NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A PRESCRIPTION FOR INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND THE MEDICAL COMMUNITY TO IMPROVE THREAT ASSESSMENTS

by

Amy L. Thibault

September 2018

Co-Advisors: Cristiana Matei
Lynda A. Peters (contractor)

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE A PRESCRIPTION FOR INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND THE MEDICAL COMMUNITY TO IMPROVE THREAT ASSESSMENTS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Amy L. Thibault	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Medical practitioners may have information that could be used to determine whether an individual poses a violent threat to the community. However, legal and cultural barriers often prevent information sharing between the medical field and law enforcement. This thesis examines the impact of laws and regulations such as HIPAA, FERPA, 42 CFR Part 2, and state duty-to-warn laws, and recommends a legal analysis of these laws to determine whether modifications are necessary. It suggests that states could enact individual laws that mandate information sharing between the medical community and law enforcement for the purposes of threat assessment, which would then allow release of the information under HIPAA and 42 CFR Part 2. It also suggests training for both law enforcement and the medical community to ensure they understand how to apply these laws, as well as joint exercises to enhance collaboration and trust.

14. SUBJECT TERMS HIPAA, FERPA, 42 CFR, Part 2, duty to warn, threat assessment	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A PRESCRIPTION FOR INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND THE MEDICAL COMMUNITY TO IMPROVE THREAT ASSESSMENTS

Amy L. Thibault
Intelligence Services Manager, Massachusetts State Police
BA, Stonehill College, 1996

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2018**

Approved by: Cristiana Matei
Co-Advisor

Lynda A. Peters
Co-Advisor

Erik J. Dahl
Associate Chair for Instruction,
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Medical practitioners may have information that could be used to determine whether an individual poses a violent threat to the community. However, legal and cultural barriers often prevent information sharing between the medical field and law enforcement. This thesis examines the impact of laws and regulations such as HIPAA, FERPA, 42 CFR Part 2, and state duty-to-warn laws, and recommends a legal analysis of these laws to determine whether modifications are necessary. It suggests that states could enact individual laws that mandate information sharing between the medical community and law enforcement for the purposes of threat assessment, which would then allow release of the information under HIPAA and 42 CFR Part 2. It also suggests training for both law enforcement and the medical community to ensure they understand how to apply these laws, as well as joint exercises to enhance collaboration and trust.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CFC	Commonwealth Fusion Center
CFR	Code of Federal Regulations
EDP	emotional disturbed person
FERPA	Family Educational Rights and Privacy Act
HIPAA	Health Insurance Portability and Accountability Act of 1996
NICS	National Instant Criminal Background Check System
NSI	Nationwide Suspicious Activity Reporting Initiative
NTAC	National Threat Assessment Center (United States Secret Service)
PDMP	prescription drug monitoring program
PHI	protected health information
SAR	Suspicious Activity Report

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The nature of violent attacks, including terrorist attacks, in the United States has evolved. Such small-scale incidents as edged-weapon attacks, small-arms attacks, and vehicles used as weapons have become more prevalent. These types of events require minimal resources and planning by the perpetrators, and they do not require a large network; they often involve just one individual. The opportunity for law enforcement to discover or disrupt such attacks is limited. Individuals may disclose information to medical professionals that they would not disclose to family, friends, or even their spouse. Such information may include indicators suggesting that the person is radicalizing or has a propensity for violence. Others may exhibit mental instability or paranoia that could lead to extreme actions. Law enforcement does not have an effective mechanism for understanding how an individual's medical condition—including mental illnesses or behavioral disorders—may influence the person's behavior in order to accurately assess their risk to the community.

Failure to identify individuals who pose a violent criminal threat to society often results in grave consequences. Medical practitioners—mental health providers and non-mental health professionals alike—may encounter, in their daily work, individuals who present a violent threat to the community. Threat assessment frameworks emphasize the need for information sharing between the medical community and law enforcement. The ability to conduct an accurate threat assessment depends on the analysis of all existing information about a subject's previous behavior and medical conditions. When medical personnel learn of a potential threat to the community, even if it is not imminent, there needs to be a mechanism for them to share the information with law enforcement. If law enforcement receives a tip related to a threat by an individual, they need a mechanism to collect all relevant information in order to assess the validity of the threat.

This thesis sought to answer the following questions: How can law enforcement enhance information sharing with the medical community to identify individuals who may pose a threat of committing violent criminal or terrorist acts? Are there laws or policies that need to be created or changed in order to foster better communication? To answer these

questions, the research analyzed existing laws and regulations as well as programs already in existence that allow information sharing between the two disciplines.

Though medical practitioners may have information that could potentially disrupt a violent attack or explain a person's abnormal behavior, laws including the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and 42 Code of Federal Regulations (CFR) Part 2, limit the information that can be shared with law enforcement. Furthermore, some state duty-to-warn laws are inadequate, applying only when there is imminent danger. Research indicates that when these regulations are put into practice, they are usually interpreted in a narrower and more conservative manner than intended. The fear of retribution, whether legal or regulatory, causes practitioners to err on the side of caution and avoid sharing information, which impacts law enforcement's ability to prevent some violent attacks. Privacy concerns, ethical guidelines, and organizational culture all may impact information sharing between the medical community and law enforcement. Current laws and programs are insufficient to proactively address the threat of violence to the community.

There are several intelligence and information sharing initiatives already in place that encourage or allow information sharing between the medical community and law enforcement. These initiatives involve cases of child or elder abuse, injuries sustained by gunshots or knives, and prescription monitoring programs. Additionally, public health regulations often require medical professionals to report cases of certain diseases in order to prevent outbreaks. Mental health and behavioral health data sharing is allowed for an individual who is incarcerated or to prevent individuals with certain illnesses from purchasing a firearm. There has been a concerted effort to incorporate public health into fusion centers, which include public health partners. Information sharing with fusion centers would allow law enforcement to more proactively identify suspicious activity before a violent incident occurs.

The nature of violent attacks necessitates better integration of all relevant information about a subject's background, both criminal and medical, to inform threat assessments and ensure the public's safety. A review of past violent incidents has shown that the lack of information sharing between the medical community and law enforcement

has contributed to law enforcement's inability to thwart attacks before they happen. Though it would be impossible to prevent every violent attack, having more information available for threat assessments will improve our ability to preempt some attacks.

Four recommendations are provided. The first recommendation is to conduct a legal analysis of HIPAA, FERPA, 42 CFR Part 2, and state duty-to-warn laws, which inhibit the ability of law enforcement and the medical community to share medical information for threat assessment purposes. Second, states could enact individual laws that mandate information sharing between the medical community and law enforcement for the purposes of threat assessment, which would then allow release of the information under HIPAA and 42 CFR Part 2. Third, training should be provided to law enforcement and the medical community to ensure they understand the circumstances in which information sharing is allowable and the extent of the information that can be shared. Finally, opportunities for the two disciplines to work together—such as during joint exercises—will foster greater mutual understanding among the different disciplines.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is dedicated to my husband and best friend, Paul, who supported me throughout this amazing journey. Paul knew when to give me space to focus on my studies and surprised me with tickets to shows or getaways to keep me sane and give me something to look forward to. As avid travelers, vacation took on a new meaning with the CHDS laptop tagging along everywhere we went. Even being stuck in Turks and Caicos during hurricane Irma couldn't keep me away from my studies. I look forward to our next adventure, sans laptop! I also couldn't have done it without the love and support of my entire family, including my parents, Brian and Sandy; sister, Melissa; her husband, Ryan; and my niece, Ava; my brother, Brian; grandmother, Betty; and in-laws, Kathy and Ed. To my best friend and cheerleader, Cathy, who texted me every single day I was in residence to make sure that I didn't get home sick, and bought me funny school supplies, you are one of a kind.

To my thesis advisors, Lynda Peters and Cris Matei, your patience, guidance and experience allowed me to reach the finish line. I couldn't have made it without both of you. To the entire faculty and staff of CHDS, your encouragement and dedication to each student is what makes this program unlike any other.

To the Massachusetts State Police, especially Lieutenant Colonel Dermot Quinn, Lieutenant Colonel Christopher Mason, and Major Scott Range, thank you for allowing me to pursue this dream of mine. To everyone in the fusion center, I am grateful for your support.

Lastly, to the entire CHDS 1701-1702 master's cohort, you are the best part of this program. I learned so much from each and every one of you and will miss you all dearly, my friends.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The nature of violent attacks, including terrorist attacks, in the United States has evolved. Such small-scale incidents as edged-weapon attacks, small-arms attacks, and vehicles used as weapons have become more prevalent. These types of events require minimal resources and planning by the perpetrators, and they do not require a large network; they often involve just one individual. Law enforcement's opportunity to discover or disrupt such attacks is limited. The public must play an ever-increasing role in reporting suspicious behavior to law enforcement in order to identify threats to the community, particularly when one person or a small group intends to instigate a small-scale attack.

This type of public cooperation requires the assistance of other disciplines, including the medical community. Individuals may disclose information to medical professionals that they would not disclose to family, friends, or even their spouse. Such information may include indicators that suggest the person is radicalizing or has a propensity for violence. Others may exhibit mental instability or paranoia that could lead to extreme actions. Research suggests that homegrown violent extremists and those who commit other types of violent attacks, such as mass-casualty attacks, have similar "behavioral and psychological characteristics."[1] Law enforcement does not have an effective mechanism for understanding how an individual's medical condition—including mental illness or behavioral disorders—may influence the person's behavior in order to accurately assess risk.

Restrictions such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) dictate the circumstances under which information may be shared. Dr. David Rosmarin, director of forensic psychology at McLean Hospital, suggests that doctors may be the only ones who know about an individual's "serious and imminent

[1] John D. Cohen, "The Next Generation of Government CVE Strategies at Home: Expanding Opportunities for Intervention," *The Annals of the American Academy of Political and Social Science* 668, no.1 (November 1, 2016): 122–123, https://doi.org/10.1177/000271621666993.

threat" to the community.[2] It is a common misconception among members of the medical and law enforcement communities that HIPAA precludes the sharing of patient information under any circumstance, even when there is imminent danger.[3] However, HIPAA provides exceptions that allow "protected health information" (PHI) to be shared with law enforcement without the patient's consent.[4] For example, according to HIPAA, medical professionals can "report PHI to a law enforcement official [who is] reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public."[5] In addition to HIPAA regulations, legal requirements or even organizational culture, as well as cognitive bias on the part of the health care community, may prevent some information from being shared.

B. RESEARCH QUESTIONS

How can law enforcement enhance information sharing with the medical community to identify individuals who may pose a threat of committing violent criminal or terrorist acts? Are there laws or policies that need to be created or changed in order to foster better communication?

C. LITERATURE REVIEW

This literature review assesses works that explore the reasons why the public cooperates with the police. It provides a foundation for understanding what motivates the public to report criminal or suspicious activity. Specifically, it looks at public cooperation,

---

[2] Erin Schumaker, "Doctors Often Know Who Might Commit Gun Violence. But They Can't Do Much about It," *Huffington Post*, March 1, 2018, https://www.huffingtonpost.com/entry/doctors-gun-violence-hipaa_us_5a95a39be4b0bef79e3086ab.

[3] The author of this thesis, Amy Thibault, has eighteen years of experience in intelligence analysis, the last ten of which she has been spent as the intelligence services manager at the Commonwealth Fusion Center (CFC). Since 2010, she has supervised the Nationwide Suspicious Activity Reporting Initiative at the CFC, where she has seen this misconception firsthand.

[4] "What is PHI?," U.S. Department of Health and Human Services, February 26, 2013, www.hhs.gov/answers/hipaa/what-is-phi/index.html.

[5] "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement," U.S. Department of Health and Human Services, accessed October 28, 2017, www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf.

which is necessary for successful crime prevention campaigns. Law enforcement has sought the public's assistance with crime prevention through such community-oriented efforts as the Take a Bite Out of Crime campaign in 1979 and "neighborhood watch," in which private citizens assist law enforcement with detecting and solving crimes.[6] Tom Tyler suggests that "these cooperative efforts are largely voluntary in character, and the police are not generally in a position to reward members of the public for their aid. Instead, the police rely on willing public cooperation with police efforts to control crime and community disorder."[7] In other words, the public is vital to the success of the police.

Scholars over the past fifteen years have focused on cooperation to explain the public's willingness to participate. Three main theories emerged from the review of contemporary literature: the procedural justice model, the instrumental model, and identity theories. While the three theories disagree as to which factor most effectively motivates the public, all of them focus on the public's perception of the police. Aziz Huq, Tom Tyler, and Stephen Schulhofer compare and contrast the perception of law enforcement legitimacy with its perceived effectiveness, while Ben Bradford considers the perception of the police as part of the same social group in determining motivating factors of cooperation.[8] The most prevalent theory is the theory of procedural justice, which is focused on legitimacy.[9]

1. Cooperation Based on Procedural Justice

According to Huq, Tyler and Schulhofer, "the 'procedural justice' model of policing contends that people's reactions to law enforcement are shaped primarily by

---

[6] Garrett J. O'Keefe, "Taking a Bite out of Crime": The Impact of a Public Information Campaign," *Communication Research* 12, no. 2 (1985): 149–150, https://doi.org/10.1177/009365085012002001; Tom R. Tyler, "Enhancing Police Legitimacy," *The Annals of the American Academy of Political and Social Science* 593, no. 1 (2004): 85, https://doi.org/10.1177/0002716203262627.

[7] Tyler, "Enhancing Police Legitimacy," 85.

[8] Aziz Z. Huq, Tom R. Tyler, and Stephen J. Schulhofer, "Why Does the Public Cooperate with Law Enforcement? The Influence of the Purposes and Targets of Policing," *Psychology, Public Policy, and Law* 17, no. 3 (2011): 5, http://dx.doi.org/10.1037/a0023367; Ben Bradford, "Policing and Social Identity: Procedural Justice, Inclusion and Cooperation Between Police and Public," *Policing and Society* 24, no. 1 (2014): 23, https://doi.org/10.1080/10439463.2012.724068.

[9] Huq, Tyler, and Schulhofer, "Why Does the Public Cooperate," 5.

evaluations of the fairness of police conduct."[10] Factors that influence police legitimacy in the procedural justice model include "neutrality, trust, and respect."[11] The public correlates police fairness with legitimacy, which leads to cooperation.[12] Tyler and Jeffrey Fagan agree, adding that "this includes both deferring to their decisions during personal encounters and generally obeying legal rules in their everyday lives. Furthermore, people are more cooperative in helping the police to deal with crime in their communities when they view the police as legitimate."[13]

Tyler and Fagan contend that the public views the police as just when they are shown respect and the police have regard for their civil rights.[14] Even individuals who experience a negative result from an interaction with law enforcement may still perceive the police as legitimate as long as the situation was handled in a fair and objective manner.[15] Tyler asserts that "the quality of interpersonal treatment is consistently found to be a distinct element of fairness, separate from the quality of the decision-making process. Above and beyond the resolution of their problems, people value being treated with politeness and having their rights acknowledged."[16]

Justin Nix refers to the procedural justice model as the process-based model, and his 2017 study disagreed with the majority of procedural justice studies; it concluded that officers in the study "believe performance to be the primary means of attaining cooperation from citizens in high-crime areas."[17]

---

[10] Huq, Tyler, and Schulhofer, 5.

