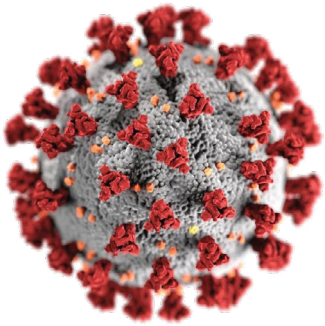

Homeland Security Affairs Journal
SPECIAL COVID-19 ISSUE

COVID-19: Public Health, Privacy, and Law Enforcement a Precarious Balancing Act

By Christopher Whiting

Abstract

In the wake of the COVID-19 pandemic, the health community faces the delicate balancing act of preserving public health by containing the outbreak, while at the same time insuring that individual health information remains protected. Playing critical roles in both areas during the COVID-19 outbreak are communicable disease reporting systems. Unfortunately, barriers to and delays in sharing health data often compromise the effectiveness of disease mitigation programs. Data must be relevant, accurate, and timely, and communicable disease reporting systems are only as precise and useful as the data that is entered. This essay examines both the successes and the failures of protected health information (PHI) data sharing, reviews the laws and rules governing PHI data sharing for first responders, determines whether the need exists for real-time sharing of PHI, and offers recommendations for future implementation. In addition, it demonstrates that the health information currently available to the first responder community has led to a sense of security and confidence that is undeserved, in part because there is an absence of timely and accurate reporting of such information. Policy and legislation updates must address the needs of both government and the private sector for accurate, timely information reporting by the state's communicable disease reporting system. Health testing capabilities should be expanded and should produce accurate, timely results to accommodate the surge in testing that is necessary to identify the population's infected members.

Suggested Citation

Whiting, Christopher. "COVID-19: Public Health, Privacy, and Law Enforcement a Precarious Balancing Act." *Homeland Security Affairs* 16, Article 9 (December, 2020) www.hsaj.org/articles16402.

Introduction

At the end of 2019, a Severe Acute Respiratory Syndrome (SARS) Novel Coronavirus 2 (CoV), SARS-CoV-2, was identified as the cause of an outbreak in Wuhan, China.[1] The disease, later named Coronavirus Disease 2019 or COVID-19, caused a global pandemic that has strained the balancing of an individual's "right to privacy" and the public's "right to know" in the effort to contain the spread of the virus. COVID-19 is primarily thought to be spread by close contact with an infected person through the production of respiratory droplets, such as coughing, sneezing, or dialogue in close proximity.[2] Considering that a significant majority of infected individuals are asymptomatic, this creates further challenges in addressing ways to contain the spread of the virus.

The virus infection rate, incubation period, and methods of transmission create unique challenges to stopping the spread of COVID-19. Law enforcement personnel and the first responder community, by the nature of their jobs, have a greater probability outside the health care environment to interact with infected persons.[3] At the onset of this pandemic, guidance was released by the Centers for Disease Control and Prevention (CDC) in order to limit exposure,

including prevention measures, contact tracing, quarantine periods, and recommendations concerning information sharing for those who were infected by COVID-19.[4] The recommendations for sharing information included surveillance, investigation, and intervention.

On March 24, 2020, the U.S Department of Health & Human Services (HHS) Office for Civil Rights (OCR) issued guidance to address the emerging needs of first responders dealing with people infected with or exposed to COVID-19.[5] This guidance specified that public health agencies may disclose Protected Health Information (PHI) to first responders in order to prevent the spread of COVID-19 without violating the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. Traditionally, federal and state laws allow for the sharing of PHI with law enforcement and other first responder entities for specifically enumerated reasons or post-exposure.

Since the issuance of the above-detailed guidance by HHS OCR on March 24, 2020, many states have implemented procedures for generating lists of individually identifiable health information for confirmed COVID-19 positive persons. However, the allowable sharing of PHI data varies from state to state, depending upon the specific state's governance. For example, the State of New Jersey has authorized the generation of lists of identifiable health information of individuals who are confirmed COVID-19 positive.

This essay will examine both the successes and the failures of existing PHI data sharing, review the laws governing PHI data sharing for first responders, determine whether a need exists for real-time sharing of PHI, and make recommendations for future implementation.

Laws and Regulations Governing PHI Data

There is no specific U.S. federal law regulating the protection of PHI on a national level. Instead, there is a complex combination of federal and state laws governing the collection, use, transmission, and disclosure of PHI. In order to understand PHI, it is essential to examine its background. PHI data is a subset of Personally Identifiable Information (PII). PII is a term referring to information that is associated with or used to identify an individual. Moreover, as defined by the Department of Homeland Security Handbook for Safeguarding Sensitive PII published December 2017, "Sensitive PII" is a type of PII, which, if lost, compromised, or disclosed without authorization, may result in harm, embarrassment, inconvenience, or unfairness to an individual. For example, Sensitive PII includes a name with medical information, social security number, date of birth, citizenship, or any combination, including details concerning addresses or family members.[6]

In order to analyze the use of PHI data by law enforcement and the first responder communities, it is essential to review the progression of laws and rules associated with the use of health data. Central to this review is an examination of the restrictions and the protections of health data, both of which are covered by the Ryan White Comprehensive AIDS Resources Emergency Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[7] Together, both acts, which are codified in U.S. Code Title 42, and are also covered in Title 45 of the U.S. Code of Federal Regulations, are the principal collective focus of this analysis.

