lawful reasons exist for collecting, retaining, or sharing that information (i.e., valid law enforcement purpose).

4. How could the First Amendment apply to TTLs and when should a threat to life (TTL) incident be actioned?

The First Amendment enumerates certain rights held by all Americans: the right to freedom of speech, freedom of religion, freedom of the press, the right to peaceably assemble, and the right to petition the government for redress of grievances.[47]

As a basic rule, an incident alleging a threat to life should not be actioned when it is based solely on First Amendment-protected activity, or is otherwise based solely on the protected attributes of the subject, such as race, ethnicity, national origin, gender, or gender identity.[48] An incident based ***solely or primarily*** on any of these considerations, including one based on lawful political rhetoric, should be purged or archived in accordance with applicable laws, regulations, and policies. Conversely, a TTL that suggests a threat of violence against another person, or otherwise demonstrates a risk of self-harm or suicidal ideation, should be immediately reviewed. If there is a question as to whether an incident includes either a threat or lawful speech, law enforcement officials should rely on their training and experience to analyze the incident based on the totality of the circumstances available. Reviewers may face the challenge of trying to distinguish lawful rhetoric from veiled threats,[49] or separating individuals' statements from group rhetoric.

Online threats inherently involve speech; the question often becomes whether that speech is protected. Another way to think about this issue is to imagine multiple categories of cases. In one category, there may be reported an incident that includes speech, but lacks any indication of self-harm or violence to others. Instead, those incidents include only rhetoric and opinions.[50] The First Amendment would apply to that category.

The second category could be viewed as TTLs involving an incident of self-harm, as reported by either the individual or third parties. The First Amendment is less likely to be influential here because these cases often do not deal with matters of public concern. Examples may include when an individual or third-party report suggests that an act of self-harm may be imminent. If a person reports that he or she is feeling despondent and may take harmful actions, a review and response should expeditiously follow to provide help as quickly as possible. At the same time, respect for the sensitivity of the situation is also important, and such information should be shared with parties only on a "need to know" basis.

Finally, the third category involves threats to others that are either explicitly unprotected speech ("I am going to take these people out") or threats that extend beyond protected speech to express a communicated threat. The context of the speech may indicate that an individual has moved beyond general or abstract advocacy,[51] and has started to conspire, plan, or incite others to take unlawful actions. Reviewers should understand that lawful political rhetoric "may well include vehement, caustic, and sometimes unpleasantly sharp attacks…"[52] The TTLs in the third category should be reviewed considering the situational context and considered actionable based on the reviewer's training and experience.

5. How can First Amendment-protected speech be distinguished from a "true threat"? How does "incitement to imminent lawless action" differ from a "true threat"?

The First Amendment prevents the government from infringing on an individual's ability to speak freely.[53] However, not all speech is protected, such as true threats and incitement to imminent lawless action.[54] To know when a statement is protected speech, social media companies, law enforcement, and intelligence

analysts must know how to distinguish between the two.

A ***true threat*** is defined as a serious expression of an intent to commit an act of unlawful violence to a particular individual or individuals; he need not actually intend to carry out the threat.[55] This "must be distinguished from idle, careless talk, exaggeration, jests, or political hyperbole."[56] To be considered a true threat, a statement must be serious, but also go beyond forceful or repugnant commentary (both of which are protected under the First Amendment, since public issues should be debated in an "uninhibited" and "robust" manner).[57]

In the majority of circuit courts, the test for determining whether a statement is a true threat is the reasonable person standard (would a reasonable person think the statement was a threat?).[58] In addition to the exact wording of the statement, the context in which the communication was made must be considered.[59] Intelligence analysts should weigh the totality of the circumstances:

- Was the statement direct/personal vs. general/open setting?[60]
- What was the recipient's response?[61]
- Does the speaker have a criminal history?[62]
- Are there recent events that may affect the threat landscape?[63]
- What is the relationship or prior contact between threatener and target(s)?[64]
- Does the method of delivery indicate physical proximity by the threatener?[65]
- How many communications were received, by whom, and over what time frame?[66] Were the statements escalating?[67]
- According to the threatener, when will the threatened action or consequence happen?[68]
- What is the significance of any identified dates or places?[69]
- Is the threatened plan of harm feasible, given what is known about the threatener?[70]
- What details are known about any grievance or issue identified in the threat?[71]

> According to the FBI, "in a school setting, conduct on school campuses that either 1) materially disrupts class work, or 2) involves substantial disorder or invasion of the rights of others, does not carry First Amendment protection. In a workplace setting, employees are not entitled to unrestricted speech on any topic; they must be speaking about a matter of "public concern" in order to have First Amendment protection. Simply stated, context matters. The First Amendment has limitations, and courts "will consider time, place, manner of expression, and organizational and individual impact" when deciding whether an expression is protected by the First Amendment." Making Prevention a Reality, at 20 (footnotes omitted).

It is helpful for intelligence analysts and officers to gather as many details/facts as possible to add to the context. This will lead to a more accurate threat analysis and determination of whether a statement is a true threat or protected speech.

Incitement to imminent lawless action is similar to a true threat; both involve unprotected speech, and as such, the First Amendment will not prevent law enforcement entities from acting on them. Incitement to imminent lawless action is a statement in which the speaker intends to incite others to engage in violation of the law that is both imminent and likely.[72] To determine whether speech is such an incitement, courts often apply the "Brandenburg test," which requires an analysis of the following:

- Whether the speaker explicitly or implicitly encourages violence or lawless action;
- Whether the speaker intends his speech to result in the use of violence or lawless action; and
- Whether imminent use of violence or lawless action is the likely result of the speech.

In determining the speaker's intent, criminal intelligence analysts should ask:[73]

- Is there evidence that the speaker knew or should have known how the recipients would react to

the statements? Had they responded violently to similar statements in the past?
- What was the exact statement?
- Did the speaker know that he or she was planning to use violence when making the statements?

6. What constitutes an "emergency involving danger of death or serious physical injury"?

Threats to life (TTL) may be discovered by friends, family members, community members, and/or online platform moderators. Many TTL reports require immediate action and notification to law enforcement to ensure public safety and/or to mitigate the known or perceived threats.