[11] Huq, Tyler, and Schulhofer, 22.

[12] Huq, Tyler, and Schulhofer, 5.

[13] Tyler, "Enhancing Police Legitimacy," 89.

[14] Tom R. Tyler and Jeffrey Fagan, "Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in their Communities," *Ohio State Journal of Criminal Law* 6 (2008): 253, http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4027&context=fss_papers.

[15] Tyler and Fagan, 262.

[16] Tyler, "Enhancing Police Legitimacy," 94–95.

[17] Justin Nix, "Do the Police Believe That Legitimacy Promotes Cooperation from the Public?," *Crime & Delinquency* 63, no. 8 (July 2017): 968, https://doi.org/10.1177/0011128715597696.

Much of the literature compares the procedural justice model with the instrumental model, in which cooperation is based on performance rather than on fairness.[18] Hybrid theories are formed by joining portions of the procedural justice model with additional elements such as belonging to the same social group or a person's role in society.[19] Several studies have shown that legitimacy, rather than instrumental factors, affects cooperation with law enforcement.[20]

As procedural justice is based on legitimacy, it is necessary to explore the concept of legitimacy. The term *legitimacy* is often used interchangeably with the terms *status* and *reputation*, even though they have different meanings.[21] Legitimacy, for the police, is most closely correlated with government legitimacy. Much of the related literature concerns the legitimacy of the government's rise to power, such as whether or not the government was elected, and if it is considered legitimate by other governments.[22] According to Carl J. Friedrich, "the 'question of legitimacy' is the 'question of fact whether a given rulership is believed to be based on good title by most men subject to it.'"[23] Good title, according to Peter G. Stillman, refers to the way in which the ruler ascended to power.[24] Jean d'Aspremont contends that internal legitimacy, how government "is perceived by the people subject to it," is different from external legitimacy, "how it is perceived by other

---

[18] Jason Sunshine and Tom R. Tyler, "The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing," *Law & Society Review* 37, no. 3 (2003): 514, https://doi.org/10.1111/1540-5893.3703002.

[19] Bradford, "Policing and Social Identity," 23; Michael A. Hogg, Deborah J. Terry, and Katherine M. White, "A Tale of Two Theories: A Critical Comparison of Identity Theory with Social Identity Theory," *Social Psychology Quarterly* 58, no. 4 (December 1995): 256, http://libproxy.nps.edu/login?url=https://search.proquest.com/docview/212697365?accountid=12702.

[20] Huq, Tyler, and Schulhofer, "Why Does the Public Cooperate," 19.

[21] David L. Deephouse and Mark Suchman, "Legitimacy in Organizational Institutionalism," in *The SAGE Handbook of Organizational Institutionalism*, eds. Royston Greenwood, Christine Oliver, Roy Suddaby, and Kerstin Sahlin (Thousand Oaks, CA: SAGE, 2008), 60–62, http://dx.doi.org/10.4135/9781849200387.n2.

[22] Peter G. Stillman, "The Concept of Legitimacy," *Polity* 7, no. 1 (Autumn 1974): 34, www.jstor.org/stable/3234268.

[23] Stillman, 34.

[24] Stillman, 34.

governments."[25] Stillman argues that "all definitions of legitimacy involve making evaluative decisions."[26] If legitimacy is subjective, it would be hard to replicate in terms of public cooperation.

2. Cooperation Based on Perceived Police Effectiveness

The instrumental model focuses on the "effectiveness of the police in managing crime and social order."[27] The instrumental model correlates the public's willingness to cooperate with police to specific measurable goals, such as number of arrests or other measures of productivity.[28] Jason Sunshine and Tom R. Tyler add that

> people's willingness to accept and cooperate with legal authorities is linked to evaluations of police performance, to risk, and to judgments about distributive justice. This model, the instrumental perspective, suggests that the police gain acceptance when they are viewed by the public as (1) creating credible sanctioning threats for those who break rules (risk), (2) effectively controlling crime and criminal behavior (performance), and (3) fairly distributing police services across people and communities (distributive fairness).[29]

Nix's study, along with the work of Huq, Tyler, and Schulhofer, supports the instrumental model, concluding that performance is more important than legitimacy in citizen cooperation.[30] Masahiro Tsushima and Koichi Hamai believe that perceived law enforcement effectiveness can have a deterrent effect and "that social order is maintained by the sanctioning of misbehavior and criminal offenses."[31] They continue: "That is, people who value police effectiveness tend to think that they will be caught and sanctioned

---

[25] Jean d'Aspremont, "Legitimacy of Governments in the Age of Democracy," *New York University Journal of International Law and Politics* 38 (2005): 882.

[26] Stillman, "The Concept of Legitimacy," 34.

[27] Huq, Tyler, and Schulhofer, "Why Does the Public Cooperate," 19.

[28] Sunshine and Tyler, "Procedural Justice and Legitimacy," 514.

[29] Sunshine and Tyler, 514.

[30] Nix, "Police Legitimacy," 19

[31] Masahiro Tsushima and Koichi Hamai, "Public Cooperation with the Police in Japan," *Journal of Contemporary Criminal Justice* 31, no. 2 (May 2015): 215, https://doi.org/10.1177/1043986214568836.

if they break the law (perceived sanctions) and therefore comply with the law and cooperate with the police."[32]

Tyler and Fagan's 2008 study also supports Nix and the instrumental model, agreeing that individuals cooperate more when they believe police are "effective and that the police create a credible threat of punishment for wrongdoing."[33] Sunshine and Tyler found that after an attack such as 9/11, procedural justice becomes less important and citizens concentrate more on effectiveness.[34]

While some studies assert that effectiveness is the most important factor in cooperation with police, an equal amount of the literature disagrees with this assertion and many studies had contrary results. Opposing views, such as those expressed by Huq, Tyler, and Schulhofer, suggest that legitimacy, rather than effectiveness, is most important in public cooperation.[35] Michael A. Hogg, Deborah J. Terry, and Katherine M. White discuss cooperation in terms of identity with either a sense of belonging or an individual's role being the most important factor.[36]

3. Cooperation Based on Self-Identity Match with Police

Social identity theory, according to David Brannan, Kristin Darken, and Anders Strindberg, contends that "an individual's sense of self and self-worth is derived from the associations he or she has with the groups of which he or she is a part."[37] Individuals will remain in a group as long as they feel that their membership benefits them in some way.[38] Research by Bradford in the United Kingdom draws on social identity theory and combines it with procedural justice theory to create the "group value theory of procedural justice,"

---

[32] Tsushima and Hamai, 215.

[33] Tyler and Fagan, "Legitimacy and Cooperation," 263.

[34] Sunshine and Tyler, "Procedural Justice and Legitimacy," 522.

[35] Huq, Tyler, and Schulhofer, "Why Does the Public Cooperate," 22.

[36] Hogg, Terry, and White, "Tale of Two Theories," 255.

[37] David Brannan, Kristin Darken, and Anders Strindberg, *A Practitioner's Way Forward* (Salinas, CA: Agile Press, 2014), 63.

[38] Brannan, Darken and Strindberg, 63.

which suggests that in-group dynamics have an effect on cooperation.[39] The public's perception of police fairness causes them to more closely identify with "the social group the police represent—the imagined local or national community."[40] This in-group identity positively affects their interactions with police.[41]

Bradford also asserts that "when people feel fairly treated by group authorities this indicates (a) that they are included and have status within the group and (b) that the group itself is worthwhile and something to be proud of."[42] Bradford raises concerns about the relevance of the group value theory to those who are members of a different religious, ethnic, or social group; he found, however, that "even in highly diverse contexts … people from different ethnic groups place a broadly similar weight on the fairness of the police in their overall judgements of the police and in the formation of their judgements about potential acts of cooperation."[43]

Gary LaFree and Amy Adamczyk also contend that social identity theory may help explain the public's willingness to cooperate following terrorist attacks. Their article, which focused on the aftermath of Boston Marathon bombing attack, states, "According to the in-group/out-group hypothesis, under the right circumstances, external conflicts can lead to greater internal cohesion of social groups"[44] In what has been referred to as the rally effect, citizens—when threatened by terrorists who are viewed as the out-group—are more likely to support their in-group, which consists of "their government and its representatives and the police are the most visible representatives of the state."[45] Bradford agrees that "legitimate authorities generate a sense of duty among those they govern that

---

[39] Bradford, "Policing and Social Identity," 23.

[40] Bradford, 23, 25.

[41] Bradford, 25.

[42] Bradford, 25.

[43] Bradford, 26.

[44] Gary LaFree and Amy Adamczyk, "The Impact of the Boston Marathon Bombings on Public Willingness to Cooperate with Police," *Justice Quarterly* 34, no. 3 (2017): 463, https://doi.org/10.1080/07418825.2016.1181780.

[45] LaFree and Adamczyk, 464.

motivates cooperation."[46] If law enforcement can make the public feel like a part of the in-group, it may have a positive influence on public cooperation with police.

Hogg, Terry, and White compare identity theory with social identity theory, contending, "The two theories occupy parallel but separate universes, with virtually no cross-referencing … and to our knowledge no published attempt has been made to systematically compare them."[47] They identify one difference between the theories, asserting that "identity theory is principally a micro socio-logical theory that sets out to explain individuals' role-related behaviors, while social identity theory is a social psychological theory that sets out to explain group processes and intergroup relations."[48] They continue: "both theories place their major theoretical emphasis on a multi-faceted and dynamic self that mediates the relationship between social structure and individual behavior."[49] According to identity theory, people have multiple role identities, as opposed to social identity theory, in which identity is based on belonging to one or more groups.[50] Finally, Hogg, Terry, and White argue that identity theory treats "the self not as an autonomous psychological entity but as a multifaceted social construct that emerges from people's roles in society."[51]

Nancy Buchanan et al. studied cooperation from the perspective of global social identity, stating that "many global problems are social dilemmas, situations in which individuals must choose between behaviors serving self-interest and behaviors benefiting the collective welfare."[52] They argue that "collectively, everyone is better off if all contribute, even though cooperation involves self-sacrifice at the individual level."[53]

---

[46] Bradford, "Policing and Social Identity," 28.

[47] Hogg, Terry, and White, "Tale of Two Theories," 255.

[48] Hogg, Terry and White, 255

[49] Hogg, Terry, and White, 255.

[50] Hogg, Terry, and White, 255.

[51] Hogg, Terry, and White, 256.

[52] Nancy R. Buchan et al., "Global Social Identity and Global Cooperation," *Psychological Science* 22, no. 6 (June 2011): 821, http://www.jstor.org/stable/25835457.

[53] Buchan et al., 821.

Similar to social identity theory, global social identity explains that "levels of cooperation are significantly higher when shared in-group identity is made salient or group members strongly identify with the collective than when no shared identity is available or group identification is weak."[54]

D. RESEARCH DESIGN

The object of this research is to identify legal and cultural barriers to sharing threat information between law enforcement and medical professionals.

1. Selection Criteria

Research focused on statutes, regulations, and policies that allow or prohibit medical information from being shared with law enforcement when there is a perceived threat to the community. Successful examples of information sharing between the medical community and law enforcement were examined. Cultural and cognitive biases on behalf of both law enforcement and the medical community that inhibit information sharing also were analyzed.

2. Limits

This thesis focuses on the problem of sharing medical information with law enforcement in the United States. It does not focus on sharing any other types of information, and it does not discuss sharing medical information with any disciplines other than law enforcement, nor with the general public. The concept of threat assessment is introduced in so far as to scope the problems of sharing medical information. This thesis does not focus on methods, benefits, or criticisms of threat assessment.

3. Data Sources

Data from professional journals, law review journals, and state and federal statutes is included in the data set. The literature review served to examine theories of cooperation with law enforcement—such as those between the public and law enforcement—in order

[54] Buchan et al., 821.

to examine smart practices for cooperation that may be applicable to cooperation between the medical community and law enforcement.

4. Type of Analysis

This thesis is qualitative in nature; it analyzes statutes, regulations, and programs that allow or prohibit medical information from being shared with law enforcement when there is a perceived threat to the community. Successful examples of information sharing between the medical community and law enforcement were analyzed to determine if any lessons could be learned from existing programs that may be applicable to sharing threat information. Cultural and cognitive biases on behalf of both law enforcement and the medical community that inhibit information sharing also were analyzed. After defining the problem, research focused on gathering data to determine the scope of the problem.[55] Data about current policies, as well as policies "that have worked effectively in situations apparently similar" were also analyzed.[56]

5. Outputs

After defining the scope of the problem, this thesis sets forth recommendations to be considered by the United States government in order to enhance information sharing between the medical community and law enforcement for the purposes of threat assessment.

---

[55] Eugene Bardach and Eric M. Patashnik, *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving*, 5th ed. (Los Angeles: SAGE/CQ Press, 2016), xvi.

[56] Bardach and Patashnik, 13.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE NEED FOR MEDICAL COMMUNITY AND LAW ENFORCEMENT ENGAGEMENT IN THREAT ASSESSMENT

Medical practitioners—mental health providers and non–mental health professionals alike—have the potential to encounter, in their daily work, individuals who may present a violent threat to the community. These individuals' aggressive conduct may be exacerbated by behavioral or mental health issues. These individuals may confide in medical personnel because of the trusted relationship patients often share with their physician or nurse. Sociologist Mario Luis Small, in his study regarding an individual's "core discussion network, the set of friends and family people turn to when discussing important matters," found that "45% of the core discussion network is composed of people whom respondents do not consider important to them. In fact, the core discussion network includes doctors, coworkers, spiritual leaders, and other alters whom ego confides in without feeling emotionally attached to." [57]

Threat assessment frameworks emphasize the need for information sharing between the medical community and law enforcement. This chapter explores some of those frameworks and provides examples of individuals who acted out their violent tendencies, causing loss of life. The literature demonstrates that increased information sharing about individuals who pose a threat to the community may allow law enforcement to disrupt future violent attacks.

A. INDIVIDUALS WHO POSE A VIOLENT THREAT

The need to identify individuals who pose a violent criminal threat to society is a persistent issue. Failure to do so often results in grave consequences. Examples such as the mass shooting that occurred at Virginia Polytechnic Institute and State University (Virginia Tech) in 2007, the attack on a movie theatre in Aurora, Colorado, in 2012, the killing spree of Elliot Rodger near the University of California, Santa Barbara, campus in 2014, and the

[57] Mario Luis Small, "Weak Ties and the Core Discussion Network: Why People Regularly Discuss Important Matters with Unimportant Alters," *Social Networks* 35 (2013): 470, http://scholar.harvard.edu/files/mariosmall/files/small_2013.pdf.

school shooting at Marjory Stoneman Douglas High School in Parkland, Florida, in 2018 illustrate the ongoing need for information sharing between the medical community and law enforcement. Each of these incidents illustrates an instance where medical personnel had knowledge about the individual who committed these acts—information that may have helped prevent the incident from occurring. It is not feasible for every act of violence to be avoided; however, barriers to sharing information with law enforcement inhibit opportunities for disruption.