A. Ryan White Comprehensive AIDS Resources Emergency Act

In 1990, the Ryan White Comprehensive AIDS Resources Emergency Act (the Ryan White Act) was enacted by Congress.[8] The Ryan White Act provided funding, treatment resources, and awareness programs to combat the AIDS / HIV epidemic. The initial enactment provided for post-exposure notification to first responders exposed to a bloodborne or airborne transmissible disease. The Act was reauthorized in 2006 and again in 2009. During the 2006 reauthorization, post-exposure notification was removed from the law. However, it was subsequently restored to the law during the 2009 reauthorization. The reauthorization of the Ryan White Act in 2009 also included updates to add coverage of other communicable diseases, such as SARS-CoV, for which post-exposure notifications were approved.[9] Enumerated in Table 1 is the updated CDC list requiring notification involving infectious diseases:[10]

Table 1: Updated CDC list requiring notification involving infectious diseases

1990 Initial List	2009 Reauthorization New Additions
• Diphtheria	• Anthrax, cutaneous
• Hepatitis B	• Novel influenza A and other influenza strains with a pandemic severity index greater than or equal to 3
• HIV, including AIDS	• Hepatitis C
• Tuberculosis	• Measles
• Viral hemorrhagic fevers	• Mumps
• Meningococcal disease	• Pertussis
• Plague, pneumonic	• Rubella
• Plague, pneumonic	• Severe acute respiratory syndrome (SARS-CoV)
	• Smallpox
	• Vaccinia
	• Varicella disease
	• Select agents

B. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Prior to HIPAA, there were no standard security or privacy rules or other requirements for protecting PHI data. HIPAA came to fruition approximately the same time that the health care industry migrated from a paper environment to electronic systems. HIPAA applies to covered entities such as health care providers, health departments, and businesses associated with health data (e.g., labs and medical supply firms). However, law enforcement agencies that are not involved in advanced medical processes are not considered covered entities under HIPAA. Two of the more significant objectives of HIPAA are the protection of an individual's privacy and the security of health information in the digital environment. HIPAA requires the Secretary

of HHS to develop and implement both privacy and security standards. These two standards are promulgated in the Privacy Rule and the Security Rule, respectively. The rules establish replicable national standards for the protection of health information, as well as a set of national security standards for electronically transmitted or stored data. HHS OCR is responsible for enforcement of both the Privacy and Security Rules, which authorize the imposition of civil penalties against violators. Certain first responder agencies such as emergency services are considered covered entities when dealing with PHI and therefore are not exempt from unauthorized disclosures or careless actions with PHI data.

An example of the enforcement of the above rules against first responders occurred on December 30, 2019, when HHS OCR fined West Georgia Ambulance, Inc., a provider of emergency medical services in Carroll County, Georgia, the sum of $65,000 for violations of HIPAA rules and noncompliance in securing PHI data. Among the violations in question was one involving the loss of a laptop computer that contained approximately 500 records of patient data. At the time, OCR Director Roger Severino stated, "all providers, large and small, need to take their HIPAA obligations seriously."[11]

The Privacy Rule was created to balance the individual's right to privacy with the ability to share PHI in certain circumstances. As identified, the Privacy Rule created a national standard that insured an individual's health information would remain private and protected but permitted sharing such information with covered entities in order to facilitate diagnosis or treatment. Under the Privacy Rule, and prior to the guidance released from HHS OCR regarding COVID-19 on March 24, 2020, PHI data sharing with law enforcement agencies and personnel was only permitted under six conditions.[12]

The above referenced six conditions include disclosure by covered entities, as follows:

1. If requested by court orders, grand jury subpoena, or administrative request
2. To identify a suspect, fugitive, material witness, or missing person
3. In response to a law enforcement official's request for information about a victim or suspected victim of a crime
4. To alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death
5. When in good faith, it is believed that protected health information is evidence of a crime that occurred on the covered entity's premises
6. For an incident not occurring on the covered entity's premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victim(s) of such an offense, and the identity, description, and location of the perpetrator of the crime[13]

Under the HIPAA Security Rule, covered entities are able to implement systems that are tailored to their specific facilities as long as they maintain the proper protection of patient information stored or transmitted electronically. Three types of security safeguards are outlined in the Security Rule, including administrative, physical, and technical safeguards. This Security Rule requires the implementation of policies and procedures that comply with HIPAA, including protecting physical data, controlling access to the systems themselves, and providing encryption of data sent over open networks.