To ensure that TTL reports receive immediate attention by law enforcement, while abiding by the Fourth Amendment's protection against unreasonable searches and seizures, most social media companies reference the Electronic Communication Privacy Act (ECPA), Voluntary Disclosure of Customer Communications or Records.[74] These provisions allow voluntary disclosure of customer information to law enforcement if the "provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency…"[75] Law enforcement only needs an "objectively reasonable basis" for believing that an individual is "seriously injured or threatened with such injury."[76] Law enforcement personnel do not need "ironclad proof of 'a likely serious, life-threatening injury' to invoke this exception."[77] Nor are they required to show that it is "mere moments away."[78] However, they do need to have an ***objectively reasonable basis*** to believe that there is a current, ongoing crisis making it reasonable to act now.[79]

When triaging and handling tips, leads, and TTL information, intelligence analysts and law enforcement officers should use their training and experience in assessing TTLs to stop any injuries before they occur. As such, analysts and officers should err on the side of caution and treat any tips and leads mentioning self-harm or harm to others as urgent. For further information, refer to *Tips, Leads, and Threats to Life Promising Practices and Success Stories*.

7. How should law enforcement entities assess individuals and groups when triaging tip and lead information?

Law enforcement entities must conduct their activities in a nondiscriminatory manner.[80] "Biased practices… are unfair, promote mistrust of law enforcement, and perpetuate negative and harmful stereotypes."[81] Biased practices are also ineffectual and counterproductive.[82] Law enforcement policies and programs therefore restrict the use of race and other protected attributes in their activities. For instance, fusion centers have adopted and implemented policies stating that they will not seek or retain information about individuals or organizations solely on the basis of their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities, or sexual orientations.[83] In addition, some programs such as the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) adhere to federal guidance prohibiting the use of protected attributes as factors creating suspicion (unless they are documented in specific suspect descriptions for identification purposes).[84]

> For information and resources addressing hate crime, refer to the Department of Justice Hate Crimes Resource Home Page, https://www.justice.gov/hatecrimes.

Law enforcement entities must also avoid conflating individuals, and their actions or motivations, with those of their group associations. Individuals in the United States have the constitutional right to associate with whomever they choose.[85] The vetting of a threat to life (TTL) may lead to the development of articulable facts or circumstances that clearly support the determination that the behavior observed is not innocent, but rather reasonably indicative of pre-operational planning associated with terrorism or other criminal activity

that should be submitted as a suspicious activity report (SAR).[86] It may also lead to a criminal investigation based on reasonable suspicion. Reviewers and investigators should understand that law enforcement cannot attribute particular criminal conduct from individuals to groups based merely on their associations. Similarly, law enforcement entities cannot assume that the criminal activity of a particular group or its members automatically includes all of its members, employees, etc.; to do so, law enforcement personnel must articulate that a primary purpose of the group itself is to engage in criminal activity (e.g., the group is an "organization" for purposes of 28 C.F.R. Part 23; criminal enterprise; criminal gang).[87] Factors that may be relevant to the analysis include whether the suspected criminal actions are attributable to individual members within the group or are in furtherance of the group's overall purpose.

8. How should a fusion center handle threat-to-life (TTL) records related to self-harm?

When a State or major urban area fusion center (fusion center) receives a TTL incident related to self-harm, the receiving fusion center should follow its protocols to ensure that the information is appropriately handled. If the receiving fusion center determines that the TTL warrants immediate action, the receiving fusion center should ***immediately forward the information to the responsible local law*** enforcement ***agency*** for: (1) appropriate action and (2) outreach to the impacted school, behavioral health professionals, or other entities.[88] For further information, refer to *Tips, Leads, and Threats to Life Promising Practices and Success Stories*.

Information about self-harm may be considered victim information and as such, it should be treated as sensitive personally identifiable information (PII)**.** Such information should only be shared on a case-by-case basis, in furtherance of an emergency response, and in a manner consistent with statutory authorities. Generally, health records should neither be requested by the receiving fusion center nor provided by the reporting party.[89] If, however, fusion center personnel determine that such records are directly relevant to the threat (e.g., as part of a behavioral threat assessment), they should consult with legal counsel to determine whether they are permitted to obtain the individual's health records.

In addition, the receiving fusion center should remain vigilant about limiting the dissemination of TTL information that relates ***exclusively to self-harm*** for information or intelligence,[90] including sharing with other fusion centers. This information should not be disseminated without a need to know because indiscriminate sharing (i.e., sharing the information beyond those who have the ability to action the information) may result in further victimization.

TTL records related exclusively to self-harm should generally ***not*** be considered or submitted as criminal intelligence information records unless specific articulable facts demonstrate otherwise. [91] The fusion center's response to such an emergency is focused on saving life and sharing the TTL information with appropriate partners to get help for the individual. Fusion centers should therefore evaluate the business need for retaining such records and identify the appropriate retention schedule.

If TTL information is requested pursuant to a public records request, the fusion center should consider all applicable exemptions under state law when determining whether the record may be legally shared.

CRIMINAL JUSTICE INFORMATION

1. **How is criminal justice information (CJI) defined under state law or in applicable federal policy?**

   The CJIS Security Policy, as written by the Federal Bureau of Investigation, defines CJI as "all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data." Criminal History Record Information (CHRI) is a subset of CJI. It is defined as "information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system." 28 C.F.R. § 20.3(d).

2. **What limitations apply to sharing criminal justice information (CJI) with school administrators, mental health professionals, etc.?**

   Generally, criminal justice entities with access to criminal justice information (CJI) will not be able to share such information with noncriminal justice agencies.

   The sharing of a "restricted subset" of CJI known as criminal history records information (CHRI) is more limited in scope. National Crime Information Center (NCIC) restricted files are named specifically in the FBI CJIS Security Policy and are to be treated consistent with the proper access, use, and dissemination policies of criminal history record information or CHRI. The remaining NCIC files not named in Section 4.2.2 are considered non-restricted and the data is not held to higher handling requirements.[92]

   Pursuant to 28 C.F.R. § 20.33(a), CHRI may be shared only with the recipients and for the purposes listed below:

   > **(1)** To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies;
   > **(2)** To federal agencies authorized to receive it pursuant to federal statute or Executive order;
   > **(3)** For use in connection with licensing or employment, pursuant to Public Law 92-544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal law…;
   > **(4)** For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses;
   > **(5)** To criminal justice agencies for the conduct of background checks under the National Instant Criminal Background Check System (NICS);
   > **(6)** To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/ information services for criminal justice agencies; and
   > **(7)** To private contractors pursuant to a specific agreement with an agency identified in paragraphs 28 C.F.R. § 20.33(a)(1) or 28 C.F.R. § 20.33(a)(6) … and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

Law enforcement practitioners should refer to their respective state laws to determine whether ***additional*** pathways for ***sharing in-state CJI*** (e.g., information related to juveniles) are permissible under certain state statutory authorizations.[93]

3. To what extent and under what circumstances are law enforcement entities permitted to report back to key stakeholders on disposition?