1. Virginia Tech Shootings

On April 16, 2007, senior student Seung Hi Cho went on a killing spree at Virginia Tech, which ended when Cho, about to be captured, killed himself. His actions left thirty-three people, including himself, dead and seventeen more injured.[58] Prior to Cho's rampage, he was exhibiting "deviant behavior—stalking, taking cell-phone photos of female students during class, violent writing, and unwillingness to participate in class," as well as threats to take his own life.[59]

There were many failures to communicate leading up to the Virginia Tech shootings. The Virginia Tech Care Team, a multidisciplinary university group that assists students with behavioral issues, was notified of Cho's behavior but did not follow up with him.[60] The school believed that they could not disclose Cho's disciplinary records to law enforcement due to the Family Educational Rights and Privacy Act (FERPA).[61] Therefore, campus police were not aware of other behavioral issues Cho was having on campus when they interacted with him. Campus police were alerted to Cho's behavior by a student who called to complain, as well as by his roommate, who reported that Cho was suicidal.[62] Cho was held overnight due to his suicidal thoughts under a "temporary detention order" and

---

[58] Gordon K. Davis, "Connecting the Dots: Lessons from the Virginia Tech Shootings," *Change* 40, no. 1 (January–February 2008): 12.

[59] Davis, 12.

[60] Davis, 12.

[61] Davis, 11.

[62] Davis, 12.

mandated to undergo counseling through the school, but the university counselors did not contact his previous mental health providers.[63] Cho's previous medical provider was aware "that he had been fascinated by the Columbine High School shootings in 1999, and that he had fantasized about carrying out a similar mass killing."[64] This information could have been used by the university counselors and campus police to develop a complete threat picture when Cho began exhibiting concerning behavior.

Following the tragedy at Virginia Tech, then-Virginia Governor Tim Kaine formed a multi-disciplinary panel to come up with lessons learned from the tragedy. Recommendations included the following:

> (3) Congress and the state legislatures should review federal and state privacy laws, and universities should know what they do and do not permit. HIPAA (the Health Insurance Portability and Accountability Act), FERPA (the Family Educational Rights and Privacy Act), and state privacy laws should be reviewed to ensure that they are compatible and that they meet the real needs of our society.
>
> (4) Colleges and universities should communicate, both within themselves and beyond. Institutions need to break through current barriers to communication to ensure that information about potential threats is shared by everyone who needs to know. ….
>
> (7) Develop a way to access students' mental-health records. Records of immunization travel with us from early childhood through institution after institution. But a college or university does not get records about communicable diseases, not to mention serious mental-health problems, psychotropic medications (which a student may stop taking), or special-education programs that may have helped a student in high school. This information clearly should not be used in admissions. But later, perhaps while choosing courses, students might be asked to sign waivers allowing the institution access to their health records. At the least, university staff should be expected to ask the parents of a student whose behavior causes concern for access to her or his health records.[65]

---

[63] Davis, 12.

[64] Davis, 12.

[65] Davis, 14–15.

More than ten years after the Virginia Tech tragedy, HIPAA and FERPA have not been amended in order to allow for increased information sharing between the medical community and law enforcement. This also makes it difficult to implement recommendation four, regarding communication, and recommendation seven, regarding access to mental health records.

2. Aurora, Colorado, Movie Theater Attack

On July 20, 2012, James Holmes shot and killed twelve individuals and injured seventy others in an attack at a movie theatre in Aurora, Colorado, during a viewing of *The Dark Night Rises*. Numerous explosive devices were found in Holmes' apartment. Holmes, who was a graduate student at the University of Colorado at the time, had sought treatment at the student health center due to homicidal thoughts.[66] The psychiatrist he was seeing, Dr. Lynne Fenton, later testified that she believed Holmes had obsessive compulsive disorder and "had thoughts of killing people. But she didn't think he was imminently dangerous."[67] Holmes told Fenton "six weeks before the shooting that he fantasized about killing 'a lot of people.'"[68] Fenton told a campus police officer, who offered to have Holmes involuntarily committed, but the therapist declined, believing he was not a threat.[69] After the killing spree, a notebook that detailed Holmes's plans and was intended for Fenton was discovered in a university mailroom.[70] Fenton did not report Holmes to law enforcement officers outside the university. Though threat assessment frameworks stress the importance of law enforcement inclusion, Fenton determined on her own that Holmes was not a threat, even though he was experiencing murderous thoughts shortly before this

---

66 Maria L. La Ganga, "James Holmes Disclosed Homicidal Thoughts but Not a Plan, Psychiatrist Says," *Los Angeles Times*, June 16, 2015, http://www.latimes.com/nation/la-na-james-holmes-fenton-20150616-story.html.

67 La Ganga.

68 Keith Coffman, "James Holmes Told Therapist Lynne Fenton That He Fantasized about Killing 'A Lot of People' Six Weeks before Shooting," *Huffington Post*, last updated February 5, 2013, www.huffingtonpost.com/2012/12/06/therapist-declined-tempor_n_2248980.html.

69 Coffman.

70 "Colorado Theater Shooting Fast Facts," CNN, last updated July 16, 2018, www.cnn.com/2013/07/19/us/colorado-theater-shooting-fast-facts/index.html.

tragic incident. Because mental health treatment records and Holmes's homicidal thoughts were not shared with law enforcement, law enforcement was unable to help assess whether or not Holmes posed a threat to himself or the community.

3. University of California Attacks

On May 23, 2014, Elliot Rodger went on a killing spree during which he stabbed and shot victims and ran others over with his vehicle, killing six and injuring fourteen.[71] The crime spree started at his apartment, where he murdered his roommates, and continued at various locations, with a total of seventeen crime scenes.[72]

Rodger had minor interactions with police over the years, including theft allegations against his roommate, reported vandalism to his vehicle, involvement in a fight, and a welfare check on April 30, 2014.[73] During the welfare check, which occurred twenty-three days before this incident, law enforcement was in contact with Rodger's mother; the only information they had about Rodger's mental state came from this phone call, during which his mother mentioned her son had been posting videos online in which he appeared to be lonely.[74] Rodger wrote a 137-page manifesto titled *My Twisted World.*[75] It is unknown when he wrote the manifesto, which he emailed on May 23, 2014, to his life skills coach and numerous others, including his mother and therapists.[76] The coach contacted Rodger's mother, who contacted police, but Rodger was already in the midst of his killing spree.[77] Law enforcement may have benefited from additional information regarding Rodger's medical diagnosis at the time of the welfare check. It is impossible to know, however, if this would have changed the outcome on May 23, 2014.

---

[71] Bill Brown, "Isla Vista Mass Murder: May 23, 2014" (investigative summary, Santa Barbara County Sheriff's Office, 2015), 1, https://assets.documentcloud.org/documents/1671822/isla-vista-investigative-summary.pdf.

[72] Brown, 59–60.

[73] Brown, 45–47.

[74] Brown, 47.

[75] Brown, 7, 30.

[76] Brown, 7, 30.

[77] Brown, 31.

4. Parkland, Florida, School Shooting

Most recently, on February 14, 2018, a gunman opened fire on students and teachers at Marjory Stoneman Douglas High School in Parkland, Florida, killing seventeen and injuring fourteen others.[78] The gunman, Nikolas Cruz, was a former student who had been expelled the previous school year.[79] Cruz was in therapy for much of his teen years and told a school psychiatrist that he dreamed about "killing people and being drenched in human blood."[80] Students at the school recalled that "Cruz would talk about his 'guns, knives and hunting,' and that 'everyone predicted' he would turn into a school shooter."[81] Cruz made posts on social media referencing school shootings prior to the incident.[82]

Around 2014, Cruz's mother planned to buy him a gun for his birthday.[83] She received mixed messages from two different therapists, with one telling her it was a bad idea and that he should not have weapons, while another therapist suggested she use the gun as a reward for good behavior.[84] At least twice when police responded to the Cruz home due to Cruz's violent behavior, therapists determined he was not a threat and told the police that he did not need to be committed.[85] Cruz was able to purchase the weapon he used in the attack legally, as he had never been committed and was therefore not legally banned from purchasing a firearm.[86]

---

[78] Elizabeth Chuck, Alex Johnson, and Corky Siemaszko, "17 Killed in Mass Shooting at High School in Parkland, Florida," NBC News, February 15, 2018, https://www.nbcnews.com/news/us-news/police-respond-shooting-parkland-florida-high-school-n848101.

[79] Lisa Marie Segarra et al., "Sheriff's Office Had Received about 20 Calls Regarding Suspect: The Latest on the Florida School Shooting," *Time*, February 18, 2018, www.time.com/5158678/what-to-know-about-the-active-shooter-situation-at-florida-high-school/.

[80] Chuck, Johnson, and Siemaszko "17 Killed in Mass Shooting."

[81] Segarra, et al., "Calls Regarding Suspect."

[82] Carol Marbin Miller and Kyra Gurney, "Shooter Revealed Gory Fantasies to His Therapists Years before the Parkland Massacre," *Miami Herald*, March 10, 2018, www.miamiherald.com/news/local/crime/article204450699.html.

[83] Miller and Gurney.

[84] Miller and Gurney.

[85] Jose Pagliery and Curt Devine, "School Shooter Showed Violence and Mental Instability at Home, Police Reports Reveal," CNN, February 17, 2018, https://www.cnn.com/2018/02/16/us/florida-shooter-cruz-records-police-calls-to-home-invs/index.html.

[86] Pagliery and Devine.

There were many potential opportunities for law enforcement or the medical community to disrupt Cruz's plans—from tips that allegedly were not followed up on to information the therapists possessed, such as observations of Cruz's behavior and statements that Cruz made to the therapists, which could have been used in a threat assessment.[87] Law enforcement had many interactions with Cruz over the years, but without access to his mental health counseling records and detailed information about his violent tendencies, they were at a disadvantage when it came to completing a threat assessment. In cases such as this, it is imperative that law enforcement and the medical community work together to protect not only the individual, but society as well.

B. THREAT ASSESSMENT FRAMEWORKS AND TOOLS

The United States Secret Service's National Threat Assessment Center (NTAC) conducted an analysis of mass-casualty attacks that took place across the United States in 2017. The analysis included attacks that occurred in public and that injured at least three people. In all, twenty-eight attacks were analyzed. The NTAC found that 54 percent of the attackers had behavioral health issues, including drug or substance abuse, and 64 percent had a history of mental health symptoms, including "psychosis (e.g., paranoia, hallucinations, or delusions) and suicidal thoughts" (see Table 1).[88]

---

[87] Miller and Gurney, "Shooter Revealed Gory Fantasies."

[88] National Threat Assessment Center (NTAC), *Mass Attacks in Public Spaces—2017* (Washington, DC: Department of Homeland Security, March 2018), 3, www.secretservice.gov/forms/USSS_NTAC-Mass_Attacks_in_Public_Spaces-2017.pdf.

Table 1. Mental Health Symptoms: Mass-Casualty Attack Perpetrators, 2017[89]

Mental Health Symptoms	*n*
Psychotic Symptoms	***9***
Paranoia	*6*
Hallucinations	*6*
Delusions	*2*
Suicidal Thoughts	***6***
Depression	***4***

The NTAC also discovered that, even in cases for which the perpetrators had subscribed to an ideology that contributed to the attack, "their particular psychosis played a dominant role in the adoption of their belief system."[90]

The NTAC also published a review of attacks on the federal government between 2001 and 2013. In this document, NTAC refers to guidelines it previously published for state and local law enforcement in January 2000 that contain areas, or concepts, to be considered during a threat assessment investigation, one of which is the "history of mental illness."[91] In the current document, NTAC suggests investigators "ask detailed questions to explore the link between mental health symptoms and an individual's motive and behavior," specifically, "whether they impact the person's decision to carry out an attack."[92] The NTAC contends that it is important to determine what "community systems" might have information such as "concerning behaviors, mental health symptoms, stressors,

---

89 Source: NTAC. There appears to be a minor discrepancy between the text, which states that "Nearly two-thirds of the attackers (*n* = 18, 64%) experienced mental health symptoms prior to their attacks," and the table, which shows nineteen individuals.

90 NTAC, 4.

91 NTAC, *Attacks on Federal Government: 2001–2013* (Washington, DC: Department of Homeland Security, December 2015), 1, https://www.secretservice.gov/data/protection/ntac/Attacks_on_Federal_Government_2001-2013.pdf.

92 NTAC, ii, 8.

and other relevant background information" about the subject of a threat assessment.[93] The NTAC also recognizes that state and federal laws, including HIPAA and FERPA, may inhibit a threat assessment team's access to certain records, such as those from colleges or mental health facilities. The NTAC noted that "unlike judicial or law enforcement records, the disclosure of educational, employment, and mental health records generally requires either the consent of the individual under investigation or an express statutory or regulatory exception."[94]

Another concept to take into account in threat assessment is leakage. Leakage is defined by J. Reid Meloy and Mary Ellen O'Toole as "the communication to a third party of an intent to do harm to a target."[95] Leakage may occur during a medical appointment, whether to a mental health or medical professional. In some cases, this leakage could trigger a duty to warn. However, the duty to warn, which is discussed further in Chapter III, is only applicable in cases of an imminent threat and is not mandatory in all states. Notification of leakage by a medical provider to law enforcement would allow law enforcement to address the validity of the information through other sources such as family members, community members, or the individual of concern.

Michelle Keeney and Lina Alathari contend that local law enforcement is a necessary component for threat assessments. They elaborate, "prevention efforts are more effective when community partners collaborate to include law enforcement, behavioral and mental health services, social services, local citizens and others."[96] Law enforcement has historically been reactive, responding or investigating after a crime has been committed. In contrast, "proactive policing is getting out in front of events in the hopes of preventing

---

[93] NTAC, 12.

[94] NTAC, 12.

[95] J. Reid Meloy and Mary Ellen O'Toole, "The Concept of Leakage in Threat Assessment," *Behavioral Sciences and the Law* 29, (June 2011): 514, onlinelibrary.wiley.com/doi/abs/10.1002/bsl.986.

[96] Michelle Keeney and Lina Alathari, "Preventing Violent Attacks on Government Facilities and Personnel," *Sheriff & Deputy* (July/August 2016): 53, https://www.secretservice.gov/data/protection/ntac/Preventing-Violent-Attacks-on-Government.pdf.

crimes and working with the community to reduce crimes."[97] The nature of violent attacks in the United States makes law enforcement community relations, including those with medical professionals, more important than ever.

C. CONCLUSION

While the incidents described in this chapter concern individuals with mental health disorders, behavioral health issues or other medical conditions could also contribute to behavior that would cause an individual to commit violent acts in the community. Regardless of the cause of the threatening behavior, when medical personnel learn of a potential threat to the community, even if it is not imminent, there needs to be a mechanism for them to share the information with law enforcement. If law enforcement receives a tip related to a threat by an individual, they need a mechanism to collect all relevant information in order to assess the validity of the threat. If law enforcement is aware that the individual is seeking treatment for a behavioral or mental health issue, they should be able to collaborate with the medical professional treating the subject of the tip in order to more fully assess the potential for violence. The ability to conduct an accurate threat assessment depends on the analysis of all existing information about a subject's previous behavior and medical conditions. A lack of information sharing between the medical community and law enforcement is often attributable to privacy laws, including provisions within HIPAA and FERPA, which are explored in the next chapter.

[97] David B. Muhlhausen, "Director's Corner: Proactive Policing—What We Know and What We Don't Know, Yet," National Institute of Justice, January 17, 2018, https://nij.gov/about/director/Pages/muhlhausen-proactive-policing.aspx.

