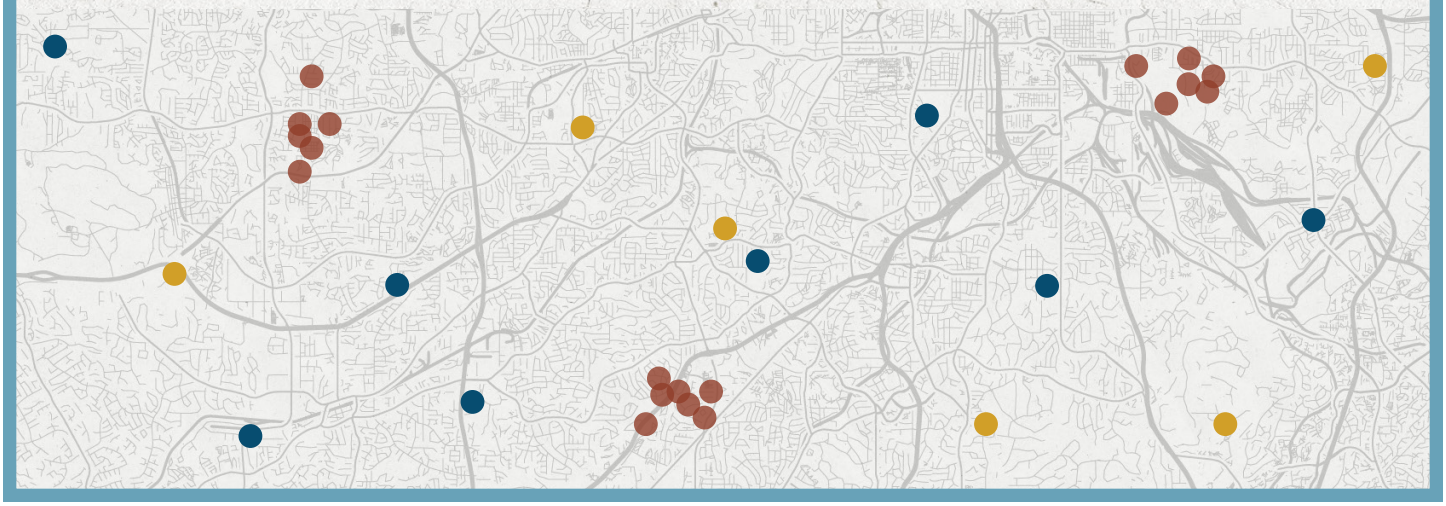
LEGAL, TECHNICAL, AND FINANCIAL CONSIDERATIONS

WHAT IS THE CARDIFF VIOLENCE PREVENTION MODEL?

More than half of violent crime (53%) in the United States (U.S.) is not reported to law enforcement according to the Department of Justice. Violence is a serious public health problem that affects people of all ages. This means that communities lack a complete understanding of where violence occurs and how to develop tailored programs for prevention.

The Cardiff Violence Prevention Model provides a way for communities to gain more information about where violence is occurring and how to prevent it by forming partnerships between hospitals, law enforcement, and others interested in violence prevention. These partnerships can help guide coordinated responses and violence prevention strategies.



Because the model requires that information about the context of violence-related injuries is shared, there are many legal, technical, and financial considerations that may be important in planning and maintaining a local community safety partnership. These considerations should be addressed before any program activities begin or early in implementation.

The Cardiff Model is intended to be implemented as a local public health program. Consequently, variation in the data elements collected and the partners involved in data sharing is likely to exist based on local prevention needs. The information below is intended to help clarify issues that are likely to arise about the HIPAA Privacy and Security Rules when the data sharing involves HIPAA "covered entities,"[1] such as hospitals or other health care providers, or their "business associates."[2]

DATA SHARING MECHANISM AND HIPAA APPLICABILITY

CARDIFF MODEL PARTNERSHIPS INVOLVING PUBLIC HEALTH AUTHORITIES

The core data elements to be collected under the Cardiff Model include: 1) location of the violent incident, 2) date/time of the violent incident, and 3) mechanism of injury. Additional data elements may also be collected and shared based on the public health needs of the local partnership. Certain data elements may be individually identifiable, and thus considered "protected health information" under HIPAA, when created, received, maintained, or transmitted by a HIPAA covered health care provider.[3] We anticipate under this model that some health care providers subject to HIPAA may be sharing these data elements with state or local health departments and agencies, which typically meet the HIPAA definition of a "public health authority."