Law enforcement entities should refrain from sharing criminal justice information (CJI) (including criminal history record information (CHRI)) with key stakeholders unless they can point to a specific authorization.[94] Instead, law enforcement entities should use CJI or CHRI as a pointer system, accessible for an authorized criminal justice purpose, to then obtain any underlying records. These records may include police reports, court records, or other public records, that may be shared under law. To some extent, this will be dependent on state public records laws.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) PRIVACY RULE

1. Who is required to comply with HIPAA Privacy Rule?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule[95] applies to: health plans; health care clearinghouses; those health care providers (e.g., doctors, psychiatrists, hospitals) that conduct certain health care transactions electronically; and business associates.[96] These are known as covered entities and they must comply with HIPAA regulations.

Many entities that may have health information are ***not*** subject to the HIPAA Privacy Rule, including:

- Most state and local police or other law enforcement agencies.
- Most schools and school districts.
- Many employers.
- Many state agencies such as child protective services.

> Even though an entity may be subject to HIPAA, it is important to understand that HIPAA permits the disclosure of protected health information to law enforcement officials, without the individual's written authorization, under certain circumstances. For further information, refer to *TLTTL Frequently Asked Questions* addressing disclosures to law enforcement under HIPAA.

2. Does the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule apply to an elementary or secondary school?

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 by definition "education records" under the Family Educational Rights and Privacy Act (FERPA) and, therefore, are not subject to the HIPAA Privacy Rule.[97]

For an overview of FERPA and its implications for information sharing in the emergency planning process, refer to Information Sharing: FERPA & HIPAA for Schools and IHEs Webinar - YouTube. This video also includes a brief discussion of the more limited

> While schools and school districts maintain student health records, ***these records are in most cases protected by the*** *Family Educational Rights and Privacy Act* (FERPA) (20 U.S.C. § 1232g) ***and not*** the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. HIPAA may apply, however, to patient records at a university hospital or to the health records of non-students at a university health clinic.

circumstances when HIPAA may apply and have an impact on information sharing in school and higher education settings.

3. **What is protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule?**

   The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."[98]

   "Individually identifiable health information" is "information, including demographic data, collected from an individual that relates to:

   - The individual's past, present or future physical or mental health or condition,
   - The provision of health care to the individual, or
   - The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or [for] which there is a reasonable basis to believe the information can be used to identify the individual."[99]

   Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, social security number).[100]

4. **What is the general principle for uses and disclosures under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule?**

   A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information (PHI), except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[101]

   Under the Privacy Rule, a covered entity ***must disclose*** protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.[102]

5. **When does the HIPAA Privacy Rule permit covered entities to disclose protected health information (PHI) to law enforcement?**

   Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, a covered entity may disclose protected health information (PHI) to law enforcement with the ***individual's signed HIPAA authorization***.

   The Privacy Rule also permits covered entities to disclose PHI to law enforcement officials, ***without the***

individual's written authorization, under certain circumstances, including:[103]

- To report PHI to a law enforcement official reasonably able to prevent or lessen ***a serious and imminent threat to the health or safety of an individual or the public***.[104]
- To report PHI that the covered entity in good faith believes to be ***evidence of a crime that occurred on the premises of the covered entity***.[105]
- To alert law enforcement to the ***death of the individual*** when there is a suspicion that death resulted from criminal conduct.[106]
- When responding to an ***off-site medical emergency***, as necessary to alert law enforcement to criminal activity.[107]

> For further information, refer to the Department of Health and Human Services, Health Information Privacy, Frequently Asked Questions regarding Disclosures for Law Enforcement Purposes.
>
> Helpful handouts addressing the circumstances under which protected health information may be disclosed to law enforcement can be found be found at Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement.

- To report PHI to law enforcement ***when required by law*** to do so (such as reporting gunshots or stab wounds).[108]
- ***To comply with a court order or court-ordered warrant, a subpoena or a summons issued by a judicial officer, or an administrative request from a law enforcement official*** (the administrative request must include a written statement that the information requested is relevant and material, specific and limited in scope, de-identified information cannot be used).[109]
- ***To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person,*** but the information must be limited to basic demographic and health information about the person.[110]
- ***To respond to a request for PHI about an adult victim of a crime when the victim agrees*** (or in limited circumstances if the individual is unable to agree). Child abuse or neglect may be reported, without a parent's agreement, to any law enforcement official authorized by law to receive such reports.[111]

It is critical to understand that the Privacy Rule establishes the ***floor*** of federal privacy protections and individual rights with respect to PHI held by covered entities and their business associates.[112] This means that states may provide ***more stringent*** protections in their laws for such information and afford greater privacy rights for individuals. This also means that a disclosure may be permissible under HIPAA but forbidden under the applicable state law. Consequently, law enforcement entities should consult with legal counsel to ensure that they have a clear understanding of both HIPAA and the applicable state law.

THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) 20 U.S.C. § 1232G; (34 C.F.R. PART 99)

1. **What does The Family Educational Rights and Privacy Act (FERPA) do and to whom does it apply?**

FERPA gives parents the right to access and seek to amend their children's education records.[113] Eligible students have the right to access and seek to amend their own education records.

- FERPA protects personally identifiable information (PII) from education records from unauthorized disclosure.
- It requires the written consent of the parent or "eligible student" before sharing PII—unless an exception applies.

FERPA applies to elementary, secondary, and post-secondary providers of education that receive funds from the United States Department of Education.[114]

For an overview of FERPA and its implications for information sharing in the emergency planning process, refer to Information Sharing: FERPA & HIPAA for Schools and IHEs Webinar - YouTube. This video also includes a brief discussion of the more limited circumstances when HIPAA may apply and have an impact on information sharing in school and higher education settings.

2. **Does The Family Educational Rights and Privacy Act (FERPA) or Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule apply to records on students at health clinics run by postsecondary institutions?**

   FERPA applies to most public and private postsecondary institutions and, thus, to the records on students at the campus health clinics of such institutions. These records will be either education records or treatment records under FERPA, both of which are excluded from coverage under the HIPAA Privacy Rule, even if the school is a HIPAA covered entity.[115]

3. **What records are covered under The Family Educational Rights and Privacy Act (FERPA)?**

   "Education records" are 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.