III. FACTORS THAT AFFECT INFORMATION SHARING

Though medical practitioners may have information that could potentially disrupt a violent attack or explain a person's abnormal behavior, depending on the nature of the incident—such as whether or not it is imminent—laws including HIPAA, FERPA and 42 Code of Federal Regulations (CFR) Part 2 may limit the information that can be shared with law enforcement. HIPAA and 42 CFR Part 2 both allow disclosures mandated by state laws, such as in cases of child abuse.[98] Privacy concerns, ethical guidelines, and organizational culture also may impact information sharing between the medical community and law enforcement. The law enforcement community may have biases about the mental health community, and vice versa, that prevent them from sharing information and working together. Mark K. Munetz and Jennifer L.S. Teller discuss these challenges. They suggest that the mental health community sees law enforcement as too rigid in their thinking—officers are unable to understand the inability of those with mental health problems to control their actions; whereas law enforcement may see the mental health community as strange and unwilling to hold those with mental illness accountable.[99] This chapter explores barriers to information sharing in more detail.

A. PRIVACY CONCERNS

1. United States Constitution

The Fourth Amendment of the United States Constitution protects against unreasonable searches and seizures. The U.S. Supreme Court has declared that the Fourth Amendment "establishes an inferred right to privacy."[100] The Fourth Amendment requires

---

[98] John Petrila and Hallie Fader-Towe, *Information Sharing in Criminal Justice–Mental Health Collaborations: Working with HIPAA and Other Privacy Laws* (New York: The Council of State Governments Justice Center, 2010), 7, https://www.bja.gov/Publications/CSG_CJMH_Info_Sharing.pdf.

[99] Mark K Munetz and Jennifer L.S. Teller, "The Challenges of Cross-Disciplinary Collaborations: Bridging the Mental Health and Criminal Justice Systems," *Capital University Law Review* 32, no. 4 (June 22, 2004): 936.

[100] Devon T. Unger, "Minding Your Meds: Balancing the Needs for Patient Privacy and Law Enforcement in Prescription Drug Monitoring Programs," *West Virginia Law Review 117*, no. 345 (Fall 2014): 5.

law enforcement to obtain a warrant in most cases before invading an individual's privacy, though there can be exceptions.[101] Privacy rights can apply to physical items as well as non-physical items.[102] Medical information and the doctor–patient relationship have typically been included in this privacy right and are impacted by "laws requiring doctors to report treatment information to receive public healthcare funds, laws establishing PDMPs [prescription drug monitoring programs], and programs that disclose medical information to law enforcement."[103]

2. Ethics for Medical Personnel

Privacy and confidentiality are ingrained in the training and professional conduct of doctors and other medical personnel. Ethics guidelines for various medical specialties include privacy and confidentiality considerations.[104] The American Medical Association's "Principles of Medical Ethics" states that "a physician shall respect the rights of patients, colleagues and other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law."[105] Most physicians pledge to uphold an oath—which is based upon the Hippocratic Oath—upon graduating from medical school or being licensed as a physician.[106] Modern versions include the "Yale Oath" or "Weill Cornell Medical College Hippocratic Oath," both of which contain a component relating to the confidentiality of patient information.[107] Doctors have an ethical duty to protect patients' confidential information, and their allegiance is to their patients

---

101 Unger, 5.

102 Unger, 5.

103 Unger, 5.

104 John C. Moskop et al., "From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine – Part I: Conceptual, Moral and Legal Foundations," *Annals of Emergency Medicine* 45, no.1 (January 2005): 53, https://doi.org/10.1016/j.annemergmed.2004.08.008; Elizabeth Henderson, "Potentially Dangerous Patients: A Review of the Duty to Warn," *Journal of Emergency Nursing* 41, no. 3 (May 2015): 193, http://dx.doi.org/10.1016/j.jen.2014.08.012.

105 "AMA Principles of Medical Ethics," American Medical Association, accessed July 17, 2018, https://www.ama-assn.org/delivering-care/ama-principles-medical-ethics.

106 Erich H. Loewy, "Oaths for Physicians—Necessary Protection or Elaborate Hoax," *Medscape General Medicine* 9, no. 1 (January 2007), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1925028/?report=printable.

107 Loewy, 2–3.

first and foremost. When law enforcement seeks information about a patient's confidential medical information, which doctors would not normally disclose, it can put the doctor's oath at odds with law enforcement and societal needs.

B. LAWS THAT AFFECT MEDICAL INFORMATION SHARING

Laws that affect the medical community's ability to share with law enforcement fall into two categories: laws relating to all medical information and laws relating only to behavioral and mental health information. HIPAA relates to medical information in general, and 42 CFR Part 2—as well as some state duty-to-warn laws—is specific to behavioral or mental health–related data. Laws relating to a mental health diagnosis are even more restrictive than those relating to other types of medical information. These restrictions may be attributable to the potential harm caused by stigmas associated with mental illness. Patrick W. Corrigan, Benjamin G. Druss, and Deborah A. Perlick note that those with mental illness may be labeled as dangerous or incompetent.[108] Additionally, "believing that people with mental illness are dangerous leads to fear, to employers not wanting to hire them or to primary care providers offering below-standard medical care."[109] To complicate matters further, existing laws that have exceptions allowing information sharing, even if only during an imminent threat, may only apply to certain categories of medical providers such as psychiatrists or psychologists.

Mental illness affects a significant portion of the population: one in five individuals.[110] While the majority of people who have mental illness are not violent, the National Institute of Mental Health's "Epidemiologic Catchment Area" study determined that, on an annual basis, those with mental health disorders experienced a relative risk of

---

[108] Patrick W. Corrigan, Benjamin G. Druss, and Deborah A. Perlick, "The Impact of Mental Illness Stigma on Seeking and Participating in Mental Health Care," *Psychological Science in the Public Interest* 15, no.2 (2014): 42, https://doi.org/10.1177/1529100614531398.

[109] Corrigan, Druss, and Perlick,: 42–43.

[110] Barbara Atwell, "Rethinking the Childhood-Adult Divide: Meeting the Mental Health Needs of Emerging Adults," *Albany Law Journal of Science and Technology* 25, no. 1 (2015): 1.

violence of 7 percent, compared to the average population's risk of 2 percent.[111] Deinstitutionalization of individuals with mental health disorders means that "mental health needs often go unmet."[112] It also increases the chances of law enforcement interacting with an individual who may display specific behavior associated with a mental health diagnosis. Law enforcement often does not have information pertaining to an individual's diagnosis; this information would help explain the individual's behavior, which would in turn help law enforcement determine if the individual is a threat.

Stigmas attached to mental illness and behavioral health problems, and a lack of insurance, leave many people in need of services without treatment. In recent years, emergency departments, primary care doctors, and nurses have become more likely to be the only practitioners an individual with behavioral or mental health symptoms seeks. This was recognized by a nurse at Massachusetts General Hospital, who wrote in 2015 that

> significant changes in the infrastructure of the American health care system have resulted in the reduction of resources and services available to persons seeking or in need of mental health services, resulting in the utilization of emergency departments as a source of primary mental health care. ED [emergency department] nurses, as frontline health care providers, are in a unique position to have an impact on the safety of the individual, the staff, and the community when working with patients who present a danger to themselves or others.[113]

As of 2018, this still holds true: there have been no significant changes in health care since 2014.

---

[111] Jeffrey W. Swanson, E. Elizabeth McGinty, Seena Fazel, and Vickie M. Mays, "Mental Illness and Reduction of Gun Violence and Suicide: Bringing Epidemiologic Research to Policy," *Annals of Epidemiology* 25 (2015): 368, http://dx.doi.org/10.1016/j.annepidem.2014.03.004.

[112] Atwell, "Rethinking the Childhood-Adult Divide," 1.

[113] Henderson, "Potentially Dangerous Patients," 193.

1. HIPAA

The federal regulation that most law enforcement and medical professionals are familiar with is HIPAA. HIPAA was enacted by the U.S. Congress in 1996 in order to provide certain protections related to health insurance and health care information.[114] It provides for protection of electronic medical information, seeks to combat fraud, protects PHI, and allows individuals to maintain health insurance upon leaving a job.[115] The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) dictates how "covered entities," which include "health care providers, health plans and health care clearinghouses," use and disclose PHI.[116] Information about an individual's mental health that is provided by non-medical stakeholders, such as a family member or friend, is not affected by HIPAA.[117] HIPAA does not prohibit law enforcement officers from sharing information about a person's medical conditions, as they "are not 'covered entities' under HIPAA."[118]

The Privacy Rule defines six "law enforcement purposes"—specific circumstances, under which PHI can be shared with law enforcement.[119] The first two exceptions include mandated disclosure due to search warrants or other court orders, and disclosure to help law enforcement track missing victims, criminals, or witnesses.[120] The other four exceptions relate to the commission of a crime, including: reporting a death that is believed to be caused by a crime; a formal inquiry about a known or suspected crime victim; PHI

---

114 Esther Seitz, "Privacy (or Piracy) or Medical Records: HIPAA and Its Enforcement," *Journal of the National Medical Association* 102, no. 8 (August 2010): 745, https://doi.org/10.1016/S0027-9684(15)30651-9.

115 "Health Insurance Portability and Accountability Act," California Department of Health Care Services, accessed July 17, 2018, www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx.

116 Seitz, "Privacy (or Piracy) or Medical Records," 746; "Summary of the HIPAA Privacy Rule," U.S. Department of Health and Human Services, accessed July 17, 2018, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

117 Petrila and Fader-Towe, *Information Sharing in Criminal Justice*, 5.

118 Petrila and Fader-Towe, 5.

119 U.S. Department of Health and Human Services, "HIPAA Privacy Rule."

120 U.S. Department of Health and Human Services.

related to the commission of a crime at the covered entity's location; and "by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime."[121]

HIPAA also permits providers to report PHI when required by other laws, such as child abuse or gunshot injuries.[122] If state law is contrary to the Privacy Rule, the Privacy Rule supersedes state law.[123] The Privacy Rule limits law enforcement's ability to receive medical information that could be used in a threat assessment, or that may explain an individual's behavior before a violent incident occurs; the exceptions that enable release of information only apply once a crime has already been committed. Violations of the HIPAA privacy rule may result in civil or criminal penalties, including fines of up to $250,000 and up to ten years in jail.[124] Providers may be fearful of these penalties; however, only fifty-five fines have been imposed out of more than 184,000 complaints since the inception of HIPAA.[125]

Furthermore, there are misconceptions about what information is legally allowed to be shared under HIPAA, "which has resulted in practitioner's misapplying the law to be far more restrictive than the actual regulatory language requires."[126] For example, police took a suspect who was under arrest to the hospital for medical care and later found out the

---

121 U.S. Department of Health and Human Services,.

122 "Guidelines for Releasing Patient Information to Law Enforcement," American Hospital Association, accessed June 24, 2018, https://www.aha.org/system/files/2018-03/guidelinesreleasing info.pdf.

123 U.S. Department of Health and Human Services, "HIPAA Privacy Rule."

124 "HIPAA Violations & Enforcement," American Medical Association, accessed July 28, 2018, https://www.ama-assn.org/practice-management/hipaa-violations-enforcement.

125 "Enforcement Highlights," U.S. Department of Health and Human Services, accessed July 28, 2018, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

126 Petrila and Fader-Towe, *Information Sharing in Criminal Justice*, viii.

subject was released without their knowledge.[127] The hospital claims that HIPAA regulations would not allow them to share the information about the patient's release.[128] This is a misapplication of HIPAA; since the suspect was in custody, HIPAA privacy rules did not apply.

2. FERPA

FERPA is a federal law that governs the privacy of students' education records at schools that receive federal funding from the U.S. Department of Education, making it applicable to "virtually all public schools … and most private and public postsecondary institutions."[129] Education records in elementary and high schools include information about a student's immunizations and school nurse records.[130] At the college level, records relating to "medical and psychological treatment" may or may not be considered "education records," depending on the situation.[131] These records are considered "treatment records" when they are strictly used in conjunction with the student's treatment and only viewed by the medical professionals administering the treatment.[132] Treatment records may be disclosed "with the student's written consent," which may include prior consent.[133] Treatment records that are disclosed to anyone other than providers administering treatment "are 'education records' under FERPA."[134]

---

[127] John Petrila, "Dispelling the Myths about Information Sharing Between the Mental Health and Criminal Justice Systems," The CMHS National GAINS Center for Systemic Change for Justice-Involved People with Mental Illness, February 2007, 1, www.pacenterofexcellence.pitt.edu/documents/Dispelling_Myths-5.pdf.

[128] Petrila, 1.

[129] U.S. Department of Health and Human Services and U.S. Department of Education, "Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records," U.S. Department of Education, November 2008, 1, https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf.

[130] Departments of Health and Human Services and Education, 2.

[131] Departments of Health and Human Services and Education, 2.

[132] Departments of Health and Human Services and Education, 2.

[133] Departments of Health and Human Services and Education, 2.

[134] Departments of Health and Human Services and Education, 8.

FERPA is unique in that, until a student is eighteen years of age, the student's parent must give consent to release education records; if the student is eighteen years or older, the student must consent.[135] FERPA provides an exception in which education records may be released "to appropriate parties, which may include law enforcement" without consent of the appropriate party, parent or student, "if knowledge of the information is necessary to protect the health or safety of the student or other individuals."[136] FERPA does not apply to behavior or conversations that non-medical staff, such as professors, observe and does not preclude those parties from sharing that information with law enforcement.[137]

The FERPA emergency exception is vague, and the concept of "necessary to protect the health or safety of the student or other individuals" is subjective. The literature has shown that poor understanding about FERPA means that "educators often err on the side of caution even in situations when public safety is at risk."[138]

3. 42 CFR Part 2

42 CFR Part 2 is a federal law that protects the disclosure of data related to treatment programs for substance abuse if they are "federally assisted."[139] Almost every substance abuse program receives federal assistance of some kind, making 42 CFR Part 2 relevant to most every substance abuse program.[140] The regulation applies "to organizations whose sole purpose is to diagnose and treat substance use disorders, as well as units within larger organizations such as a clinic within a jail, prison, or hospital."[141] Law enforcement officers are not "a 'federally assisted program' within the meaning of 42

---

135 Richard Brusca and Colin Ram, "A Failure to Communicate: Did Privacy Laws Contribute to the Virginia Tech Tragedy?," *Washington and Lee Journal of Civil Rights and Social Justice* 17, no. 141 (Fall 2010): 3.

136 Departments of Health and Human Services and Education, 4, 10.

137 Davis, "Connecting the Dots," 11.

138 Davis, 11.

139 "Basics of 42 CFR, Part 2," Justice and Health Connect, accessed July 17, 2018, 1, www.jhconnect.org/wp-content/uploads/2013/09/42-CFR-Part-2-final.pdf.