In 2013, the Omnibus Rule was added as an update to HIPAA regulations in order to strengthen privacy and security protections of covered entities. This amendment includes addendums whereby the covered entity's business associates and subcontractors are held to the same standards required in HIPAA, including the Privacy and Security Rules.[14]
It is essential to have a grasp of existing federal laws in order to understand the permitted uses of PHI information sharing. However, the mixture of federal and state laws complicates this legal analysis, adversely impacting the permissible sharing of PHI with law enforcement and the first responder communities. Further research is warranted in order to understand the effect of PHI related laws on information sharing.

C. Synopsis
The Ryan White Act forged the way for the sharing of PHI with the first responder community in a post-exposure incident, irrespective of medical privacy concerns. HIPAA and the Omnibus Rule expand the sharing of PHI within the medical community and its sub-partners, which require the data. Additionally, HIPAA exceeds PII security and sharing protocols in the requirements for organizations and sub-partners. Under the HIPAA Privacy Rule, both health care entities and sub-partners are subject to substantial legal liability for any breach caused by security shortfall in the storage, use, and transmission of PHI data.

Nevertheless, HIPAA is a valuable framework, which insures that sensitive information does not "fall through the cracks" and that covered entities and their sub-partners provide the highest level of care, security, and confidentiality of medical information. It is noteworthy that health information privacy in the context of the legal framework does not govern information that does not contain PII, that is patient-generated, or that is in a nonregulated entity's (e.g., Google, Apple) possession.[15]

This includes the collection of health data by smartphone apps, wearable devices, and direct-to-consumer testing companies.

COVID-19 PHI Data Sharing

The COVID-19 pandemic has led to an unprecedented challenge within the health community with respect to containing the outbreak. In order to manage the pandemic, home quarantine, implementation of social distancing strategies, prohibitions against large public gatherings, testing (fixed and mobile), and innovative approaches to contact tracing have been implemented. To further, address this challenge, the sharing of health information among medical partners, research facilities, law enforcement, and first responder communities has become a key element in identifying both symptomatic and asymptomatic infected persons in order to contain the outbreak, while at the same time protecting the public from further exposure.

COVID-19 PHI data includes specific information about an identifiable patient, test results, treatment, and the creation of COVID-19 positive patient and address lists. Additionally, the data includes released COVID-19 reports aggregating confirmed cases or deaths concerning a specific region, county, town, or state, and the personal information of a patient, such as a home address. HHS OCR provided two specific scenarios that are relevant to the many covered entities on the

front lines of the pandemic. First, a covered entity provider may disclose a list of names and addresses of those individuals who have tested positive or received treatment for COVID-19 to a dispatch center for use on a per-call basis. Second, a 911 call center that is designated as a covered entity may ask callers to answer COVID-19 screening questions and disclose the information received to law enforcement officers who are dispatched to the subject locations. In these scenarios, the ability to disclose this PHI allows the first responders and law enforcement officers to take extra precautions, such as the use of personal protective equipment (PPE).[16,17]

State, county, and local health departments are capable of tracking COVID-19 positive test results through their respective communicable disease reporting systems. An Associated Press article published on May 19, 2020, listed several states, including Colorado, Iowa, Louisiana, Nevada, New Hampshire, North Dakota, New Jersey, Ohio, and South Dakota, which provide law enforcement officials with the names and addresses of COVID-19 patients. However, Wisconsin and Tennessee terminated sharing the COVID-19 data with law enforcement after privacy concerns were raised by the public and several special interest groups.[18] The sharing of COVID-19 PHI varies across several states with regard to policy, laws, and, in some cases, involves signed memorandums of understanding.

Typically, any COVID-19 data that is provided is flagged in computer-aided dispatch (CAD) systems so that responding officers can be alerted that there may be a positive infected person at the incident address. The COVID-19 PHI is furnished so that extra precautions are taken when dealing with an incident at a specific address, and not as a pretext to refuse a call for service or to deny treatment to an infected person.

Although sharing of COVID-19 PHI is legal under federal and state laws, several questions arise from the disclosure of such data. These questions include:

- Whether the COVID-19 PHI sharing with law enforcement serves a purpose?
- Is the COVID-19 data disclosure to law enforcement accurate and timely?
- In absence of testing capabilities, many positive individuals may not be tested, and given the possibility of asymptomatic COVID-19 persons, should first responders simply utilize universal precautions on all incidents during this pandemic, rather than rely on COVID-19 lists?
- Has COVID-19 PHI data sharing led to a false sense of security in first responders due to the lack of testing, delays in COVID-19 data aggregation, and the absence of timely reporting of positive COVID-19 persons?

To further analyze these questions and the usage of PHI data for law enforcement, the procedures implemented in Bergen County, New Jersey for PHI disclosures and the policies drawn up for the use of PHI data in New Jersey next will be examined.