4. **Does The Family Educational Rights and Privacy Act (FERPA) permit educational institutions to disclose education records in the event of an emergency?**

   Education records (or personally identifiable information contained therein) may be disclosed in an emergency if disclosure is ***necessary*** to protect the health or safety of the student or others, or if there is an articulable and significant threat to the health or safety of a student or other individuals.[116] However, the educational institution must record pertinent information when it discloses Personally Identifiable Information.[117]

5. **Are records maintained by a school resource officer or other law enforcement officer considered "education records" under The Family Educational Rights and Privacy Act (FERPA)?**

   Records maintained by a law enforcement unit do ***not*** require consent for disclosure. "Law enforcement unit" means "any individual, office, department, division, or other component of a school that is officially authorized or designated by the school to (1) enforce any local, state, or federal law, or to refer to appropriate authorities a matter for enforcement of any law against any individual or organization other than the school itself; or (2) to maintain the physical security and safety of the school."

6. **What exactly are law enforcement unit (LEU) records?**

   The law enforcement unit (LEU) records, files, documents, and other materials that are covered include:
   - Created by a law enforcement unit;
   - Created for a law enforcement purpose; and
   - Maintained by the law enforcement unit.[118]

   LEU records do not include:
   - Records created by a LEU for a law enforcement purpose that are maintained by another component of the school.
   - Records created and maintained by a LEU exclusively for a non-law enforcement purpose, such as a disciplinary action or proceeding conducted by the school.[119]

7. Are there other records that school officials may have that are not considered education records?

Records created by school officials for their personal use that they keep entirely to themselves, without any intention of sharing with anyone, except someone substituting for them, are not "education records."[120]

8. Are school health professionals' records education records?

As a general rule, school health professionals' records are considered ***education records*** for purposes of **The Family Educational Rights and Privacy Act (FERPA).**[121] As such, they are subject to the same exceptions regarding consent/notice as every other type of educational record.

However, school health records are not considered education records when the following criteria are met:

- The student must be 18 years of age or older, or attending a postsecondary school;
- The records must be made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in a professional or paraprofessional capacity, or assisting in that capacity;
- The records are made, maintained, or used only in connection with the provision of treatment to the student; ***and***
- The records are not available to anyone other than persons providing treatment, except the treatment records can be personally reviewed by a physician or other appropriate professional of the student's choice.[122]

9. Is a student's activity on social media, even if using school computers, an education record under The Family Educational Rights and Privacy Act (FERPA)?

Social media posts that can be viewed by the public are not education records. If a school official creates a record for himself or herself regarding a student's threats of violence shared on social media platforms (whether this record is based on his/her own observations or reports to the official by other students), the record is not an education record.[123]

10. Under what circumstances does The Family Educational Rights and Privacy Act (FERPA) require written consent for the disclosure of education records? Are there any exceptions?

Generally, a parent or an eligible student shall provide a signed and dated written consent before a school may disclose education records. The consent must:

- Specify the records that may be disclosed;
- State the purpose of disclosure; and
- Identify the party or class of parties to whom the disclosure may be made.[124]

Education records may be lawfully disclosed ***without consent***, in the following circumstances:[125]

- A school may disclose personally identifiable information (PII) from education records necessary to comply with a ***judicial order or lawfully issued subpoena***. However, the school must make a reasonable effort to notify the parent or eligible student of the order or subpoena before complying with it to allow parent or eligible student the opportunity to seek a protective action. In some cases, judicial orders and subpoenas are exempt from FERPA's notification requirement.
- A school may disclose, without consent or knowledge of student or parent, PII from education records to the U.S. Attorney General or his or her designee in response to an ***ex parte order*** in connection with the investigation or prosecution of terrorism crimes specified in 18 U.S.C. §§ 2332b(g)(5)(B) and 2331.

- The school may be ordered to disclose PII from education records to the entity or persons designated in a ***subpoena issued for a law enforcement purpose*** and the issuing court or agency may, for good cause shown, order the institution not to disclose to anyone the existence or contents of the subpoena or the response. If the court issues such an order, the notification requirements in FERPA do not apply.
- The school may disclose PII from education records to the entity or persons designated in a ***federal grand jury subpoena***. The court may order the institution not to disclose to anyone the existence or contents of the subpoena or the response. If the court orders, the notification requirements in FERPA do not apply.

11. Does The Family Educational Rights and Privacy Act (FERPA) have an exception for "directory information"? If so, what does that include?

Consent and notification are not required to obtain directory information.[126] The term "directory information" refers to "[i]nformation in a student's education records that would not generally be considered harmful or an invasion of privacy." This generally includes the following:

- Name, address, telephone number, email address, photograph, and date and place of birth; grade level, major field of study, and dates of attendance (e.g., year or semester); participation in officially recognized sports and activities; height and weight of athletes; degrees, honors, and awards received; and most recent school attended.

Directory information can never include a social security number, and it generally may not include student identification number, except under specified circumstances.[127]