140 Justice and Heath Connect, 1.

141 Justice and Heath Connect, 1.

CFR Part 2."[142] Substance abuse, like mental or behavioral health treatment, is often stigmatized, or its disclosure may have a negative effect on an individual's personal or professional life.[143] Under 42 CFR Part 2, information about an individual's treatment may only be released with the patient's consent; however, the law allows an exception for medical professionals in cases of medical emergency, defined as "for the purpose of treating a physical or mental health condition that poses an immediate threat to the individual's health."[144]

Unlike HIPAA, 42 CFR Part 2 does not have an automatic exception to share information with law enforcement in cases of an imminent threat.[145] In general, 42 CFR Part 2 requires law enforcement to get a court order to acquire medical information, unless a crime takes place at the substance abuse treatment facility or the patient has a medical emergency.[146] Essentially, this law impedes sharing any treatment information that could be used to determine if an individual poses a threat to the community.

4. State Duty-to-Warn Laws

Duty-to-warn laws are predicated on the California Supreme Court case *Tarasoff v. The Regents of the University of California*.[147] In the Tarasoff case, a patient made death threats against a certain—though unidentified—woman during a psychotherapist appointment, and the therapist did not warn the individual, who the patient then killed.[148] Even though the patient did not tell the therapist the name of the person he intended to harm, the court said that the therapist should have been able to determine the target's

---

142 Petrila and Fader-Towe, *Information Sharing in Criminal Justice*, 5.

143 Justice and Heath Connect, "Basics of 42 CFR, Part 2," 1.

144 Justice and Heath Connect, 2.

145 Justice and Heath Connect, 2.

146 Justice and Heath Connect, 3.

147 California Supreme Court Tarasoff v. The Regents of the University of California, 17 Cal. 3d 425 (1976).

148 Charles Patrick Ewing, "Tarasoff Reconsidered," *Monitor on Psychology* 36, no. 7 (July/August 2005): 112, http://www.apa.org/monitor/julaug05/jn.aspx.

identity.[149] The parents of the murdered woman sued the therapist for failing to warn their daughter, while the therapist argued that she only had a duty to her patient.[150] The court ruled that "if a therapist determines or reasonably should have determined 'that a patient poses a serious danger of violence to others, he bears a duty to exercise reasonable care to protect the foreseeable victim of that danger.'"[151]

Most states have duty-to-warn laws of some type, though they vary—for instance, some include nurses while others do not, and some are mandatory while others are voluntary.[152] Several options are available to medical providers acting upon the duty to warn. They can inform law enforcement and/or the potential victim of the threat, or they may have the patient committed.[153] The map in Figure 1 illustrates the U.S. states that have a duty to warn and those that do not, and if the duty is mandatory.

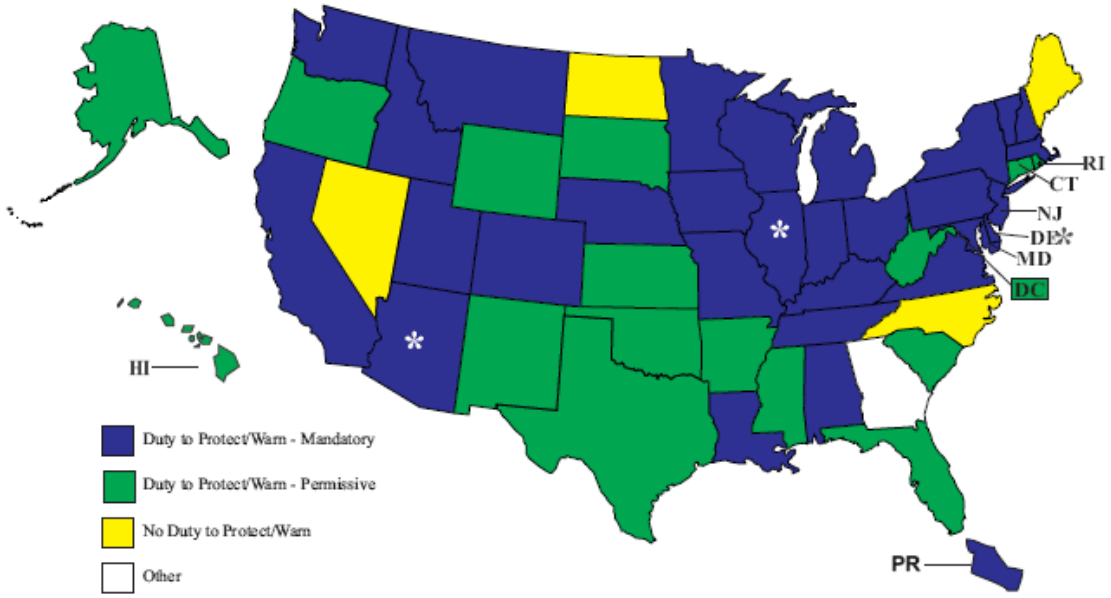
[149] Ewing, 112.

[150] Ewing, 112.

[151] Ewing, 112.

[152] Henderson, "Potentially Dangerous Patients," 193.

[153] Henderson, 193.



As of 2014, thirty-three states impose a mandatory duty to warn. The mandatory states include Arizona, California, Colorado, Delaware, Idaho, Indiana, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New York, Ohio, Pennsylvania, South Carolina, South Dakota, Tennessee, Utah, Vermont, Washington, Wisconsin, Alabama, Georgia, Hawaii, and North Carolina. Eleven states, Alaska, Connecticut, District of Columbia, Florida, Illinois, New York, Oregon, Rhode Island, Texas, West Virginia, and Wyoming, recognize *Tarasoff* as a legitimate piece of legislation, allowing but not mandating named professionals to warn potential victims. Six states, including Arkansas, Iowa, Kansas, Maine, Nevada, and North Dakota, have not yet addressed the issue of duty to warn and currently have no law pertaining to the subject. Lastly, only one state, Virginia, does not recognize the duty to warn.[154]

Figure 1. Duty-to-Warn Laws by State[155]

[154] Source: Henderson, 193.

[155] "Mental Health Professionals' Duty to Warn," National Conference of State Legislatures, July 6, 2018, http://www.ncsl.org/research/health/mental-health-professionals-duty-to-warn.aspx.

Some duty-to-warn laws are inadequate for several reasons, including the fact that some are not mandatory, and that some only include certain medical professionals. Laws that only include psychiatrists and psychologists are insufficient since many individuals suffering from mental health or behavioral health conditions may not ever seek treatment from a mental health professional, but may only interact with a primary care team or emergency department. Additionally, duty-to-warn laws may be ineffective in decreasing violent attacks; as shown in the Secret Service analysis of mass attacks in public spaces for 2017, 57 percent of the attacks were perpetrated against random victims.[156]

C. CONCLUSION

The regulations and policies examined in this chapter are designed to protect individuals' rights to privacy and protect their personal information. However, when these regulations are put into practice, they are usually interpreted in a narrower and more conservative manner than intended. The fear of retribution, whether legal or regulatory, causes practitioners to restrict information sharing, which impacts law enforcement's ability to prevent some violent attacks.

[156] NTAC, *Mass Attacks in Public Spaces*, 4.

IV. INTELLIGENCE / INFORMATION SHARING

This chapter explores intelligence and information sharing initiatives already in place that encourage or allow information sharing between the medical community and law enforcement. Some of the initiatives, such as fusion centers, may not have achieved the integration with the medical community that they strive to create. This may be partially attributable to the legal inability to share PHI with law enforcement unless there is an imminent threat and a state duty-to-warn law. Information sharing with fusion centers would allow law enforcement to more proactively identify suspicious activity before a violent incident occurs. Successful programs such as those relating to child abuse have been in existence for many years and have legislation that allows information sharing.

A. FUSION CENTERS

After the attacks of September 11, 2001, fusion centers began to emerge at the state and local level in order to bridge the gap between state and local information and federal information and intelligence.[157] Fusion centers may focus on all crimes, all hazards, all threats, or a combination of these. They are intended to be multi-disciplinary and may include law enforcement, public safety, public health, and even private sector representatives.[158] Because fusion centers are run either locally or by the state and are designed to serve the needs of their area of responsibility, no two fusion centers are exactly alike .[159] Fusion centers interact with both the Department of Homeland Security and the Federal Bureau of Investigation (FBI). As of 2018, every state has at least one fusion center.[160]

---

157 "State and Major Urban Are Fusion Centers—Unique Role," Department of Homeland Security, June 26, 2017, https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

158 U.S. Department of Justice, "Fusion Center Guidelines—Developing and Sharing Information and Intelligence in a New Era" (report, U.S. Department of Justice), 9, https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

159 "National Network of Fusion Centers Fact Sheet," Department of Homeland Security, June 21, 2017, https://www.dhs.gov/national-network-fusion-centers-fact-sheet.

160 "Fusion Center Locations and Contact Information," Department of Homeland Security, April 26, 2018, https://www.dhs.gov/fusion-center-locations-and-contact-information.

Fusion centers play a central role in the Nationwide Suspicious Activity Reporting Initiative (NSI); many fusion centers serve as the central repository for Suspicious Activity Reports (SARs).[161] This responsibility includes determining whether suspicious activity warrants further investigation. The NSI is a collaborative effort of local, state, tribal, territorial, and federal law enforcement to collect and analyze suspicious behavior that may have a nexus to preoperational planning for a terrorist incident or other criminal activity.[162] SARs are not based on an individual's race, religion, or ethnicity; rather, they are based on behaviors, some of which are criminal and some of which are not.[163] These behaviors are defined in the Information Sharing Environment SAR Functional Standard, the most recent being version 1.5.5.[164]

SARs can be forwarded to fusion centers by law enforcement or members of the public who see suspicious behavior. Upon receipt of a SAR, analysts or investigators in the fusion center vet the SAR by accessing all legally accessible, relevant data sets as well as open-source information in order to determine if the report is valid.[165] If it is determined that the SAR is in line with the Information Sharing Environment SAR Functional Standard, the SAR may be passed to the FBI's Joint Terrorism Task Force for further investigation.[166] In addition, the SAR may be entered into eGuardian, the FBI's unclassified system for tips and leads, which can be accessed by local, state, tribal, territorial, and federal law enforcement in order to vet additional suspicious activities related to the same subject, or to identify patterns and trends of behavior.[167]

---

161 "About the NSI," Nationwide SAR Initiative (NSI), accessed July 11, 2018, https://nsi.ncirc.gov/about_nsi.aspx.

162 NSI.

163 "Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5.," Nationwide SAR Initiative, accessed July 11, 2018, 10, https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf.

164 NIS, "About the NSI."

165 NSI, "ISE Functional Standard," 10.

166 NSI, 11.

167 "eGuardian," Federal Bureau of Investigation, accessed July 11, 2018, https://www.fbi.gov/resources/law-enforcement/eguardian.

When vetting a SAR, it is imperative that the fusion center has access to all available data in order to accurately assess the report's validity. In contrast to the threat assessment process detailed by the NTAC, which involves a multi-disciplinary approach, the SAR process is focused on law enforcement participation to conduct comprehensive threat assessments.[168] SAR training teaches law enforcement to understand the "difference between innocent cultural behaviors and behavior indicative of criminal activity."[169] Since SARs are focused on behaviors that may indicate criminal or terrorist activity, it is important to understand the factors that influence an individual's behavior, including medical diagnoses.

Many of the SARs received at fusion centers involve individuals considered to be emotionally disturbed persons (EDPs). Law enforcement uses the term EDP "to describe a person with emotional, mental, or erratic behavior that affects their decision-making process that may include hurting themselves or others."[170] Though statistics are not available related specifically to how many SARs involve EDPs, the literature addresses law enforcement response to and interactions with EDPs. *Police Magazine* provides a guide titled "How to Respond to an Emotionally Disturbed Person," which suggests that law enforcement is "on the frontlines" of interactions with EDPs, who are "seven times more likely to encounter law enforcement" than individuals without mental illness; further, an EDP's mental illness may affect the individual's "thoughts, mood, behavior and the way they perceive the world around them."[171] Restrictions on sharing medical information, as described in the previous chapter, are detrimental to fusion centers, as they limit the center's ability to determine if a subject's behavior is truly a threat, or if it is due to behavioral or mental health issues.

---

168 Program Manager, Information Sharing Environment (PM-ISE), *Nationwide Suspicious Activity Reporting Initiative Status Report* (Washington, DC: Office of the Director of National Intelligence, 2010), 13, https://www.dni.gov/files/ISE/documents/DocumentLibrary/SAR/NSI_Status_Report_FINAL_2010-02-03.pdf.

169 PM-ISE, 17.

170 Amaury Murgado, "How to Respond to an Emotionally Disturbed Person," *Police Magazine*, May 12, 2017, http://www.policemag.com/channel/patrol/articles/2017/05/how-to-respond-to-an-emotionally-disturbed-person.aspx.

171 Murgado.

1. Public Health Participation in Fusion Centers

There has been a concerted effort to incorporate public health into fusion centers, including public health partners and data. An appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers* published in 2011 addresses the integration.[172] This document indicates that public health and health care personnel are able to "provide fusion centers with information on criminal acts and/or terrorism precursors," which is further defined to include "suspicious symptoms and/or abnormal environmental conditions that may be caused by an emergent disease or agent or abnormal patterns and trends indicative of the production or abuse of narcotics."[173] The focus is on disease surveillance, with little to no focus on integrating medical information that may be useful in determining an individual's capacity to commit a violent criminal act.

The Department of Homeland Security's Health Security Intelligence Enterprise (HSIE) was created with the goal "to make the nation safer from all crimes and all hazards, through timely and appropriate exchange of information among healthcare, public health community, and other multi-disciplinary partners, including the Intelligence Community, law enforcement, fire service, emergency management and private sector."[174] The HSIE does mention the public health sector as a contributor, stating that its role is to "use the appropriate protocols to share information with a fusion center on suspicious activity or criminal/terrorism indicators and warnings."[175] Though suspicious activity is mentioned, the areas for collaboration tend to focus on pandemic outbreaks and chemical, biological, radiological, and nuclear (CBRN) monitoring. This is further evidenced by a National Governors Association issue brief on *Improving Preparedness through Sharing Public Health and Homeland Security Information*, which touts the work at two fusion centers, the Central Florida Intelligence Exchange and the Colorado Intelligence and Analysis

---

[172] U.S. Department of Justice, *Health Security: Public Health and Medical Integration for Fusion Centers* (Washington, DC: U.S. Department of Justice, 2011), 1, https://it.ojp.gov/GIST/159/Health-Security--Public-Health-and-Medical-Integration-for-Fusion-Centers.

[173] U.S. Department of Justice, 2.

[174] Department of Homeland Security Office of Health Affairs, "Health Security Intelligence Enterprise" (PowerPoint presentation, Department of Homeland Security, 2012), slide 3.

[175] Department of Homeland Security Office of Health Affairs, slide 6.

Center.[176] Both fusion centers were recognized for utilizing public health data to ensure officer safety by providing guidelines for safely handling crime scenes that involve a suicide committed with hazardous materials.[177] The information shared was limited to proper handling of hazardous materials and did not include any PHI or specific medical information.

In support of outreach for the NSI SAR program, the Department of Homeland Security has developed a series of videos for law enforcement or other public safety communities that can either be viewed online or on CDs, and that fusion centers can use to train their partners.[178] The videos are designed to help the viewers identify types of behavior that indicate preoperational planning for criminal activity or a terrorist event. One of the CDs is geared toward the emergency medical services (EMS) community.[179] However, laws and policies—such as HIPAA, barring exceptions—may prohibit EMS technicians from sharing observations with law enforcement if they involve PHI.