Bergen County COVID-19 DATA Sharing Analysis

In New Jersey, public health reporting is mandated by state law, and reportable communicable diseases are identified in the New Jersey Statutes Annotated (N.J.S.A.), Section 26, Chapter 4-1, and New Jersey Administrative Code (N.J.A.C.), Title 8, Chapter 57. It is the responsibility of health care providers to notify the local health department where an infected patient resides when the presence of a communicable disease is determined.[19] New Jersey utilizes a web-based system, the Communicable Disease Reporting and Surveillance System (CDRSS), by which public health partners statewide report and track incidents involving communicable diseases. Hospitals and labs enter patient information, such as testing, results, and treatment. Public health officials are then able to conduct follow up investigations and contact tracing for patients who have tested positively for communicable diseases, such as COVID-19.[20] Disclosures of confidential individual medical information mandated by the New Jersey Commissioner of Health are defined under New Jersey's Emergency Health Powers Act, N.J.S.A. 26:13-1.[21] Once a notification is received, and patient information is entered into CDRSS, the County Local Information Network and Communication System (LINCS) is engaged. As stated by the New Jersey Department of Health, "LINCS is a system of public health professionals and electronic public health information that enhances the identification and containment of diseases and hazardous conditions which threaten civilization."[22] For the purpose of controlling the spread of the virus to the at-risk population, the New Jersey Department of Health (NJDOH) empowers local Public Health Officers to share the names and addresses of individuals who have tested positive for COVID-19 with law enforcement agencies. This information sharing was authorized in order to enable law enforcement officers across New Jersey to protect themselves better and more effectively use their limited supplies of PPE amid the COVID-19 pandemic.[23]

In order to secure the information that is shared and protect the privacy of the individuals affected, the NJDOH and the New Jersey Attorney General's Office require Public Health Officers to follow specific steps for the disclosure of PHI. Delineated in New Jersey Attorney General Directive 2020-1 are the established procedures for obtaining COVID-19 PHI from health officials, the process for sharing such information with law enforcement and others, and the limitations on its use.[24] New Jersey Attorney General Directive 2020-1 was issued on March 19, 2020, revised on March 27, 2020, and again revised on April 11, 2020. This directive established the County Prosecutor's Office (CPO) as the primary conduit to streamline the process by which COVID-19 PHI is shared in New Jersey. Requirements of the directive are outlined as follows:

- CPOs will receive COVID-19 PHI from their County LINCS agency, including name and address information.
- The CPO will provide a list of specific names and addresses associated with an agency's jurisdiction so that the file can be maintained in a CAD system. This will be completed in accordance with the following procedure:
  - If a county-wide CAD system exists, the list will be flagged by name and address in the county system.
  - If a local agency operates its own CAD system, then the list is provided to a single point of contact who will flag the address.
    - The assigned person is not permitted to share the list with any other persons and will be responsible solely for adding the flags in the CAD.
    - The assigned person must ensure the confidentiality and security of the list.
- COVID-19 PHI will be transmitted in protected, encrypted, and/or secure emails, or, if hand-delivered, must be similarly protected.
- COVID-19 PHI will be deleted when the County LINCS officer or CPO determines an individual should be cleared or upon a declaration that the public emergency is concluded.
- A person is considered cleared when 30 days have passed from the date of their positive test and must then be removed from the CAD.
- COVID-19 information contained in the CAD system will be utilized solely for the limited purpose of protecting the health and safety of first responders.
- No law enforcement officer may use COVID-19 information as a basis for refusing any call for service.
- No law enforcement officer may require individuals to identify themselves as COVID-19 positive or to quarantine when seeking assistance from law enforcement.
- No individuals or addresses can be flagged in CAD systems unless obtained through this procedure from the County LINCS officer or CPO.[25]

The Bergen County Prosecutor's Office (BCPO) is the designated CPO for Bergen County, New Jersey, and oversees 72 law enforcement agencies with approximately 2,700 sworn law enforcement officers. Bergen County is one of New Jersey's twenty-one counties and has the largest population with approximately one million residents. The initial outbreak of COVID-19 in New Jersey occurred in Bergen County on March 4, 2020. Since the onset of the outbreak, Bergen County has led the state in confirmed positive cases, as well as deaths as a result of COVID-19.

As of June 29, 2020, Bergen County had 19,423 confirmed COVID-19 cases, whereas the state had a total of 171,272 cases. Bergen County peaked on April 10, 2020, after experiencing a 2,585-case increase, and the state peaked on April 14, 2020, with a 4,059-case increase. The following table (Figure 1) shows the progression of confirmed COVID-19 cases in Bergen County relative to the entire state:[26]