[1] *Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template (Fusion Center P/CRCL Template)* (March 2019), at 44. For further information about tips and leads information, refer to Promising Practices document.
[2] The Federal Bureau of Investigation, Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks (Making Prevention a Reality), at 11.
[3] National Network of Fusion Centers (NNFC), Office of the Director of National Intelligence's (ODNI) Office of Partner Engagement-Information Sharing Environment (PE-ISE), U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Criminal Intelligence Coordinating Council (CICC), *Real-time and Open Source Analysis Resource Guide* (ROSA Resource Guide), 32 (July 2017).
[4] *Face Recognition Policy Development Template for Use in Criminal Investigations*, at 48 (December 2017) and n.41 (December 2017), citing *the Attorney General's Guidelines For Domestic FBI Operations*, (using a similar term, "authorized law enforcement activity") (*citations omitted*).
[5] *Fusion Center P/CRCL Policy Template,* at 41, citing the Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016.
[6] *Fusion Center P/CRCL Policy Template,* at 41, citing the Revised OMB Circular A-130, at 3 and n.2.
[7] See U.S. Department of Education, Privacy Technical Assistance Center, Frequently Asked Questions, Personally Identifiable Information for Education Records, citing Family Educational Rights and Privacy Act Regulations, 34 C.F.R. § 99.3 for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII. Additional information is available in Protecting Student Privacy While Using Online Educational Services.
[8] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191(August 21, 1996). Summary of the HIPAA Privacy Rule | HHS.gov.
[9] *Fusion Center P/CRCL Policy Template,* at 41.
[10] Id. at 36.
[11] Id.
[12] Id. at 38, quoting Section 511 of the 9/11 Commission Act.
[13] Id. at 40.
[14] Id. at 42.
[15] Virginia Department of Criminal Justice Services, Virginia Center for School and Campus Safety, Threat Assessment and Management in Virginia Public Schools: Model Policies, Procedures, and Guidelines (rev. 2020) -
- https://www.dcjs.virginia.gov/sites/dcjs.virginia.gov/files/publications/law-enforcement/threat-assessment-model-policies-procedures-and-guidelinespdf_0.pdf and Behavioral Threat Assessment and Management for Educators and Administrators | Texas School Safety Center (txstate.edu) https://txssc.txstate.edu/tools/tam-toolkit/.
[16] United States Secret Service (USSS), National Threat Assessment Center (2021) *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools.* U.S. Secret Service, Department of Homeland Security. United States Secret Service and United States Department of Education, THE FINAL REPORT AND FINDINGS OF THE SAFE SCHOOL INITIATIVE: IMPLICATIONS FOR THE PREVENTION OF SCHOOL ATTACKS IN THE UNITED STATES (2004); Bryan Vossekuil; Robert A. Fein, Ph.D.; Marisa Reddy, Ph.D.; Randy Borum, Psy.D; William Modzeleski, Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States (2002).
[17] National Threat Assessment Center. (2019). *Protecting America's Schools: A U.S. Secret Service Analysis of Targeted School Violence*. U.S. Secret Service, Department of Homeland Security.
[18] Alternatives to formal charges including restorative justice programs, referrals to mental health professionals, and available community services are important to consider in each incident. The purpose is to redirect and support a juvenile, not to punish the juvenile. How to achieve that will look different in every case.
[19] See U.S. Department of Homeland Security, United States Secret Service, National Threat Assessment Center, *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools,* (2021), USSS Averting Targeted School Violence.2021.03.pdf (secretservice.gov); U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, School Safety: Research on Gathering Tips and Addressing Threats (April 2021), School Safety: Research on Gathering Tips and Addressing Threats | National Institute of Justice (ojp.gov); U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, School Safety: Research on Gathering Tips and Addressing Threats (April 2021), School Safety: Research on Gathering Tips and Addressing Threats | National Institute of Justice (ojp.gov) -- https://nij.ojp.gov/topics/articles/school-safety-research-gathering-tips-and-addressing-threats?utm_campaign=justinfo&utm_medium=email&utm_source=govdelivery
[20] In addition to the resources available from the federal government, professional associations such as the Association of Threat Assessment Professionals (ATAP) and ASIS International that offer BTAM training to public and private sector entities.
[21] SAMHSA – Behavioral Health Integration, available at https://www.samhsa.gov/sites/default/files/samhsa-behavioral-health-integration.pdf. For information about sharing behavioral health information, refer to the U.S. Department of Justice Bureau of Justice Assistance and the Council of State Governments, Sharing Behavioral Health Information: Tips and Strategies for Police-Mental Health Collaborations (October 2019), https://csgjusticecenter.org/projects/police-mental-health-collaboration-pmhc/sharing-

behavioral-health-information/; U.S. Department of Justice Bureau of Justice Assistance and the Council of State Governments, Information Sharing in Criminal Justice-Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (2010), https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/CSG_CJMH_Info_Sharing.pdf.

[22] Centers for Disease Control and Prevention, About Mental Health.

[23] For further information about the currently recognized categories of mental health disorder, refer to the American Psychiatric Association, *Diagnostic and Statistical Manual of Mental Disorders* (*DSM–5*).

[24] Tori DeAngelis, Mental illness and violence: Debunking myths, addressing realities (apa.org) Vol. 52, No. 3 (April 1, 2021).

[25] Treatment Advocacy Center (consolidating the findings of several studies) (*emphasis added*); see also Desmarais, S.L., Van Dorn, R.A., Johnson, K.L., Grimm, K.J., Douglas, K.S., & Swartz, M.S., Am. J. Public Health, *Community Violence Perpetration and Victimization Among Adults with Mental Illness* (2014) (individuals with mental illness are more likely to be the victims rather than the perpetrators of violence).

[26] Within this context, an "unusual interest in weapons" would be such that it would arouse concern in a reasonable person that the individual is at risk of harming self or others. (See, e.g., ISE-SAR Functional Standard Version 1.5.5, Part B (Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person).

[27] United States Secret Service, Protecting America's Schools: A U.S. Secret Service Analysis of Targeted School Violence, at 45-46 (2019).

[28] Treatment Advocacy Center (summarizing several studies related to the impact of medication nonadherence).

[29] This concept originated in two significant rulings by the California Supreme Court in *Tarasoff v. Regents of the University of California*, 529 P.2d 553 (Cal. 1974) (Tarasoff I) (identifying a duty for mental health professionals to warn potential victims) and *Tarasoff v. Regents of the University of California* 551 P.2d 334 (Cal. 1976) (Tarasoff II) (identifying a duty to protect potential victims from serious threats made by patients and delineating the steps they may take to discharge this responsibility (i.e., directly warning the victim, notifying law enforcement, voluntary/involuntary hospitalizations). For further information, refer to the National Council of State Legislatures, Mental Health Professionals' Duty to Warn (10/12/2018), at https://www.ncsl.org/research/health/mental-health-professionals-duty-to-warn.aspx; American Psychological Association, APA Practice Organization, *Duty to Protect*, Fall2013GP.pdf (apaservices.org); Rebecca Johnson, MA, Govind Persad, JD, and Dominic Sisti, PhD., J. Am. Acad. Psychiatry and the Law, Vol. 42, Number 4 (2014), The Tarasoff Rule: The Implications of Interstate Variation and Gaps in Professional Training.

[30] APA Practice Organization, *Duty to Protect*, Fall2013GP.pdf (apaservices.org).

[31] See National Council of State Legislatures, Mental Health Professionals' Duty to Warn (10/12/2018), at https://www.ncsl.org/research/health/mental-health-professionals-duty-to-warn.aspx; American Psychological Association, APA Practice Organization, *Duty to Protect*, Fall2013GP.pdf (apaservices.org); Rebecca Johnson, MA, Govind Persad, JD, and Dominic Sisti, PhD., J. Am. Acad. Psychiatry and the Law, Vol. 42, Number 4 (2014), The Tarasoff Rule: The Implications of Interstate Variation and Gaps in Professional Training.

[32] For promising practices related to the mental health professionals' duty to warn/protect, refer to *Tips, Leads, and Threats to Life Promising Practices and Success Stories*.

[33] Law enforcement agencies interested in obtaining further information on this issue should contact the fusion center with responsibility for their area or the FBI.