B. OTHER PROGRAMS THAT ENABLE INFORMATION SHARING BY MEDICAL PROVIDERS

In some cases, medical providers are permitted to disclose a patient's PHI to law enforcement. These instances include cases of child or elder abuse, injuries sustained by gunshots or knives, and prescription monitoring programs. Additionally, public health regulations often require medical professionals to report cases of certain diseases to prevent outbreaks.

---

176 David Henry, *Improving Preparedness through Sharing Public Health and Homeland Security Information* (Washington, DC: National Governors Association, 2012), 3, https://www.nga.org/files/live/sites/.../1212ImprovingPreparedness_IssueBrief.pdf.

177 Henry, 3.

178 "Online SAR Training for Law Enforcement and Hometown Security Partners," NSI, accessed July 11, 2018, https://nsi.ncirc.gov/training_online.aspx.

179 NSI.

1. Child Abuse

The Child Abuse Prevention and Treatment Act (CAPTA) was first enacted in 1974 and has been reauthorized eight times since, most recently in 2015.[180] Every state in the United States has a state-specific child abuse law, and no two are alike.[181] The need to protect children from abuse takes priority over patient confidentiality in the majority of state child abuse laws; the laws require doctors who suspect a child has been abused or neglected to report the allegations to the state's authority on child abuse.[182] Law enforcement and child protective services usually have the responsibility for investigating child abuse allegations.[183] Under the HIPAA privacy rule, "child abuse or neglect may be reported to any law enforcement official authorized by law to receive such reports."[184] In cases where law enforcement is not a reporting agency, doctors may still provide PHI to law enforcement in cases of imminent harm to the child or when investigating a missing child.[185] Reports of child abuse or neglect usually occur after a suspected crime has been committed, when the medical professional detects evidence of the abuse.

---

[180] "The Child Abuse Prevention and Treatment Act Including the Justice for Victims of Trafficking Act of 2015 and the Comprehensive Addiction and Recovery Act of 2016," U.S. Department of Health and Human Services, accessed July 3, 2018, 4, https://www.acf.hhs.gov/sites/default/files/cb/capta2016.pdf.

[181] Debra Schilling Wolfe, "Revisiting Child Abuse Reporting Laws," *Social Work Today* 12, no. 2 (March/April 2012): 14, http://www.socialworktoday.com/archive/031912p14.shtml.

[182] Wolfe; "Policy Statement—Child Abuse, Confidentiality, and the Health Insurance Portability and Accountability Act," *Pediatrics* 125, no. 1 (January 2015), 199, http://pediatrics.aappublications.org/content/125/1/197.full-text.pdf.

[183] American Academy of Pediatrics, "Policy Statement—Child Abuse, Confidentiality, and the Health Insurance Portability and Accountability Act," *Pediatrics* 125, no. 1 (January 2015), http://pediatrics.aappublications.org/content/125/1/197.full-text.pdf.

[184] "When Does the Privacy Rule Allow Covered Entities to Disclose Protected Health Information to Law Enforcement Officials?," U.S. Department of Health and Human Services, July 23, 2004, https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.

[185] American Academy of Pediatrics, "Policy Statement," 199.

2. Prescription Drug Monitoring Programs (PDMPs)

According to the Centers for Disease Control and Prevention, "a prescription drug monitoring program (PDMP) is an electronic database that tracks controlled substance prescriptions in a state."[186] Data from PDMPs can be used to assess the extent of prescription drug problems in a state, such as the opioid crisis, and inform response strategies.[187] Prescription drug monitoring programs are intended to detect "inappropriate prescribing trends" and patients who may be getting prescriptions for the same or similar medication from more than one doctor at a time.[188] Studies measuring the effectiveness of PDMPs found some evidence of "changes in prescribing behaviors, use of multiple providers by patients, and decreased substance abuse treatment admissions."[189] The first prescription drug monitoring program began in California in 1939 and by 1992 there were PDMPs in ten states.[190] By 2014, thirty-nine states had PDMPs.[191]

Federal support for state PDMPs is provided through legislation called the National All Schedule Prescription Electronic Reporting Act (NASPER), which was passed in 2005 and reauthorized in 2016.[192] Courts have determined that it can be necessary to disclose medical information to a variety of medical personnel for a "legitimate governmental purpose," even if it "reflects unfavorably on the character of the patient," when the public interest outweighs privacy expectations.[193] More than twenty states allow law enforcement

---

186 "What States Need to Know about PDMPs," Centers for Disease Control and Prevention, October 3, 2017, https://www.cdc.gov/drugoverdose/pdmp/states.html.

187 Centers for Disease Control and Prevention.

188 Centers for Disease Control and Prevention.

189 Centers for Disease Control and Prevention.

190 Unger, "Minding Your Meds," 2.

191 Unger, "Minding Your Meds," 2.

192 "National All Schedules Prescription Electronic Reporting Act," American Society of Interventional Pain Physicians, accessed June 24, 2018, http://nasper.org/.

193 Unger, "Minding Your Meds," 6

access to PDMP information for use in an investigation, after a crime has occurred, though a handful of states require a court order or subpoena.[194]

In February 2018, Senate Bill 2451, the Protection for Overprescribing Act, was introduced in Congress.[195] The bill, which has yet to be voted on, ties federal grant dollars to a state's analysis and sharing of PDMP data with law enforcement.[196] Medical information that is shared with law enforcement as a result of PDMPs is used to target the opioid crisis through criminal cases against physicians or patients. While abuse of prescriptions may lead to death and contributes to a public health crisis, individuals who abuse opiates are generally a threat to themselves as opposed to a violent threat to society.

3. Injuries Caused by Violence

Many states have laws that require doctors to report weapon-related injuries, such as gunshot or knife injuries—or other injuries that appear to have been inflicted during a criminal act—to law enforcement.[197] Some states also include injuries caused by domestic violence in this reporting requirement.[198] In fact, "forty-five states have laws that mandate physician reports of injuries caused by weapons, crimes, or domestic violence."[199] Physicians' awareness of weapon-related injury laws is not as widespread as awareness of child abuse reporting laws.[200] The reporting requirements vary greatly by state; some

---

194 The National Alliance for Model State Drug Laws, *Interstate Sharing of Prescription Monitoring Database Information* (Manchester, IA: National Alliance for Model State Drug Laws, 2016), http://www.namsdl.org/library/8C2F8F5B-F426-FC5F-226056040DF15FD6/.

195 Protection for Overprescribing Act, S. 2451, 115 Cong. 2 (2018), https://www.congress.gov/bill/115th-congress/senate-bill/2451?q=%7B%22search%22%3A%5B%22s.+2451%22%5D%7D&r=1

196 Protection for Overprescribing Act.

197 "Mandatory Reporting of Non-accidental Injuries: A State-by-State Guide," Victim Rights Law Center, 2014, https://www.victimrights.org/sites/default/files/Mandatory%20Reporting%20of%20Non-Accidental%20Injury%20Statutes%20by%20State.pdf (no page number included in forward).

198 Debra Houry et al., "Violence-Inflicted Injuries: Reporting Laws in the Fifty States," *Annals of Emergency Medicine* 39, no. 1 (2002): 57, https://doi.org/10.1067/mem.2002.117759.

199 Houry et al., 56.

200 Houry et al., 59.

states require reporting of burns, for example, and others require reporting only when a crime is involved.[201]

One such example is the Massachusetts Weapon Related Injury Surveillance System (WRISS), "an emergency department-based system that collects health information on persons treated for gunshot wounds or assault-related sharp instrument wounds."[202] Since 1994, WRISS has been collecting information about gunshots and "'criminally suspicious' sharp instrument wounds."[203] Reporting of violence-related injuries allows law enforcement to investigate crimes they may not know about otherwise; but, as with child abuse reporting, violence-related injury reporting programs are reactive in nature, providing notice after a criminal act has already occurred.[204]

C. MENTAL AND BEHAVIORAL HEALTH DATA SHARING

Though laws such as HIPAA and 42 CFR Part 2 restrict sharing data related to mental illness or behavioral health, there are some programs that allow the sharing of this information with public safety professionals in order to protect the public. These limited instances are discussed in this section.

1. Criminal Justice and Behavioral Health Collaborations

The criminal justice system shares information with behavioral or mental health providers in order to coordinate treatment. This is prevalent among corrections facilities to facilitate the care of inmates before and after trial as well as for integration back into society once an offender is released. A special provision within HIPAA allows disclosure of mental health records to the

---

201 Houry et al., 57.

202 "About the Weapon Related Injury Surveillance System (WRISS)," Mass.gov, accessed July 7, 2018, https://www.mass.gov/service-details/learn-more-about-wriss.

203 Mass.gov; Massachusetts Department of Public Health, *Weapon-Related Injuries to Massachusetts Residents 1994–2007: Findings from the Weapon Injury Surveillance System (WRISS)* (Boston: Massachusetts Department of Public Health, 2009), 1, http://archives.lib.state.ma.us/bitstream/handle/2452/50056/ocn477247709.pdf?sequence=1.

204 Houry et al., "Violence-Inflicted injuries," 59.

> correctional institution or law enforcement official with custody of the individual, if the information is necessary for the provision of health care to the individual; the health and safety of the inmate, other inmates, or correctional officials and staff; the health and safety of those providing transportation from one correctional facility to another; for law enforcement on the premises of the correctional facility; and for the administration and maintenance of the safety, security, and good order of the facility. This general provision does not apply when the person is released on parole or probation or otherwise released from custody.[205]

This provision relates specifically to custody within, or transport to, a correctional facility. A related provision does not exist that would allow mental health records to be shared with law enforcement before an individual enters the criminal justice system.

2. Reporting Related to Gun Purchases

The Gun Control Act of 1968 requires background checks for those seeking to purchase guns, and declares that individuals who have been "adjudicated to be mentally defective or who have been committed to a mental institution are prohibited from possessing, shipping, transporting, and receiving firearms and ammunition."[206] The Brady Handgun Violence Protection Act of 1993 (also known as the Brady Act) required creation of an electronic database for use in background checks for gun purchases. This led to the creation of the National Instant Criminal Background Check System (NICS), which is maintained by the FBI and also contains information about those deemed to be mental defectives. The term *mental defectives* is further defined as

> individuals who have been involuntarily committed to a mental institution; found incompetent to stand trial or not guilty by reason of insanity; or otherwise have been determined by a court, board, commission, or other lawful authority to be a danger to themselves or others or to lack the mental capacity to contract or manage their own affairs, as a result of marked

---

[205] Petrila, "Dispelling the Myths," 2.

[206] Edwin Liu et al., *Submission of Mental Health Records to NICS and the HIPAA Privacy Rule*, CRS Report No. R43040 (Washington, DC: Congressional Research Service, 2013), summary, https://fas.org/sgp/crs/misc/R43040.pdf.

> subnormal intelligence or mental illness, incompetency, condition, or disease.[207]

In 2012, the Congressional Research Service found that "a variety of technological, coordination, and legal (i.e., privacy) challenges limit the states' ability to report mental health records to NICS."[208] These challenges include some state and federal privacy laws, including HIPAA, and outdated technology, as well as law enforcement's inability to access mental health records to share with NICS.[209] Additionally, the Congressional Research Service reported that, prior to 2013, Congress debated whether HIPAA or other privacy laws prohibited mental health data from being submitted to NICS.[210] Under the HIPAA privacy rule, a state mandate is the exception that allows states to report to NICS. The Congressional Research Service determined that "it is not clear that there are any other provisions in the privacy rule that provide such a permission."[211] Therefore, without a state mandate, reporting to NICS may not be allowed.

As of January 2013, the Congressional Research Service found that twenty-three states have laws requiring reporting to NICS.[212] An additional seven—Arizona, Florida, Missouri, Nebraska, New Jersey, Pennsylvania, and West Virginia—have laws that allow but do not require disclosure to NICS. Eight states—Arkansas, California, Hawaii, Massachusetts, Maryland, Michigan, Ohio, and Utah—do not have laws that mention NICS reporting at all, though they collect relevant data at the state level. The remaining twelve states and the District of Columbia do not collect any data that would be relevant to reporting to NICS.[213]

---

207 "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the National Instant Criminal Background Check System (NICS)," Federal Register, January 6, 2016, 382, www.federalregister.gov/documents/2016/01/06/2015-33181/health-insurance-portability-and-accountability-act-hipaa-privacy-rule-and-the-national-instant.

208 Liu et al., *Submission of Mental Health Records*, summary.

209 Liu et al., 7–8.

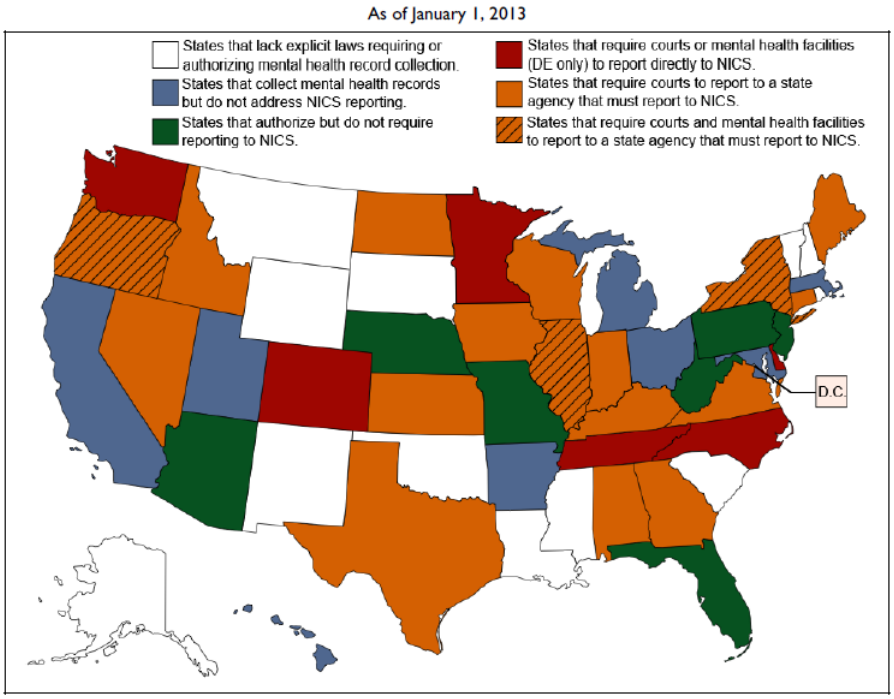
210 Liu et al., summary.

211 Liu et al., 11.

212 Liu et al., 11.

213 Liu et al., 12.

Additionally, while law enforcement generally provides the records to NICS, information about an involuntary commitment resides in medical records that law enforcement do not have access to.[214] Figure 2 depicts the state of reporting to NICS in January 2013.



Source: Prepared by CRS based on a review and analysis of laws in all 50 states and the District of Columbia that address the reporting of mental health records for use in firearm purchaser background checks.

Note: CRS's characterization of state laws is in broad agreement with a similar analysis by the Law Center to Prevent Gun Violence—a nonprofit organization that advocates for gun-control legislation and provides legal expertise and information on U.S. gun laws—but with one key difference. Whereas the Law Center characterized Virginia as a state that authorizes but does not require reporting to NICS, CRS concluded that Virginia's law requires NICS reporting. The Law Center's analysis is available at http://smartgunlaws.org/mental-health-reporting-policy-summary/.