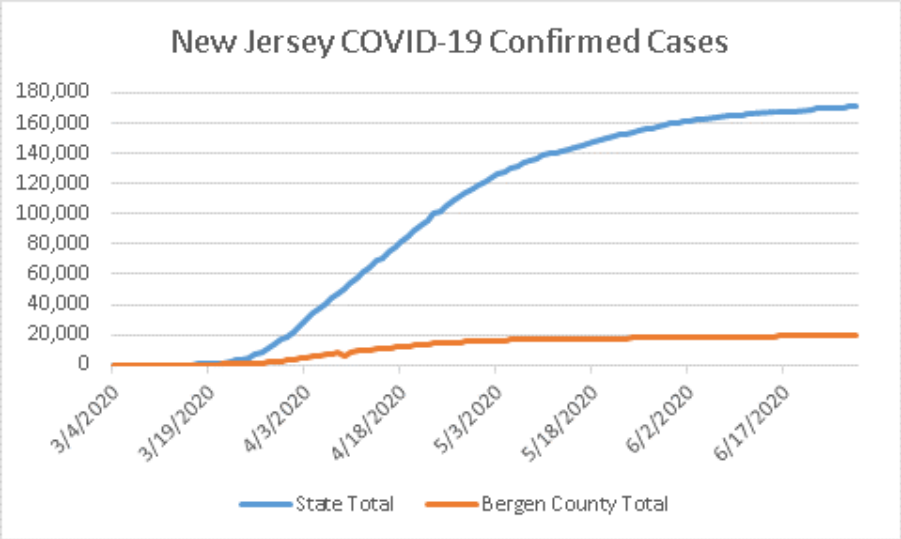

Figure 1: New Jersey COVID Cases Source: NJ Department of Health

Beginning on March 19, 2020, the BCPO started a weeklong pilot program to produce daily name and address lists of positive COVID-19 persons. After completion of the initial pilot, the plan was authorized to continue for the duration of the COVID-19 pandemic. On March 28, 2020, Bergen County Prosecutor Mark Musella issued Directive 2020-6, implementing procedures to share PHI data with law enforcement officers in Bergen County that were outlined in New Jersey Attorney General Directive 2020-1. The Prosecutor's Directive additionally specified that Bergen County law enforcement officers were not permitted to request that any person publicly identify as COVID-19 positive or quarantine when seeking police assistance, nor to provide any public notice of COVID-19 positive or quarantine status, nor record any voluntary disclosures of positive or quarantined individuals in CAD systems that were not obtained through the outlined procedure.[27]

As New Jersey is a home-rule state, only 13 of the 72 law enforcement agencies are able to access the county-wide CAD system. In order to accommodate the other 59 agencies, the BCPO created a Secure File Transfer Protocol (SFTP) server with two-factor authentication required in order to transmit PHI data to these agencies. Each agency designated a single point of contact responsible for downloading a list produced daily by the BCPO from confirmed cases of COVID-19. The list generated by the BCPO is provided through a daily report function in CDRSS. Only confirmed positive names and addresses are extracted from the system and then further broken out by jurisdiction so that such limited information may be shared among the 72 law enforcement agencies based on their geographical locations.

New Jersey reports that as of June 28, 2020, 1,403,984 of approximately 9,241,900 New Jersey residents, or roughly 15% of the state's population, have been tested. With an incubation period of up to 14 days for COVID-19 and a median time of 4-5 days from exposure to the onset of symptoms, the low percentage tested presents serious challenges to public health and first responders.[28] Furthermore, in the public disclosure by the Bergen County Executive on June 26, 2020, it was reported that of the 19,283 confirmed cases in the county, approximately 799 cases

had no address information associated with the record. During the daily reports provided to the public by the Bergen County Executive, the number of cases without an address record has varied from 600 to as high as 890.[29] The high number of unknown addresses adds to the misperception of accuracy in the lists of COVID-19 confirmed positive individuals because this number represents individuals who have tested positive but are not associated with a residence. Consequently, these individuals are not be part of any COVID-19 list provided to law enforcement.

The NJDOH and New Jersey Commissioner of Health Judith Persichilli raised additional concerns on delays in reporting of COVID-19 confirmed positive individuals. At a press conference held on March 27, 2020, Commissioner Persichilli stated that "the backlog of testing due to the overwhelming volume of requested tests is being reported as high as seven days. That's the time between having the test specimen collected and getting a result."[30] Then again, on July 13, 2020, Commissioner Persichilli further reported that, "in New Jersey testing turnaround time has been steadily increasing for three weeks due to national demand and a national supply shortage. Our average turnaround time is now more than five days when previously, it had been two to four."[31] This delay in testing directly impacts the CDRSS system and the entry of a COVID-19 confirmed positive individuals in the system. The data extracted from CDRSS and then provided to law enforcement only includes confirmed positive individuals who are placed on the list.
Part of the appendix of New Jersey Attorney General Directive 2020-1 was Exhibit B, labeled "Frequently Asked Questions" (FAQ). This document provided by the NJDOH expanded on additional possible delays for CDRSS entries. Further adding to delayed reporting, Exhibit B - FAQ outlined several reasons why individuals who test positive may not be on the lists provided to law enforcement, as noted below:[32]

- Delays in getting cases entered in CDRSS, such as faxed reports of individuals.
- Delays in getting the CDRSS case assigned to a Local Health Department (LHD) for verification. The LHD has to manually review cases before confirmation of the individual in the system.
- Delays in getting the CDRSS case assigned to the correct LHD. As an example, some individuals provided a PO Box and not a residential address during testing.
- Delays in getting the current address of an individual who did not have one listed in CDRSS.
- Inability to obtain the current address of the individual.
- The Individual's current address does not match the individual's driver's license or other documented legal address. The LHD does not have access to law enforcement systems or databases and therefore, has to rely on the individual's self-reporting or disclosure during the testing process.
- Lastly, conflicting reports about the individual from different sources which list separate addresses.