[34] The development and implementation of a memorandum of understanding between law enforcement agencies and schools that reflects a common vision and shared objectives provides a strong foundation for a school-based partnership. For further information, refer to the U.S. Department of Justice, Office of Community Oriented Policing Services (COPS Office), Protecting Students – Protecting Schools (usdoj.gov), Vol. 14, Issue 4 (April 2021); U.S. Department of Justice, COPS Office, How to Write a Compelling Memorandum of Understanding for your School Resource Officer Program, Vol. 12, Issue 7 (August 2019); see also National Association of School Resource Officers (nasro.org). The memorandum of understanding (MOU) should delineate the roles and responsibilities of the partners involved, including the school resource officers (SROs), establish the circumstances under which information will be shared with law enforcement, and identify applicable laws. See, e.g., The Office of the Attorney General of the State of New Jersey, A Uniform State Memorandum of Agreement between Education and Law Enforcement Officials (2019 Revisions).

[35] The FBI defines "targeted violence" as an incident of violence where an assailant chooses a particular target prior to a violent attack." The Federal Bureau of Investigation, Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks (Making Prevention a Reality), at 99.

[36] The purpose of a P/CRCL policy is to articulate that the agency will adhere to legal requirements and policy and procedural provisions that enable gathering and sharing of information to occur in a manner that protects constitutional rights, including personal privacy and other civil liberties, and civil rights. See *Fusion Center P/CRCL Policy Template* (March 2019); Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities (April 2012). For additional information, refer to the Frequently Asked Questions related to the privacy, civil rights, and civil liberties, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and criminal justice information.

[37] See, e.g., U.S. CONST. AM 1. See also *Fusion Center P/CRCL Policy Template* (March 2019*);* Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities (April 2012). For additional information, refer to the *TLTTL Frequently Asked Questions* related to privacy, civil rights, and civil liberties, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and criminal justice information. For information about sharing behavioral health information, refer to the U.S. Department of Justice Bureau of Justice Assistance and the Council of State Governments, Sharing Behavioral Health Information: Tips and Strategies for Police-Mental Health Collaborations (October 2019), https://csgjusticecenter.org/projects/police-mental-health-collaboration-pmhc/sharing-behavioral-health-information/; U.S. Department of Justice Bureau of Justice Assistance and the Council of State Governments, Information Sharing in Criminal Justice-Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (2010), https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/CSG_CJMH_Info_Sharing.pdf.

[38] *ROSA Resource Guide*, at 32; *Face Recognition Policy Development Template for Use in Criminal Investigations*, at 48 and n.41. (*citations omitted*). To collect PII relating to threats to life (TTLs), law enforcement personnel must work for an entity that has the legal authority to receive and/or respond to tips and leads information. In addition, the individual's official duties in that entity must include receiving, processing, and responding to TTL information and the individual can only act for a valid law enforcement purpose. If, on the other hand, this activity is outside the scope of the entity's authorities or the individual's official responsibilities, then the individual must immediately refer the information to the appropriate entity so it can take appropriate action.

[39] 28 C.F.R. 23.20(e); see also https://28C.F.R..ncirc.gov/FAQ.

[40] See FBI, Making Prevention a Reality, at 20. However, if law enforcement determines that such speech is protected by the First Amendment, it must stop its review. Id. With protected speech, government agencies cannot take any action "that destroys, or even significantly diminishes, [an individual's] ability to communicate a public message or idea through his words or deeds." Id.

[41] See 28 C.F.R. § 23.20. Online training for 28 C.F.R. Part 23 is available at https://28cfr.ncirc.gov/.

[42] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Ver. 1.5.5. A terrorism-related SAR is also known as an ISE-SAR. The ISE-SAR FS Ver. 1.5.5 defines an ISE-SAR as a SAR that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of criminal activity associated with terrorism).

[43] See ISE-SAR Functional Standard Version 1.5.5 Section II.B and Part B.

[44] For further information, refer to the National Network of Fusion Centers (NNFC), Office of the Director of National Intelligence's (ODNI) Office of Partner Engagement-Information Sharing Environment (PE-ISE), U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Criminal Intelligence Coordinating Council (CICC), *Real-time and Open Source Analysis Resource Guide* (ROSA Resource Guide) (July 2017).

[45] Congressional Research Service, The First Amendment: Categories of Speech (January 2019), at 1-2. Examples of unprotected speech include advocating imminent lawless action, true threats, fighting words, fraudulent misrepresentation, etc. Id.

[46] U.S. CONST. AM. 1 ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."). See *Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template*, 11 (March 2019*);* Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities, 8 (April 2012). For examples of First Amendment activities, refer to https://www.uscourts.gov/about-federal-courts/educational-resources/educational-activities/first-amendment-activities.

[47] U.S. CONST. AM. 1 ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."). For further information, refer to https://www.law.cornell.edu/constitution/first_amendment.

[48] See *Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template*, 11 (March 2019*);* Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities, 8 (April 2012).

[49] *Watts v. United States*, 394 U.S. 705 (1969) (*per curiam*).

[50] See *Watts v. United States*, 394 U.S. 705 (1969) (*per curiam*).

[51] *ROSA Resource Guide*, at 9 ("[A]dvocacy of violence or lawbreaking, depending on context, may be protected speech under the First Amendment, and as such, consultation with agency legal counsel is encouraged. For speech advocating violence or lawlessness to be unprotected, it must be directed at inciting "imminent lawless action" and be likely to produce the intended lawlessness or violence.")

[52] *Watts v. United States*, 394 U.S. 705, 708 (1969).

[53] U.S. CONST. AM. 1 ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."). For further information, refer to https://www.law.cornell.edu/constitution/first_amendment.

[54] *See, e.g., Virgina v. Black*, 538 U.S. 343, 360 (2003).

[55] *Watts v. United States*, 394 U.S. 705 (1969); *Virginia v. Black*, 538 U.S. 343, 359, 123 S. Ct. 1536, 1548 (2003). For more information, refer to the "*ROSA Resource Guide*," at 5-6, 9-10, Appendix 29-36, July 2017, and the FBI, Making Prevention a Reality, at 20.