The HIPAA Rules define "public health authority" as "[A]n agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a delegation of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate."[4]

HIPAA permits a covered entity, such as a health care provider, to disclose protected health information to a public health authority for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, for public health surveillance, investigations, and interventions for injury prevention. Authorization is not needed from the individual to whom the protected information pertains, and a covered provider is not required to establish a data sharing agreement to disclose "protected health information" to the authorized public health authority for public health purposes.[5] However, a disclosure to a public health authority must be the "minimum necessary" information to achieve the public health objective, and a covered entity may rely on the representation of the public health authority to determine what constitutes the minimum necessary.[6]

1. 45 C.F.R. § 160.102.
2. See 45 C.F.R. § 160.103. A "business associate" is a person or entity who performs functions or activities on behalf of a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. See also https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.
3. See 45 CFR § 160.103.
4. 45 CFR § 164.501
5. See 45 CFR § 512(b) and OCR's Public Health guidance, https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html.
6. See 45 CFR § 164.502(b). If the disclosure is required by law, the HIPAA covered provider may disclose the amount of information required; if the disclosure is not required by law, the amount of information disclosed must be the minimum necessary to accomplish the public health purpose. HIPAA covered entities may rely on representations from public health officials that the amount of information requested is the minimum necessary. See https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html.

Public health agencies may join with other organizations to form initiatives or coalitions to achieve violence reduction, for example, by targeting interventions and resources to specific populations or geographic areas. In fact, standards[7] for national voluntary accreditation of state, local, tribal, and territorial health departments envision health departments that lead collaborative efforts to assess and address public health issues facing the community.

In a public health initiative, a public health agency can delegate authority to multiple types of organizations to carry out its official public health mandate. When an organization is acting under such a delegation from a public health authority, a HIPAA covered provider, such as a hospital, may disclose protected health information without patient authorization to the organization in the same manner as it could disclose to a public health authority.[8]

Each local collaborative will need to determine which entities will carry out the data-handling functions and determine how HIPAA applies. For example, a hospital may collect the data and disclose it to a third party for the purpose of removing unnecessary identifiers before disclosing the information to the public health authority. In this case, the third party would be acting as a business associate for the hospital with a business associate agreement. The business associate agreement would specify the activities the third party is doing on behalf of the covered provider.[9] In another example, the covered provider may disclose the data directly to the public health authority, which may then format it and aggregate the data with other information, such as law enforcement data. A disclosure from covered provider to public health authority for public health activities would not require a business associate agreement or consent.

In a Cardiff Model public health partnership, collaborating organizations may use the data received from the public health authorities or organizations acting under a delegation of authority to create maps for the partnership or to develop local violence prevention solutions. Local public health agencies should ensure compliance with applicable local and state laws in addition to HIPAA, where applicable.

CARDIFF MODEL PARTNERSHIPS WITHOUT INVOLVEMENT OF A PUBLIC HEALTH AUTHORITY

It is possible that some communities wishing to implement the Cardiff Model may not have a public health authority able to engage in the collaboration. In these scenarios, hospitals, law enforcement agencies, and other municipal and community partners could seek to form partnerships; however, the nature and function of these partnerships may be more limited than when a public health authority is involved. For example, a HIPAA covered entity, such as a hospital, may share information with a third party acting as a business associate for the hospital pursuant to a business associate agreement. If specified in the business associate agreement, the business associate could perform data analysis, mapping, or data processing functions on behalf of the hospital; however, all functions performed by the business associate must be consistent with the terms set forth in the business associate agreement. Business associates who use the data or disclose the data to third parties must comply with the terms of the business associate agreement and all applicable HIPAA requirements, including those related to data aggregation and de-identification as applicable.[10]

7. Public Health Accreditation Board (PHAB), Standards & Measures for Domain 1: Conduct and Disseminate Assessments Focused on Population Health Status and Public Health Issues Facing the Community, and Domain 4: Engage with the community to identify and address health problems, available at http://www.phaboard.org/wp-content/uploads/SM-Version-1.5-Board-adopted-FINAL-01-24-2014.docx.pdf.
8. See 45 CFR § 164.501, definition of Public health authority; and 45 CFR § 164.514(h), verification requirements.
9. See 45 CFR § 164.502(e); 45 CFR § 504(e)
10. See 45 CFR § 164.502, 164.514(a) and (b), and 164.501 (definition of data aggregation).

PUBLIC PRESENTATION OF INFORMATION FROM CARDIFF MODEL PARTNERSHIPS

Lastly, the Cardiff Model program may raise questions about what injury incident data can be shared, presented, or discussed with the public. For example, Cardiff Model partnerships in other countries have benefitted from presenting maps at community forums or among a broad set of municipal partners. Health care providers that provide data for this program may have concerns about disclosing information that may ultimately be shared publicly. To allay these concerns, maps showing the locations of violent incidents occurring in public or commercial spaces and treated at a hospital may be presented by aggregating incident information over time such that the information could not be used to identify an individual. An example map is presented below. The minimum time period for aggregation should be one month. Summary descriptive information, such as listing the businesses experiencing the highest counts of violent injuries in a city, can also be presented.