In light of the potential of individuals to be asymptomatic for up to 14 days, the delays in reporting positive patients up to seven days, compounded with LHD delays in confirming addresses, present significant challenges in publishing timely COVID-19 confirmed positive lists. Furthermore, the limited testing of individuals adversely affects the value of PHI data sharing. Timely reporting and greater testing capabilities are needed in order to reflect the threat environment for infected people accurately. Law enforcement and first responder personnel

need to rely on universal precautions when responding to such incidents, as data may not be accurately reflected in COVID-19 lists or the persons involved may not have been tested. Additionally, while the assignment of a single point of contact at a law enforcement agency was implemented in order to secure the PHI data, there exists a potential that data entry into CAD systems can further be delayed depending on work schedules or remote computer access.

Bergen County Directives and Quarantined Officer Statistics

To further examine the benefit of sharing PHI data with law enforcement officers, it is similarly important to review the policies and procedures implemented to prevent further spread of COVID-19 in the law enforcement community. The Bergen County Prosecutor, under the authority established in N.J.S.A. 2A:158-5, issued several directives to all law enforcement agencies in Bergen County for the response to, and preparation for the COVID-19 pandemic. To limit the exposure of law enforcement officers in the county and to further the implementation of PHI sharing as outlined in New Jersey Attorney General Directive 2020-1, the Bergen County Prosecutor issued the following directives:[33]

- Bergen County Prosecutor's Directive 2020-2 requiring law enforcement agencies must take all reasonable precautions to prevent the contracting and spread of COVID-19 virus, issued on March 16, 2020.[34]
- Bergen County Prosecutor's Directive 2020-3 providing additional direction for procedures that law enforcement agencies may take to minimize the spread of the COVID-19 virus to staff and public, issued on March 18, 2020.[35]
- Bergen County Prosecutor's Directive 2020-5 requiring all law enforcement employment for private entities must generally cease during the present state of emergency. Furthermore, every Bergen County law enforcement executive must implement a written plan to allocate law enforcement and civilian personnel to ensure minimal contact among staff, issued on March 23, 2020.[36]

The directives mentioned above were issued in order to prevent the spread of COVID-19 and conserve workforce resources should an outbreak occur in a law enforcement agency within the county. The directives issued to law enforcement agencies in Bergen County mandated the following:

- Agency personnel may not visit the department while off duty without permission.
- Agency personnel who can practically work remotely are permitted to do so.
- The Agency administration shall implement scheduling that facilitates no contact or overlapping shifts.
- Agency personnel who are ordered to quarantine, test positive or report sick shall remain home.
- Agency personnel should, at a minimum, disinfect workstation equipment and vehicle interiors at the start of the shift.
- Agency administration is to cancel off duty job assignments or extra duties that are not emergencies.

During the COVID-19 pandemic, New Jersey implemented daily press conferences to provide updates to residents on the prevention and response measures. These regular conferences included New Jersey Governor Phil Murphy, Health Commissioner Judith Persichilli, New Jersey State Police Superintendent Colonel Patrick Callahan, and various other government officials as needed. For this analysis, we reviewed three of the daily press conferences in which Colonel Callahan provided disclosures of law enforcement officers statewide who tested positive for COVID-19 or were ordered to self-quarantine due to symptoms or exposure. Table 2 illustrates the number of such reported officers on March 31, 2020, April 7, 2020, and April 13, 2020, and provides a comparison with Bergen County's reporting during the same time period.

Table 2: Officers Statewide vs Bergen County

	New Jersey (Statewide) Law Enforcement Officers			Bergen County Law Enforcement Officers		
	Tested Positive	Quarantined	Total	Tested Positive	Quarantined	Total
March 31, 2020[37]	383	3,081	3,464	34	130	164
April 7, 2020[38]	562	2,941	3,503	73	125	198
April 13, 2020[39]	645	2,310	2,955	84	111	195

As reported by Colonel Callahan, New Jersey has approximately 36,000 law enforcement officers statewide, based on the Federal Bureau of Investigation's Uniformed Crime Reporting numbers.[40] Of this number, Bergen County represents approximately 2,700 law enforcement officers in the state. Utilizing the data contained in Table 2, the New Jersey statewide percentage of law enforcement officers testing positive or quarantined was greater than that in Bergen County. The data indicates that statewide the total percentage of officers who tested positive or were quarantined was 9.63% on March 31, 2020, 9.73% on April 7, 2020, and 8.2% on April 13, 2020. During this same time period, the data indicates that in Bergen County, the total percentage of officers who test positive or were quarantined was 6.07% on March 31, 2020, 7.33% on April 7, 2020, and 7.22% on April 13, 2020. It is important to understand the limitations in the data, that is, utilizing an approximate number of officers statewide and, in addition, agencies underreporting officers who tested positive or were quarantined.