[56] *People v. Prisinziano*, 648 N.Y.S.2d 267, 275-76 (N.Y. Crim. Ct. 1996) (citing *Watts,* at 708 (the context, the conditional nature of statements, and the reaction of the listeners were considered by the U.S. Supreme Court in concluding that the statements made were "political hyperbole" and not a true threat)).
[57] *New York Times Co. v. Sullivan*, 376 U.S. 254.
[58] *See, e.g., United States v. White*, 670 F.3d 498, 510 (4th Cir. 2012); *United States v. Cassel*, 408 F.3d 622, 625 (9th Cir. 2005) (requiring a speaker to possess a subjective intent to threaten in order for his speech to be deemed a true threat); https://www.mtsu.edu/first-amendment/article/1025/true-threats; https://mtsu.edu/first-amendment/article/970/incitement-to-imminent-lawless-action.
[59] *Virgina v. Black,* 538 U.S. 343 (2003); *Elonis v. United States*, 135 S. Ct. 2001 (2015); see also FBI, Making Prevention a Reality, at 20.
[60] *Watts v. United States*, 394 U.S. 705 (1969); *Elonis v. United States*, 135 S. Ct. 2001 (2015); *United States v. Carrillo*, 2020 U.S. Dist. LEXIS 7628
[61] *Watts v. United States*, 394 U.S. 705 (1969); *United States v. Bradley*, 590 F.2d 335 (1978); Virginia v. Black, 538 U.S. 343 (2003); *State v. Kohonen*, 192 Wn. App. 567, 2016 Wash. App. LEXIS 162.
[62] *Id.* at 59, 61 (S.D. Ohio May 1, 2018); *United States v. Hoff*, 767 F. App'x 614, at 626 (6th Cir. 2019).
[63] *United States v. Hoff*, 767 F. App'x 614, 625-26 (6th Cir. 2019) (where the caller threatened a Republican congressman, four days after Republican congressmen and their staff members were shot at during a baseball practice in DC, and referenced the shooting. The court held that "…in concert with the actions that occurred on that baseball field, [and] the timing of the June 18th phone call," a reasonable person would interpret the caller's comments as a "serious intention to inflict bodily harm."). *Id.* at 626.
[64] The FBI, Making Prevention a Reality, at 18.
[65] Id.
[66] The FBI, Making Prevention a Reality, at 18
[67] *Bonds v. Univ. of Cincinnati Med. Ctr.*, 2018 U.S. Dist. LEXIS 73605 at 20, 25, 54 (S.D. Ohio, May 1, 2018).
[68] Id. at 18.
[69] Id. at 19.
[70] Id.
[71] Id.
[72] *Brandenburg v. Ohio*, 395 US 444, 89 S. Ct. 1827, 23 L. Ed. 2d 430 (1969). For a summary of the *Brandenburg* test, see https://www.law.cornell.edu/wex/brandenburg_test.
[73] *Hess v. Indiana*, 414 U.S. 105 (1973); *Nwanguma v. Trump,* No. 17-6290 (6th Cir. 2018); *Brandenburg v. Ohio*, 395 US 444 (1969).
[74] Title 18 U.S.C. §§ 2702 (b)(8) and (c)(4).
[75] *Id.*
[76] *Caniglia v. Strom*, 141 S.Ct. 1596 (2021).
[77] *Michigan v. Fisher*, 558 U.S. 45, 49 (2009).
[78] *Caniglia*, 141 S. Ct. 1596, at 1603.
[79] *See, e.g., Sheehan*, 575 U. S., at 612, 135 S. Ct. 1765, 191 L. Ed. 2d 856 (officers could enter the room of a mentally ill person who had locked herself inside with a knife); *Michigan v. Fisher*, 558 U. S., at 48-49, 130 S. Ct. 546, 175 L. Ed. 2d 410; *Brigham City*, 547 U. S., at 406-407, 126 S. Ct. 1943, 164 L. Ed. 2d 650 (Emphasis added); *United States v. Andrews,* 2019, 381 F.Supp.3d 1044 (D.Minn.) (the officer reasonably believed that the defendant was a suspect in the shootings, and that he was still armed and dangerous, where witnesses placed the defendant at the scene of shooting and identified him as the gunman, there was reason to believe that the defendant had participated in the earlier shooting in same general area, investigating officers determined that the defendant had an extensive criminal history involving weapons and narcotics, and shooter had recklessly used deadly force, thus causing an emergency involving the danger or death or serious physical injury sufficient to meet disclosure requirements of the Stored Electronic Communications Act); *U.S. v. Takai*, 943 F.Supp.2d 1315 (D.Utah 2013) (a detective familiar with the defendant had positively identified the defendant as prime suspect in robbery and violent shooting of the clerk in face at point blank range earlier that day, and the detective who applied for GPS pinging data had been informed that the defendant was known to be violent and was believed to be currently armed and dangerous, and reasonably believed that additional robbery might be imminent).
[80] U.S. Department of Justice, Guidance for Federal Law Enforcement Agencies regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (December 2014); ISE-SAR Functional Standard Version 1.5.5, at 10 fn.9 and Part B ("Consideration and documentation of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity shall be consistent with applicable guidance, including, for federal law enforcement officers…."); *Fusion Center P/CRCL Policy Template,* at E.2.
[81] Department of Homeland Security, Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity | Homeland Security (dhs.gov).
[82] Id.

[83] *Fusion Center P/CRCL Policy Template,* at E.2.
[84] ISE-SAR Functional Standard Version 1.5.5, at 10 fn.9 and Part B ("Consideration and documentation of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity shall be consistent with applicable guidance, including, for federal law enforcement officers…."), citing U.S. Department of Justice, Guidance for Federal Law Enforcement Agencies regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (December 2014).
[85] Cornell Law School, Legal Information Institute, Right of Association ("It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech..... It appears from the Court's opinions that the right of association is derivative from the First Amendment guarantees of speech, assembly, and petition …."), citing *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460 (1958); *Bates v. City of Little Rock*, 361 U.S. 516, 522–23 (1960); *United Transportation Union v. State Bar of Michigan*, 401 U.S. 576, 578–79 (1971); Healy v. James, 408 U.S. 169, 181 (1972).
[86] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Ver. 1.5.5.
[87] For example, 28 C.F.R. Part 23 establishes criteria for criminal intelligence information records that are submitted to interjurisdictional or multijurisdictional criminal intelligence systems that are operated by state, local, tribal, or territorial agencies and supported with Omnibus Crime Control and Safe Streets Act funding. The reasonable suspicion standard is one of the submission criteria in 28 C.F.R. Part 23. Section 23.20(c) states, in part, that the reasonable suspicion or criminal predicate is "established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise." Online training for 28 C.F.R. Part 23 is available at https://28cfr.ncirc.gov/.
[88] For further information about fusion centers, refer to State and Major Urban Area Fusion Centers Fact Sheet (dhs.gov); and The National Network of Fusion Centers – National Fusion Center Association (NFCA) (wpengine.com).
[89] If medical records are provided (as opposed to simply reported health information, e.g., "he previously tried to commit suicide and spent three days in the hospital), the fusion center should evaluate the business need for retaining such records and identify the appropriate retention schedule.
[90] This does not include suicide by cop or other scenarios that involve threats to others in addition to a desire for self-harm (e.g., suicidal/homicidal acts).
[91] For example, the agency articulates specific facts about the subject's suicidal-homicidal intent (e.g., "I'm taking others out with me").
[92] Section 4.2.3.2 in the FBI CJIS Security Policy addresses the proper access, use, and dissemination of NCIC non-restricted files information. NCIC nonrestricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Nonrestricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