EXAMPLE MAP OF INCIDENTS COLLECTED BY EMERGENCY DEPARTMENT

TECHNICAL CONSIDERATIONS

The Cardiff Model does not require any specific technologies for implementation. Efficient capturing, comparing, and mapping of violent incidents can be done with minimal technological inputs or advanced technological support. However, there are several components of the Cardiff Model that require consideration of current and future technological capacity.

11. See 45 CFR § 164.502(b).

COLLECTING INFORMATION

Collecting injury information can be accomplished through separate data forms or integrated into a hospital's existing electronic medical record (EMR) system. Integration of injury information into the EMR is the most efficient process for collecting and extracting data.

CLEANING INFORMATION

Once collected, injury information needs to be retrieved from the EMR and/or organized. Before a HIPAA covered entity can share this information, it needs to be reviewed and cleaned to ensure it does not contain more than the necessary data elements for the purposes of the project (most patient identifiable information will be excluded)[11] and that the information is entered in the correct data fields. This is also a good time to consider how to benchmark the extent and quality of the information that is collected.

SHARING INFORMATION

The technical requirements for sharing information will depend on the data sharing agreement established by the local partnership. Important considerations include the data format (i.e. structure and file type), the security of data transfers, frequency of data transfers, and potential for computer-automated sharing.

MAPPING

Mapping areas of violence (known as "hotspots" by law enforcement) can be accomplished by using a range of technologies. Partnerships may have the capacity to use advanced mapping processes to create maps. There are also a range of mapping resources, including free and open source software, such as R or QGis, for producing maps and managing geospatial data.

SECURING INFORMATION

Any electronic protected health information created, received, maintained or transmitted by a HIPAA covered entity or its business associate must be used or disclosed consistent with the HIPAA Security Rule.[12] Participating organizations that are not subject to HIPAA should also consider the use of protective mechanisms such as data encryption or other forms of web-based data transfer security for data sharing.

MONITORING AND EVALUATING

Regular monitoring and evaluation of the data collection system is important, especially during the early stages of implementation. Collaborating institutions should consider the technological inputs required to ensure that the injury information collected from the health system and law enforcement agencies is as accurate and complete as possible, and to monitor the changes that occur as the program progresses.

FINANCIAL CONSIDERATIONS

Initiation and maintenance of the Cardiff Model may be based on volunteer effort or supported through municipal, foundation, or federal/state grants. However, the Cardiff Model can be feasibly implemented without external funding (e.g., grants) if there is institutional support for dedicating staff time to work on the initiative, as staff time is the major input. Small amounts of funding to support data collection, data collection system development, and incentives to support program activities are helpful. Cost-benefit analyses reveal that the model saves approximately **$25 in criminal justice costs and $19 in health system costs for every $1 spent.**[13] Potential costs to bear in mind include:

12. 45 CFR § 164.302.
13. Florence, Curtis, et al. "An economic evaluation of anonymised information sharing in a partnership between health services, police and local government for preventing violence-related injury." Injury prevention 20.2 (2014): 108-114

PERSONNEL

What financial or other compensation (if any) are required to:

- Develop and sustain the community safety partnership
- Refine the information collection system (e.g., hospital IT staff time if integrated into an electronic medical record)
- Collect information
- Conduct trainings and promote the program among staff and within the community
- Clean, transfer, and map data
- Attend partnership meetings and other program activities
- Develop and implement violence prevention interventions
- Write and apply for grants

HARDWARE AND SOFTWARE

Will there be additional costs to:

- Collect, store, and manage violence-related injury information data
- Program data collection fields into an electronic medical record or other parallel database
- Create and maintain a process for data to be secured and securely shared
  - » Manual
  - » Automated
- Procure mapping software

PARTNERSHIP FACILITATION

Who pays and what will be the costs for:

- Partnership meetings
- Partnership materials (i.e. program promotion, local branding)
- Public events

PROGRAM EVALUATION

What support is required for the monitoring and evaluation of:

- Program Effectiveness
  How will the evaluation of process or outcome effectiveness of a local program be supported?
- Cost-benefits
  How will the evaluation of cost savings associated with local prevention of violence and violent injuries relative to program inputs be supported?

LEARN MORE about the Cardiff Model and how to start using it in your community's violence prevention efforts at **www.cdc.gov/violenceprevention/fundedprograms/cardiffmodel**

This material was developed by the Centers for Disease Control and Prevention (CDC). The pilot of the Cardiff Violence Prevention Model was a collaboration between the CDC, DeKalb County Police Department, Grady Health System, the University of Pennsylvania, and the CDC Foundation. Support for this pilot was provided by the Robert Wood Johnson Foundation.