Figure 2. State Laws that Require or Authorize the Reporting of Mental Health Records to NICS[215]

[214] Liu et al., 7.

[215] Source: Liu et al., 13.

In 2014, a new rule was proposed by the Department of Health and Human Services to facilitate the sharing of information by covered entities with NICS or "to a state repository of NICS data," which might be a law enforcement agency.[216] A final rule issued by the Department of Health and Human Services became effective in February 2016; this rule created an "express permission" within HIPAA that allows covered entities to report "individuals who are subject to a Federal 'mental health prohibitor' that disqualifies them from shipping, transporting, possessing, or receiving a firearm" directly to NICS or to the state agency responsible for reporting to NICS.[217] As of the date of this thesis, data relative to the effectiveness of this rule change was not available.

D. CONCLUSION

There are provisions in HIPAA and 42 CFR Part 2 that allow some medical information to be shared with law enforcement and other public safety agencies, under certain circumstances. Even when laws or programs are in place that allow information sharing to occur, however, there can be inadequacies—such as a lack of awareness or improper application of the involved legal requirements. In the case of the Virginia Tech gunman, for example, Cho's name was not entered into NICS due to a discrepancy between federal law and Virginia's understanding of what constitutes "involuntary commitment," which allowed Cho to purchase two weapons.[218]

The programs and laws addressed in this chapter allow information sharing when a suspected crime has already occurred or is imminent, such as in cases of child abuse, injuries caused by violence, and prescription drug abuse. In terms of sharing mental or behavioral health data, however, the allowable reasons for sharing are very narrow—either related to an individual who is incarcerated or to prevent individuals with certain illnesses from purchasing a firearm. These legal allowances and programs are insufficient; they do not allow law enforcement to obtain information that would assist in the threat assessment process to proactively address a threat to the community before an act of violence occurs.

---

216 Federal Register, "HIPAA," 386.

217 Federal Register.

218 Davis, "Connecting the Dots," 12.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. DISCUSSION AND RECOMMENDATIONS

The nature of violent attacks necessitates better coordination and integration of all relevant information about a subject's background, both criminal and medical, to inform threat assessments and ensure the safety of the public. A review of several relatively recent violent incidents in the United States has shown that the lack of information sharing between the medical community and law enforcement has contributed to law enforcement's inability to thwart attacks before they happen.

As previously stated, privacy laws and the public perception of privacy—especially in terms of mental health data—due to stigmas associated with mental illness are often at odds with the need to share information for legitimate law enforcement purposes. Also, the fear of retribution, whether legal or regulatory, causes practitioners to err on the side of caution and avoid sharing, which negatively affects law enforcement's ability to prevent some violent attacks.

Current laws and programs are insufficient to proactively address the threat of violence to the community. It is necessary to modify or create new statutory language to address legal barriers. Under these circumstances, this thesis provides several recommendations to amend the current legal framework in order to increase information sharing between the medical field and law enforcement.

1. Privacy Laws Are Deficient

Threat assessment guidelines recognize the importance of gathering information from non–law enforcement sources; the NTAC specifically includes "history of mental illness" as a necessary component of understanding an individual's behavior in order to ensure the most accurate threat assessment is compiled.[219] Dating back to the *Tarasoff* case in 1976, the California Supreme Court ruled that "if a therapist determines or reasonably should have determined 'that a patient poses a serious danger of violence to

[219] NTAC, *Attacks on Federal Government*, 1.

others, he bears a duty to exercise reasonable care to protect the foreseeable victim of that danger.'"[220] Though it would be impossible to prevent every violent attack, the more information available to conduct threat assessments may improve law enforcement's ability to preempt some attacks.

A lack of information sharing between the medical community and law enforcement is often attributable to federal or state privacy laws. Current laws that require information sharing are limited in some instances—applying only when there is imminent danger—and ambiguous in others, such as in the interpretation of FERPA laws relating to student records. In the absence of legal barriers, unfamiliarity with the laws or improper application of the laws may contribute to a lack of information sharing.

The after-action review following the Virginia Tech tragedy recommended that "Congress and the state legislatures should review federal and state privacy laws, and universities should know what they do and do not permit"; the review noted that HIPAA, FERPA, and state privacy laws should be reviewed to ensure that they are compatible and that they meet the real needs of our society.[221] More than ten years after the Virginia Tech tragedy, HIPAA and FERPA have not been amended.

(1) Recommendation #1: Privacy Laws Need to Be Evaluated and Amended

A legal analysis of privacy laws is necessary. This thesis reaffirms the suspicion that the laws are deficient and identifies gaps and limitations that inhibit the ability of law enforcement and the medical community to share medical information for threat assessment purposes. This thesis is a necessary precursor to conducting a comprehensive legal analysis of HIPAA, FERPA, 42 CFR Part 2, and state duty-to-warn laws. Legal analysis will determine whether any proposed amendments are necessary to preempt violent attacks against the community.

---

[220] Ewing, "Tarasoff Reconsidered," 112.

[221] Davis, "Connecting the Dots," 14–15.

Privacy advocates and citizens may view the increased ability for law enforcement to obtain medical information as a violation of an individual's civil rights. Another limitation may be the fact that each state's laws—such as duty-to-warn laws or mandatory reporting of medical information—are different. Any amendments to federal laws must take this into consideration.

(2) Recommendation #2: States Could Enact Laws That Mandate Information Sharing between the Medical Community and Law Enforcement

The HIPAA privacy rule permits providers to report PHI when required by other laws, such as in cases of child abuse or gunshot injuries.[222] 42 CFR Part 2 allows disclosures mandated by state laws.[223] States could enact individual laws that mandate information sharing between the medical community and law enforcement for the purposes of threat assessment, which would then allow release of the information under HIPAA and 42 CFR Part 2. Current state laws that enable the sharing of medical information for specific programs or purposes are not consistent among states. Each state would have to conduct its own legal analysis to determine how existing state and federal laws would impact any newly proposed laws or amendments. Privacy advocates would likely try to block these types of laws from being created.

2. Training on Privacy Laws Is Deficient

Insufficient training makes it difficult for law enforcement and the medical community to understand the specific provisions of each of the laws analyzed. For example, both HIPAA and 42 CFR Part 2 allow disclosures mandated by state law; but unlike HIPAA, 42 CFR Part 2 does not have an automatic exception to share information with law enforcement in cases of an imminent threat.[224] Additionally, law enforcement

---

[222] American Hospital Association, "Releasing Patient Information."

[223] Petrila and Fader-Towe, *Information Sharing in Criminal Justice*, 7.

[224] Petrila and Fader-Towe, 7; Justice and Heath Connect, "Basics of 42 CFR, Part 2," 2.

officers are not prohibited from sharing information about a person's medical conditions under HIPAA, as they are not considered "covered entities."[225]

(3) Recommendation #3: Training for Both Law Enforcement and the Medical Community

Misconceptions exist in both vocations regarding the current privacy laws that govern the ability to share medical information. For example, Virginia Tech believed that the university could not disclose Cho's disciplinary records to law enforcement due to FERPA.[226] Training should be provided to law enforcement and the medical community to ensure that they understand the specific circumstances governing when information sharing is allowable and the extent of the information that can be shared.

Opponents of training may argue that it is too expensive or time consuming. Training could be accomplished as a component of continuing education, such as in-service training for law enforcement, in which the cost could potentially be absorbed into work performed by already existing teaching staff and classroom facilities. Those in the medical community are already required to participate in continuing education by a licensing authority. Training on privacy laws could be offered for continuing medical education credits. Professional associations such as the American Medical Association or the International Association of Chiefs of Police (IACP) could offer training at conferences or provide reference materials about the applicability of the current laws to their constituencies. For example, the IACP conducts an annual conference that includes training seminars; conference registration costs as little as $425 for its members who register early, and as much as $725 for non-members who do not register early.[227] A review of the 2018 conference agenda shows twelve legal topics being offered.[228] A training block on the

---

225 Petrila and Fader-Towe, *Information Sharing in Criminal Justice*, 5.

226 Davis, "Connecting the Dots," 11.

227 "Registration Information," International Association of Chiefs of Police, accessed August 9, 2018, https://www.theiacpconference.org/event-overview/registration-category-and-fees/#site-navigation.

228 "Events," International Association of Chiefs of Police, accessed August 9, 2018, https://plan.core-apps.com/iacp2018/events?trackIds=2f717394f6594a422becdcebe6e05d82.

privacy laws that impact sharing medical information could be offered in a similar fashion at future conferences.

3. Collaboration between Law Enforcement and the Medical Community Is Necessary

Threat assessment guidelines from the NTAC note that "prevention efforts are more effective when community partners collaborate to include law enforcement, behavioral and mental health services, social services, local citizens and others."[229] Organizational culture may impact information sharing between the medical community and law enforcement. The law enforcement community may have biases about the mental health community, and vice versa, that prevent them from sharing information and working together. Ethics guidelines for various medical specialties include privacy and confidentiality considerations.[230] Those in the medical community may be concerned about violating the doctor–patient relationship if they share information about an individual's medical condition or medical records with law enforcement.[231]

(4) Recommendation #4: Enhance Collaboration between Law Enforcement and the Medical Community through Joint Training or Exercises

Opportunities for the two disciplines to work together will bring greater familiarity and could help establish communications and trust, and provide each group with a better understanding of the other's needs. Research shows that the health community recognizes the increasing role it plays in dealing with potentially dangerous patients, and law enforcement recognizes the need to have access to the subject-matter expertise of the medical community. Bringing the two groups together through exercises or joint training will help them foster relationships and interact with one another outside of times of crisis. A study titled "Disaster Exercise Outcomes for Professional Emergency Personnel and

---

[229] Keeney and Alathari, "Preventing Violent Attacks," 53.

[230] Moskop et al., "From Hippocrates to HIPAA," 53.; Henderson, "Potentially Dangerous Patients,"193.

[231] Unger, "Minding Your Meds," 5.

Citizen Volunteers" found that after participation in an exercise, participants' "confidence in collective teamwork … nearly doubled."[232]

Opponents of joint exercises or training may cite cost and time considerations. However, there may be a government agency in a given state, such as an emergency management agency, that is already tasked with creating and conducting exercises. Grant funding also can sometimes be used to fund exercises.

B. AREAS FOR FURTHER RESEARCH

This thesis reaffirms the suspicion that privacy laws are deficient and it identifies gaps and limitations that inhibit information sharing between the medical community and law enforcement to identify people who are a threat to the community. While the notion of intelligence-led policing has been in vogue for some time, including the medical community as a source of intelligence is a newer idea. Once the legal hurdles are eliminated, research could focus on how best to integrate medical intelligence into law enforcement practices while recognizing individuals' rights to privacy. There is minimal research on culture or professional biases in either community that prevent information sharing. While this thesis introduced the concept of threat assessment only in so far as to reveal the need for inclusion of both law enforcement and medical professionals, further research could be conducted on threat assessment methodologies to determine which one(s) are most effective.

C. SUMMARY

It has been known for quite some time that privacy laws create barriers to sharing medical information that could potentially prevent an attack with law enforcement. Legal hurdles still remain in place, even after these barriers have been recognized both in official after-action documents and in the news media. Maintaining the status quo is not the best option for the safety of U.S. citizens. After conducting a comprehensive review of literature

---

[232] Ronald W. Perry, "Disaster Exercise Outcomes for Professional Emergency Personnel and Citizen Volunteers," *Journal of Contingencies and Crisis Management* 12, no. 2 (June 2004): 74, https://doi.org/10.1111/j.0966-0879.2004.00436.x.

and laws, the next step is a legal analysis to determine the changes necessary to the current laws or to enact new laws that will address the deficiencies.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

American Academy of Pediatrics. “Policy Statement—Child Abuse, Confidentiality, and the Health Insurance Portability and Accountability Act.” *Pediatrics* 125, no. 1 (January 2015): 197–201. http://pediatrics.aappublications.org/content/125/1/197.full-text.pdf.

American Hospital Association. “Guidelines for Releasing Patient Information to Law Enforcement.” Accessed June 24, 2018. https://www.aha.org/system/files/2018-03/guidelinesreleasinginfo.pdf.

American Medical Association. “AMA Principles of Medical Ethics.” Accessed July 17, 2018. https://www.ama-assn.org/delivering-care/ama-principles-medical-ethics.

———. “HIPAA Violations & Enforcement.” Accessed July 28, 2018. https://www.ama-assn.org/practice-management/hipaa-violations-enforcement.

American Society of Interventional Pain Physicians. “National All Schedules Prescription Electronic Reporting Act.” Accessed June 24, 2018. http://nasper.org/.

Atwell, Barbara. “Rethinking the Childhood-Adult Divide: Meeting the Mental Health Needs of Emerging Adults.” *Albany Law Journal of Science and Technology* 25, no. 1 (2015): 1-35

Bardach, Eugene, and Eric M. Patashnik. *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving*, 5th ed. Los Angeles: SAGE/CQ Press, 2016.

Bradford, Ben. "Policing and Social Identity: Procedural Justice, Inclusion and Cooperation Between Police and Public." *Policing and Society* 24, no. 1 (2014): 22-43. https://doi.org/10.1080/10439463.2012.724068.

Brannan, David, Kristin Darken, and Anders Strindberg. *A Practitioner’s Way Forward*. Salinas, CA: Agile Press, 2014.

Brown, Bill. “Isla Vista Mass Murder: May 23, 2014.” Investigative summary, Santa Barbara County Sheriff’s Office, 2015. https://assets.documentcloud.org/documents/1671822/isla-vista-investigative-summary.pdf.

Brusca, Richard, and Colin Ram. “A Failure to Communicate: Did Privacy Laws Contribute to the Virginia Tech Tragedy?” *Washington and Lee Journal of Civil Rights and Social Justice* 17, no. 141 (Fall 2010): 1-33.

Buchan, Nancy R., Marilynn B. Brewer, Gianluca Grimalda, Rick K. Wilson, Enrique Fatas, and Margaret Foddy. "Global Social Identity and Global Cooperation." *Psychological Science* 22, no. 6 (June 2011): 821-828. http://www.jstor.org/stable/25835457.

California Department of Health Care Services. "Health Insurance Portability and Accountability Act." Accessed July 17, 2018. http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx.

Centers for Disease Control and Prevention. "What States Need to Know about PDMPs." October 3, 2017. https://www.cdc.gov/drugoverdose/pdmp/states.html.

Chuck, Elizabeth, Alex Johnson, and Corky Siemaszko. "17 Killed in Mass Shooting at High School in Parkland, Florida." NBC News, February 15, 2018. https://www.nbcnews.com/news/us-news/police-respond-shooting-parkland-florida-high-school-n848101.

CNN. "Colorado Theater Shooting Fast Facts." Last updated July 16, 2018. https://www.cnn.com/2013/07/19/us/colorado-theater-shooting-fast-facts/index.html.

Coffman, Keith. "James Holmes Told Therapist Lynne Fenton That He Fantasized about Killing 'A Lot of People' Six Weeks before Shooting." *Huffington Post*, last updated February 5, 2013. https://www.huffingtonpost.com/2012/12/06/therapist-declined-tempor_n_2248980.html.