As previously noted, Bergen County has had the highest amount of confirmed cases in the state since the onset of the COVID-19 pandemic, yet compared to statewide numbers, a lesser percentage of positive or quarantined officers. While there is no conclusive proof, the data presented does suggest that procedures implemented for law enforcement agencies in Bergen County assisted in reducing the exposure of officers. This is in addition to CDC guidance for social distancing, face coverings, disinfecting and monitoring personal health.

Recommendations

As delineated in this research, several recommendations are identified for future pandemic planning, mitigation, and remediation regarding PHI data sharing to protect law enforcement and first responder communities. Fundamental to the value of PHI Data sharing with law

enforcement is that the data must be relevant, accurate, and timely. Policy and legislation updates should address the need of both government and private sectors for accurate, timely reporting in the state's communicable disease reporting system. Additionally, testing capabilities must be expanded to accommodate the surge of testing required to identify infected members of the population accurately.

The myriad of federal and state laws covering HIPAA and PHI data present challenges in our existing legal framework. Agencies must be educated in their roles and responsibilities when it comes to receiving, disclosing, and storing PHI data. The expansion of training in the area of PHI, PII, and data security must be implemented in the law enforcement community. As noted in Bergen County's example, proactive directives to address officer safety must be implemented globally without regard for traditional shift structure and operation arrangements. Planning and implementation of officer safety policies will help prevent further diminished workforce potentials. If training and security protocols are appropriately implemented, the reporting system does not have to rely on a single point of contact, and improved timely reporting will occur. Lastly, regardless of data sharing and identification of COVID-19 confirmed positive individuals, universal safety protections must be implemented, and PPE utilized when appropriate.

Conclusion

In a public health emergency, law enforcement and the first responder community require additional safeguards so that they can continue to do their jobs safely, effectively and efficiently. As a result of a public health emergency, expanded duties may develop to mitigate the public health crisis. The COVID-19 pandemic presented this challenge and produced unprecedented responsibilities for law enforcement. Balancing law enforcement resources with new responsibilities and everyday service demands is a formidable distinctive challenge. Resources can quickly become overwhelmed or absorbed. Still, it is essential to protect law enforcement personnel; otherwise, the health risks of continuing to report to work will become too great for both them and their families.

Achieving a balance between the need to protect individual health information and the need to protect public health is the paramount challenge. Agencies must work together in order to achieve the common goals of health and safety. Communicable disease reporting systems play a critical role during widespread outbreaks. Impediments to, and delays in data sharing may compromise the effectiveness of mitigation programs. Without accurate and timely data sharing, the potential exists to create a false sense of security. Crucial to the mitigation process is efficiently collaborating cross-sector in order to develop and share knowledge, and thereby prevent any worsening of the public health crisis. The ability of law enforcement to respond effectively to any emergency, whether it is a public health crisis or otherwise, depends principally upon its preparedness. The creation of a unified framework for sharing data is useful as an essential step in addressing the effective response to the challenges we currently face.

About the Author

Christopher Whiting is currently pursuing a master's degree at the Naval Postgraduate School (Cohort 2001/2002) while continuing his role as a Detective Sergeant with the Bergen County Prosecutor's Office (New Jersey) Intelligence & Counterterrorism Unit. He serves as Bergen County's Counterterrorism Coordinator (CTC) and Chair of the New Jersey Urban Area Security Initiative (UASI) Law Enforcement Subcommittee. For the duration of the COVID-19 pandemic, Sgt. Whiting's assignment is with the Bergen County Health Department to assist in data analysis and facilitate the sharing of COVID-19 positive patient info with Bergen County law enforcement agencies. He holds a MS from Farleigh Dickinson University in Homeland Security and a BS from Manhattan College in Computer Engineering. He may be reached at Christopher.Whiting@NPS.edu

Notes

1. "WHO | Novel Coronavirus – China," WHO (World Health Organization), accessed May 25, 2020, http://www.who.int/csrdon/12-january-2020-novel-coronavirus-china/en/.

2. CDC, "Coronavirus Disease 2019 (COVID-19) - Transmission," Centers for Disease Control and Prevention, June 1, 2020, https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/how-covid-spreads.html.

3. "The Role of Law Enforcement in Public Health Emergencies," n.d., 39.

4. CDC, "CDC Strategies to Reduce COVID-19 Spread," Centers for Disease Control and Prevention, February 11, 2020, https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/strategies-to-reduce-spread.html.

5. "OCR Issues Guidance to Help Ensure First Responders and Others Receive Protected Health Information about Individuals Exposed to COVID-19 | HHS.Gov," accessed May 18, 2020, https://www.hhs.gov/about/news/2020/03/24/ocr-issues-guidance-to-help-ensure-first-responders-and-others-receive-protected-health-information-about-individuals-exposed-to-covid-19.html.

6. "DHS Handbook for Safeguarding Sensitive PII," December 4, 2017.

7. "Public Law 101-381"; "Public Law 104-191."

8. "Public Law 112-168."