[93] See, e.g., FLA. Stat. 985.04 (sharing of confidential juvenile information).
[94] See 28 C.F.R. Part 20 (detailing the specific authorizations); see also Criminal Justice Information (CJIS) Security Policy, Version 5.9, June 1, 2020, available at https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view.
[95] For Frequently Asked Questions about the HIPAA Privacy Rule, refer to Summary of the HIPAA Privacy Rule | HHS.gov.
[96] U.S. Department of Health and Human Services, OCR Privacy Brief, Summary of the HIPAA Privacy Rule, at 2-3 (Last revised May 2003). For information about sharing behavioral health information, refer to the U.S. Department of Justice Bureau of Justice Assistance and the Council of State Governments, Sharing Behavioral Health Information: Tips and Strategies for Police-Mental Health Collaborations (October 2019), https://csgjusticecenter.org/projects/police-mental-health-collaboration-pmhc/sharing-behavioral-health-information/; U.S. Department of Justice Bureau of Justice Assistance and the Council of State Governments, Information Sharing in Criminal Justice-Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (2010), https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/CSG_CJMH_Info_Sharing.pdf.
[97] For further information, refer to the U.S. Department of Education and the Office for Civil Rights at the U.S. Department of Health and Human Services, Joint Guidance on the Application of FERPA and HIPAA to Student Health Records (Joint Guidance on FERPA and HIPAA) (December 2019 Update) (Addressing the application of FERPA and HIPAA to records maintained on students); see also https://www.hhs.gov/hipaa/for-professionals/faq/513/does-hipaa-apply-to-an-elementary-school/index.html.

[98] U.S. Department of Health and Human Services, OCR Privacy Brief, Summary of the HIPAA Privacy Rule, at 3 citing 45 C.F.R. § 160.103.
[99] U.S. Department of Health and Human Services, OCR Privacy Brief, Summary of the HIPAA Privacy Rule, at 4 citing 45 C.F.R. § 160.103.
[100] U.S. Department of Health and Human Services, OCR Privacy Brief, Summary of the HIPAA Privacy Rule, at 4 citing 45 C.F.R. § 160.103. The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
[101] U.S. Department of Health and Human Services, OCR Privacy Brief, Summary of the HIPAA Privacy Rule, at 4 citing 45 C.F.R. § 164.502(a).
[102] U.S. Department of Health and Human Services, OCR Privacy Brief, Summary of the HIPAA Privacy Rule, at 4 citing 45 C.F.R. § 164.502(a)(2).
[103] Department of Health and Human Services, Health Information Privacy, Frequently Asked Questions regarding Disclosures for Law Enforcement Purposes. See also the U.S. Department of Education and the Office for Civil Rights at the U.S. Department of Health and Human Services, Joint Guidance on FERPA and HIPAA; U.S. Department of Justice Bureau of Justice Assistance and the Council of State Governments, Sharing Behavioral Health Information: Tips and Strategies for Police-Mental Health Collaborations (October 2019), https://csgjusticecenter.org/projects/police-mental-health-collaboration-pmhc/sharing-behavioral-health-information/; U.S. Department of Justice Bureau of Justice Assistance and the Council of State Governments, Information Sharing in Criminal Justice-Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (2010), https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/CSG_CJMH_Info_Sharing.pdf. For handout comparing the statutory requirements and permitted disclosures under HIPAA with The Family Educational Rights and Privacy Act (FERPA)), refer to https://www.cdc.gov/phlp/docs/hipaa-ferpa-infographic-508.pdf.
[104] 45 C.F.R. § 164.512(j)(1)(i).
[105] 45 C.F.R. § 164.512(f)(5).
[106] 45 C.F.R. § 164.512(f)(4)
[107] 45 C.F.R. § 164.512(c).
[108] 45 C.F.R. § 164.512(f)(1)(i).
[109] 45 C.F.R. § 164.512(f)(1)(ii)(A)-(B))
[110] 45 C.F.R. § 164.512(f)(2).
[111] 45 C.F.R. § 164.512(f)(3).
[112] U.S. Department of Health and Human Services, How does the HIPAA Privacy Rule Reduce the Potential for conflict with state laws?
[113] Joint Guidance on FERPA and HIPAA, at 3.
[114] Id.
[115] Id.
[116] U.S. Department of Education, Privacy Technical Assistance Center, School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA), at 18 (February 2019) ("The phrase "articulable and significant threat" means that a school official is able to explain, based on all the information available at the time, what the threat is and why it is significant when he or she makes and records the disclosure").
[117] U.S. Department of Education, Privacy Technical Assistance Center, School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA), at 18.
[118] Title 20 U.S.C. § 1232g(a)(4)(B)(ii); U.S. Department of Education, Privacy Technical Assistance Center, School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA), at 15 (February 2019).
[119] Id.
[120] Title 20 U.S.C. § 1232g(a)(4)(B).
[121] Joint Guidance on FERPA and HIPAA, at 8-9.
[122] Title 20 U.S.C. § 1232g(a)(4)(B)(iv).
[123] *Owasso Independent School Dist. No. I-011 v. Falvo*, 534 U.S. 426 (2002) citing 20 U.S.C. § 1232g(a)(4)(A) (*emphasis added*) (A student's posts on social media are maintained by the social media company; therefore, the posts do not constitute "education records" under FERPA which defines this term as "records, files, documents, and other materials" containing information directly related to a student, which "***are maintained by an educational agency*** or institution or by a person acting for such agency or institution").
[124] U.S. Department of Education, Privacy Technical Assistance Center, School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA), at 8.
[125] Id. at 10-12; see also 34 C.F.R. §§ 99.31(a)(9)(i) and (ii).
[126] U.S. Department of Education, Privacy Technical Assistance Center, School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA), at 7-8; 34 C.F.R. §§ 99.31(a)(11) and 99.37.
[127] 38 C.F.R. §§ 99.31(a)(11) and (b)(2)(iii) and 99.37.