Cohen, John D. "The Next Generation of Government CVE Strategies at Home: Expanding Opportunities for Intervention." *The Annals of the American Academy of Political and Social Science* 668, no.1 (November 1, 2016): 118-128. https://doi.org/10.1177/0002716216669933.

Corrigan, Patrick W., Benjamin G. Druss, and Deborah A. Perlick. "The Impact of Mental Illness Stigma on Seeking and Participating in Mental Health Care." *Psychological Science in the Public Interest* 15, no.2 (2014): 37-70. https://doi.org/10.1177/1529100614531398.

d'Aspremont, Jean. "Legitimacy of Governments in the Age of Democracy." *New York University Journal of International Law and Politics* 38 (2005): 877-917.

Davis, Gordon K. "Connecting the Dots: Lessons from the Virginia Tech Shootings." *Change* 40, no. 1 (January–February 2008): 8-15.

Deephouse, David L., and Mark Suchman. "Legitimacy in Organizational Institutionalism." In *The SAGE Handbook of Organizational Institutionalism*, edited by Royston Greenwood, Christine Oliver, Roy Suddaby, and Kerstin Sahlin. Thousand Oaks, CA: SAGE, 2008. http://dx.doi.org/10.4135/9781849200387.n2.

Department of Homeland Security. “Fusion Center Locations and Contact Information.” April 26, 2018. https://www.dhs.gov/fusion-center-locations-and-contact-information.

———. “National Network of Fusion Centers Fact Sheet.” June 21, 2017. https://www.dhs.gov/national-network-fusion-centers-fact-sheet.

———. “State and Major Urban Are Fusion Centers—Unique Role.” June 26, 2017. https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

Department of Homeland Security Office of Health Affairs. “Health Security Intelligence Enterprise.” PowerPoint presentation, Department of Homeland Security, 2012.

Ewing, Charles Patrick. “Tarasoff Reconsidered.” *Monitor on Psychology* 36, no. 7 (July/August 2005): 112. http://www.apa.org/monitor/julaug05/jn.aspx.

Federal Bureau of Investigation. “eGuardian.” Accessed July 11, 2018. https://www.fbi.gov/resources/law-enforcement/eguardian.

Henderson, Elizabeth. “Potentially Dangerous Patients: A Review of the Duty to Warn.” *Journal of Emergency Nursing* 41, no. 3 (May 2015): 193-200. http://dx.doi.org/10.1016/j.jen.2014.08.012.

Henry, David. *Improving Preparedness through Sharing Public Health and Homeland Security Information*. Washington, DC: National Governors Association, 2012. https://www.nga.org/files/live/sites/.../1212ImprovingPreparedness_IssueBrief.pdf.

Hogg, Michael A., Deborah J. Terry, and Katherine M. White. “A Tale of Two Theories: A Critical Comparison of Identity Theory with Social Identity Theory.” *Social Psychology Quarterly* 58, no. 4 (December 1995): 255-269. http://libproxy.nps.edu/login?url=https://search.proquest.com/docview/212697365?accountid=12702.

Houry, Debra, Carolyn J. Sachs, Kim M. Feldhaus, and Judith Linden. “Violence-Inflicted Injuries: Reporting Laws in the Fifty States.” *Annals of Emergency Medicine* 39, no. 1 (2002): 56–60. https://doi.org/10.1067/mem.2002.117759.

Huq, Aziz Z., Tom R. Tyler, and Stephen J. Schulhofer. "Why Does the Public Cooperate with Law Enforcement? The Influence of the Purposes and Targets of Policing." *Psychology, Public Policy, and Law* 17, no. 3 (2011): 419-450. http://dx.doi.org/10.1037/a0023367.

International Association of Chiefs of Police. “Events.” Accessed August 9, 2018. https://plan.core-apps.com/iacp2018/events?trackIds=2f717394f6594a422becdcebe6e05d82.

———. “Registration Information.” Accessed August 9, 2018. https://www.theiacpconference.org/event-overview/registration-category-and-fees/#site-navigation.

“Justice and Health Connect. Basics of 42 CFR, Part 2.” Accessed July 17, 2018. http://www.jhconnect.org/wp-content/uploads/2013/09/42-CFR-Part-2-final.pdf.

Keeney, Michelle, and Lina Alathari. “Preventing Violent Attacks on Government Facilities and Personnel.” *Sheriff & Deputy* (July/August 2016): 52–55. https://www.secretservice.gov/data/protection/ntac/Preventing-Violent-Attacks-on-Government.pdf.

LaFree, Gary, and Amy Adamczyk. "The Impact of the Boston Marathon Bombings on Public Willingness to Cooperate with Police." *Justice Quarterly* 34, no. 3 (2017): 459-490. https://doi.org/10.1080/07418825.2016.1181780.

La Ganga, Maria L. “James Holmes Disclosed Homicidal Thoughts but Not a Plan, Psychiatrist Says.” *Los Angeles Times*, June 16, 2015. http://www.latimes.com/nation/la-na-james-holmes-fenton-20150616-story.html.

Liu, Edwin, Erin Bagalman, Vivian Chu, and C. Stephen Redhead. *Submission of Mental Health Records to NICS and the HIPAA Privacy Rule*. CRS Report No. R43040. Washington, DC: Congressional Research Service, 2013. https://fas.org/sgp/crs/misc/R43040.pdf.

Loewy, Erich H. “Oaths for Physicians—Necessary Protection or Elaborate Hoax.” *Medscape General Medicine* 9, no. 1 (January 2007). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1925028/?report=printable.

Massachusetts Department of Public Health. *Weapon-Related Injuries to Massachusetts Residents 1994–2007: Findings from the Weapon Injury Surveillance System (WRISS.* (Boston: Massachusetts Department of Public Health, 2009. http://archives.lib.state.ma.us/bitstream/handle/2452/50056/ocn477247709.pdf?sequence=1.

Mass.gov. “About the Weapon Related Injury Surveillance System (WRISS).” Accessed July 7, 2018. https://www.mass.gov/service-details/learn-more-about-wriss.

Meloy, J. Reid, and Mary Ellen O’Toole. “The Concept of Leakage in Threat Assessment.” *Behavioral Sciences and the Law* 29, (June 2011): 513-527. https://onlinelibrary.wiley.com/doi/abs/10.1002/bsl.986.

Miller, Carol Marbin, and Kyra Gurney. “Shooter Revealed Gory Fantasies to His Therapists Years before the Parkland Massacre.” *Miami Herald*, March 10, 2018. https://www.miamiherald.com/news/local/crime/article204450699.html.

Moskop, John C., Catherine A. Marco, Gregory Luke Larkin, Joel M. Geiderman, and Arthur R. Derse. "From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine – Part I: Conceptual, Moral and Legal Foundations." *Annals of Emergency Medicine* 45, no.1 (January 2005): 53-59. https://doi.org/10.1016/j.annemergmed.2004.08.008

Muhlhausen, David B. "Director's Corner: Proactive Policing—What We Know and What We Don't Know, Yet." National Institute of Justice, January 17, 2018. https://nij.gov/about/director/Pages/muhlhausen-proactive-policing.aspx.

Munetz, Mark K. and Jennifer L.S. Teller. "The Challenges of Cross-Disciplinary Collaborations: Bridging the Mental Health and Criminal Justice Systems." *Capital University Law Review* 32, no. 4 (June 22, 2004). 935–950.

Murgado, Amaury. "How to Respond to an Emotionally Disturbed Person." *Police Magazine*, May 12, 2017. http://www.policemag.com/channel/patrol/articles/2017/05/how-to-respond-to-an-emotionally-disturbed-person.aspx.

The National Alliance for Model State Drug Laws. *Interstate Sharing of Prescription Monitoring Database Information*. Manchester, IA: National Alliance for Model State Drug Laws, 2016. http://www.namsdl.org/library/8C2F8F5B-F426-FC5F-226056040DF15FD6/.

National Conference of State Legislatures. "Mental Health Professionals' Duty to Warn." July 6, 2018. http://www.ncsl.org/research/health/mental-health-professionals-duty-to-warn.aspx.

National Threat Assessment Center (NTAC). *Attacks on Federal Government: 2001–2013*. Washington, DC: Department of Homeland Security, December 2015. https://www.secretservice.gov/data/protection/ntac/Attacks_on_Federal_Government_2001-2013.pdf.

———. *Mass Attacks in Public Spaces—2017*. Washington, DC: Department of Homeland Security, March 2018. https://www.secretservice.gov/forms/USSS_NTAC-Mass_Attacks_in_Public_Spaces-2017.pdf.

Nationwide SAR Initiative (NSI). "About the NSI." Accessed July 11, 2018. https://nsi.ncirc.gov/about_nsi.aspx.

———. "Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5." Nationwide SAR Initiative, accessed July 11, 2018. https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf.

———. "Online SAR Training for Law Enforcement and Hometown Security Partners." Accessed July 11, 2018. https://nsi.ncirc.gov/training_online.aspx.

Nix, Justin. “Do the Police Believe That Legitimacy Promotes Cooperation from the Public?” *Crime & Delinquency* 63, no. 8 (July 2017): 951-975. https://doi.org/10.1177/0011128715597696.

O'Keefe, Garrett J. "Taking a Bite out of Crime”: The Impact of a Public Information Campaign." *Communication Research* 12, no. 2 (1985): 147-178. https://doi.org/10.1177/009365085012002001.

Pagliery, Jose, and Curt Devine. “School Shooter Showed Violence and Mental Instability at Home, Police Reports Reveal.” CNN, February 17, 2018. https://www.cnn.com/2018/02/16/us/florida-shooter-cruz-records-police-calls-to-home-invs/index.html.

Perry, Ronald W. “Disaster Exercise Outcomes for Professional Emergency Personnel and Citizen Volunteers.” *Journal of Contingencies and Crisis Management* 12, no. 2 (June 2004): 64–75. https://doi.org/10.1111/j.0966-0879.2004.00436.x.

Petrila, John. “Dispelling the Myths about Information Sharing Between the Mental Health and Criminal Justice Systems.,” The CMHS National GAINS Center for Systemic Change for Justice-Involved People with Mental Illness, February 2007. http://www.pacenterofexcellence.pitt.edu/documents/Dispelling_Myths-5.pdf.

Petrila, John, and Hallie Fader-Towe. *Information Sharing in Criminal Justice–Mental Health Collaborations: Working with HIPAA and Other Privacy Laws*. New York: The Council of State Governments Justice Center, 2010. https://www.bja.gov/Publications/CSG_CJMH_Info_Sharing.pdf.

Program Manager, Information Sharing Environment (PM-ISE). *Nationwide Suspicious Activity Reporting Initiative Status Report*. Washington, DC: Office of the Director of National Intelligence, 2010. https://www.dni.gov/files/ISE/documents/DocumentLibrary/SAR/NSI_Status_Report_FINAL_2010-02-03.pdf.

Schumaker, Erin. “Doctors Often Know Who Might Commit Gun Violence. But They Can’t Do Much about It.” *Huffington Post*, March 1, 2018. https://www.huffingtonpost.com/entry/doctors-gun-violence-hipaa_us_5a95a39be4b0bef79e3086ab.

Segarra, Lisa Marie, Katie Reilly, Eli Meixler, and Jennifer Calfas. “Sheriff’s Office Had Received about 20 Calls Regarding Suspect: The Latest on the Florida School Shooting.” *Time*, February 18, 2018. http://www.time.com/5158678/what-to-know-about-the-active-shooter-situation-at-florida-high-school/.

Seitz, Esther. “Privacy (or Piracy) or Medical Records: HIPAA and Its Enforcement.” *Journal of the National Medical Association* 102, no. 8 (August 2010): 745-748. https://doi.org/10.1016/S0027-9684(15)30651-9.

Small, Mario Luis. “Weak Ties and the Core Discussion Network: Why People Regularly Discuss Important Matters with Unimportant Alters.” *Social Networks* 35 (2013): 470-483. http://scholar.harvard.edu/files/mariosmall/files/small_2013.pdf.

Stillman, Peter G. “The Concept of Legitimacy.” *Polity* 7, no. 1 (Autumn 1974): 32-56. http://www.jstor.org/stable/3234268.

Sunshine, Jason, and Tom R. Tyler. “The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing.” *Law & Society Review* 37, no. 3 (2003): 513-548. https://doi.org/10.1111/1540-5893.3703002.

Swanson, Jeffrey W., E. Elizabeth McGinty, Seena Fazel, and Vickie M. Mays. “Mental Illness and Reduction of Gun Violence and Suicide: Bringing Epidemiologic Research to Policy.” *Annals of Epidemiology* 25 (2015): 366-376. http://dx.doi.org/10.1016/j.annepidem.2014.03.004.

Tsushima, Masahiro, and Koichi Hamai. “Public Cooperation with the Police in Japan.” *Journal of Contemporary Criminal Justice* 31, no. 2 (May 2015): 212-228. https://doi.org/10.1177/1043986214568836.

Tyler, Tom R. "Enhancing Police Legitimacy." *The Annals of the American Academy of Political and Social Science* 593, no. 1 (2004): 84-99. https://doi.org/10.1177/0002716203262627.

Tyler, Tom R., and Jeffrey Fagan. "Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in their Communities." *Ohio State Journal of Criminal Law* 6 (2008): 231-275. http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4027&context=fss_papers.

Unger, Devon T. “Minding Your Meds: Balancing the Needs for Patient Privacy and Law Enforcement in Prescription Drug Monitoring Programs.” *West Virginia Law Review 117*, no. 345 (Fall,2014): 1-47.

U.S. Department of Health and Human Services. “Enforcement Highlights.” Accessed July 28, 2018. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

———. “Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement.” Accessed October 28, 2017. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf.

———. “Summary of the HIPAA Privacy Rule.”Accessed July 17, 2018. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

———. “What is PHI?” February 26, 2013. https://www.hhs.gov/answers/hipaa/what-is-phi/index.html.

U.S. Department of Health and Human Services and U.S. Department of Education. "The Child Abuse Prevention and Treatment Act Including the Justice for Victims of Trafficking Act of 2015 and the Comprehensive Addiction and Recovery Act of 2016." Accessed July 3, 2018. https://www.acf.hhs.gov/sites/default/files/cb/capta2016.pdf.

———. "Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records." U.S. Department of Education, November 2008. https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf.

———. "When Does the Privacy Rule Allow Covered Entities to Disclose Protected Health Information to Law Enforcement Officials?" July 23, 2004. https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.

U.S. Department of Justice. "Fusion Center Guidelines—Developing and Sharing Information and Intelligence in a New Era." Report, U.S. Department of Justice. https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

———. *Health Security: Public Health and Medical Integration for Fusion Centers*. Washington, DC: U.S. Department of Justice, 2011. https://it.ojp.gov/GIST/159/Health-Security--Public-Health-and-Medical-Integration-for-Fusion-Centers.

Victim Rights Law Center. "Mandatory Reporting of Non-accidental Injuries: A State-by-State Guide." 2014. https://www.victimrights.org/sites/default/files/Mandatory%20Reporting%20of%20Non-Accidental%20Injury%20Statutes%20by%20State.pdf (no page number included in forward).

Wolfe, Debra Schilling. "Revisiting Child Abuse Reporting Laws." *Social Work Today* 12, no. 2 (March/April 2012): 14. http://www.socialworktoday.com/archive/031912p14.shtml.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California