9. "Public Law 111-87."

10. "CDC - NIOSH Update - Revised, Updated Resources Are Announced To Help Prevent Exposures Of Emergency Response Employees To Infectious Diseases During Duty," February 28, 2019, https://www.cdc.gov/niosh/updates/upd-11-02-11.html.

11. News Division, "Ambulance Company Pays $65,000 to Settle Allegations of Longstanding HIPAA Noncompliance," Text, HHS.gov, December 30, 2019, https://www.hhs.gov/about/news/2019/12/30/ambulance-company-pays-65000-settle-allegations-longstanding-hipaa-noncompliance.html.

12. "45 C.F.R. § 164.512(f)".

13. Office for Civil Rights (OCR), "Summary of the HIPAA Security Rule," Text, HHS.gov, November 20, 2009, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

14. "HIPAA Omnibus Regulations," accessed July 14, 2020, http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php.

15. Jane Hyatt Thorpe and Elizabeth Alexandra Gray, "Big Data and Public Health: Navigating Privacy Laws to Maximize Potential," *Public Health Reports (Washington, D.C. : 1974)* 130, no. 2 (2015): 171–75, https://doi.org/10.1177/003335491513000211.

16. "OCR Issues Guidance to Help Ensure First Responders and Others Receive Protected Health Information about Individuals Exposed to COVID-19 | HHS.Gov."

17. "45 C.F.R. § 164.512(b)(1)(Iv)."

18. "COVID-19 Data Sharing with Law Enforcement Sparks Concern," AP NEWS, May 19, 2020, https://apnews.com/ab4cbfb5575671c5630c2442bc3ca75e.

19. "N.J.S.A. § 26:4-1"; "N.J.A.C. § 8:57-1, et seq."

20. "Department of Health | Communicable Disease Service | Communicable Disease Reporting and Surveillance System," accessed June 9, 2020, https://www.state.nj.us/health/cd/reporting/cdrss/.

21. "N.J.S.A. § 26:13-1, et Seq." (n.d.).

22. "New Jersey Department of Health | Local Public Health | LINCS," accessed June 28, 2020, https://www.nj.gov/health/lh/professionals/.

23. Shereen Semple, "New Jersey Department of Health Memorandum Titled Limited COVID-19 Information Sharing," March 18, 2020.

24. Honorable Gurbir Grewal, "New Jersey Attorney General Law Enforcement Directive No. 2020-1 v3.0" (2020).

25. Honorable Gurbir Grewal, "New Jersey Attorney General Law Enforcement Directive No. 2020-1 v3.0" (2020).

26. Honorable Mark Musella, "Bergen County Prosecutor," accessed July 12, 2020, https://www.bcpo.net/home/meet-the-prosecutor.

27. Honorable Mark Musella, "Bergen County Prosecutor's Directive 2020-6" (2020).

28. Lauer SA, Grantz KH, Bi Q, et al., "The Incubation Period of Coronavirus Disease 2019 (COVID-19) From Publicly Reported Confirmed Cases: Estimation and Application," *Annals of Internal Medicine*, May 5, 2020, https://www.acpjournals.org/doi/10.7326/M20-0504.; Guan WJ, Ni ZY, Hu Y, et al, "Clinical Characteristics of Coronavirus Disease 2019 in China," *New England Medical Journal* 2020, no. 382 (n.d.): 1708–20.

29. "Bergen County COVID-19 Public Reporting," Bergen County New Jersey, accessed June 30, 2020, https://www.co.bergen.nj.us/health-promotion/2019-novel-corona-virus.

30. "Office of the Governor Transcript March 27, 2020 Coronavirus Briefing to Media," accessed July 13, 2020, https://www.nj.gov/governor/news/news/562020/20200328b.shtml.

31. "Office of the Governor Transcript July 13, 2020 Coronavirus Briefing to Media," accessed July 13, 2020, https://www.nj.gov/governor/news/news/562020/20200413g.shtml.

32. Honorable Gurbir Grewal, "New Jersey Attorney General Law Enforcement Directive No. 2020-1 v3.0 Exhbiit B (DOH FAQ)" (2020).

33. "N.J.S.A. § 2A:158-5" (n.d.).

34. Honorable Mark Musella, "Bergen County Prosecutor's Directive 2020-2" (2020).

35. Honorable Mark Musella, "Bergen County Prosecutor's Directive 2020-3" (2020).

36. Honorable Mark Musella, "Bergen County Prosecutor's Directive 2020-5" (2020).

37. "Office of the Governor Transcript March 31, 2020 Coronavirus Briefing to Media," accessed July 12, 2020, https://www.nj.gov/governor/news/news/562020/20200331b.shtml.

38. "Office of the Governor Transcript April 7, 2020 Coronavirus Briefing to Media," accessed July 12, 2020, https://www.nj.gov/governor/news/news/562020/20200407f.shtml.

39. "Office of the Governor Transcript July 13, 2020 Coronavirus Briefing to Media."

40. "2016 New Jersey Uniform Crime Report," n.d.

Copyright