POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

City of Seattle Privacy Impact Assessment

RIDEALONG RESPONSE PROJECT

Owner: Seattle Police Department
Date: 10/31/2016

CONTENTS

PURPOSE OF PIA

A Privacy Impact Assessment is designed to outline the anticipated privacy impacts from a City project/program or project/program update that collects, manages, retains or shares personal information from the public. The PIA will provide project/program details that will be used to determine how privacy impacts may be mitigated or reduced in accordance with the City of Seattle Privacy Principles and Privacy Statement.

ABSTRACT

***Please provide a brief abstract.** The abstract is the single paragraph that will be used to describe the project and **will be published on the Privacy Program website.** It should be a minimum of three sentences and a maximum of four, and use the following format:*

- *The first sentence should include the name of the project, technology, pilot, or project/program (hereinafter referred to as "project/program").*
- *The second sentence should be a brief description of the project/program and its function.*
- *The third sentence should explain the reason the project/program is being created or updated and why the PIA is required. This sentence should include the reasons that caused the project/program to be identified as a "privacy sensitive system" in the Privacy Intake Form, such as the project/program requiring personal information, or the technology being considered privacy sensitive.*

Definitions: For purposes of this PIA, the following definitions apply:

"Crisis Response Unit" or "CRU" is the unit of the Patrol Operations Unit comprised of the Crisis Response Team responsible for responding to incidents in the field and for following up on incidents involving subjects in crisis and where warranted, developing a Crisis Response Plan based on factors reflected in the Seattle Police Department (SPD), SPD Manual 16.110. The CRU is also responsible for administering the operational aspects of the RideAlong Response application.

"Crisis Response Plan" is an individualized plan tailored to an individual's needs and behavioral challenges. A plan contains guidance to officers responding to a person in behavioral crisis on how to best approach the person and information on how to mobilize an individual's support network of service providers and family members.

"Core Profile" is information entered in the app about an individual who does not have a Crisis Response Plan but who has had seven or more Crisis Incident Templates submitted in the last year.

Abstract: The RideAlong Response Project gives patrol officers and dispatchers an application to access Crisis Response Plans, and Core Profiles of individuals that Seattle Police Department patrol officers frequently contact for mental health-related behavioral issues. The application provides officers ready access to information tailored to the individual, including specific techniques for understanding behavior, approaching and communicating with the individual during encounters to de-escalate the situation, as well as case manager contact information. The project collects and assembles highly-sensitive information about individuals with Crisis Response Plans who frequently contact police because of mental-health related issues, including mental health care, and substance abuse treatment information. A PIA is required because of the nature of the data in the app and the heightened privacy interest in that data.

Background: RideAlong Response is a web-based application that contains Crisis Response Plans previously stored on a bulletin system alongside “wanted” or “missing person” bulletins, shared with officers via email. The application provides a better way to deliver this useful information to officers in the field than the pre-existing bulletin delivery method. A review of resource allocation across twelve individuals with Crisis Response Plans in 2015 showed a 72.6% reduction in the amount of police hours after implementation of a plan (comparing three-month periods before and after a plan was in place). The application allows officers to view the Crisis Response Plans and Core Profiles on the officers’ in-car computer and mobile phones. The application displays key information in a way that is easier for officers to scan while in route to a scene.

SPD’s interaction with persons in crisis is a key component of the Consent Decree with the Department of Justice (DOJ). SPD’s Crisis Intervention Policy was developed by SPD in conjunction with the Crisis Intervention Committee ("CIC"), an interagency group composed of a cross-section of stakeholders, including mental health professionals, clinicians, community advocates, academics, and representatives of the judiciary and non-SPD law enforcement agencies. The CIC develops the critical components of SPD's strategy for engaging with individuals who are in behavioral crisis (e.g., experiencing mental health issues, substance abuse concerns, etc.). All officers received basic training in crisis intervention issues and techniques in 2014, and all are receiving follow-up training during 2015.

The Seattle Police Monitor’s Fifth Systemic Assessment of SPD’s progress toward complying with the provisions of the Consent Decree with the Department of Justice states that SPD “has recognized the importance of crisis work and dedicated significant resources to create a full-fledged crisis intervention program.” SPD Manual 16.110 prescribes policy for providing all officers with resources for individuals in behavioral crisis. The Crisis Intervention Team is composed of certified officers who respond to persons in mental health crises, with the objective of diverting them from the criminal justice system and getting them help to address their physical and mental health needs. This not only provides more appropriate treatment to individuals in crisis, but also reduces the justice system costs associated with the mentally ill. RideAlong Response assists in and enhances SPD’s crisis intervention efforts.

Officers are required to fill out a Crisis Intervention Template documenting all contacts with subjects who are in behavioral crisis (SPD Manual 16.110-POL-9). The CRU triages behavioral crisis incidents for follow up (16.110-POL-12). Crisis Response Plans are initiated by identifying incidents involving a person in behavioral crisis who demonstrates a pattern of escalating behavior or whose behavior causes a significant risk of injury to themselves or others. The CRU develops the plans by utilizing best practices and intervention strategies based on a sequential intercept continuum, by speaking with existing support structures, by including patrol officer input, and, if feasible, by speaking to the person in crisis.

SPD has distributed Crisis Response Plans in the past by preparing a bulletin, storing it on a bulletin system alongside “wanted” or “missing person” bulletins, and sharing it with officers via email. The RideAlong Response program makes the information more searchable and accessible to officers in the field in real-time. It also limits access to sensitive information because access to the app is more restricted than distribution via email or on the SPD in-web, as only authorized individuals with a need for the information can access it.

RideAlong Response application was built by Code for America, a national non-profit technology organization that partners with city governments to build technology. This is part of a structured fellowship program where a city agrees to host three Code for America fellows. The team builds an application for the city around a specific area using open source software and user-centered design. The application is then provided to the city for a free licensing cost for the entire life of the application, and includes the original code. Code for America and the Seattle Police Department were programmatic partners in building RideAlong Response.

(2018 Update: RideAlong it is now a commercial company and the City of Seattle holds contract is with that company.)

PROJECT/PROGRAM OVERVIEW

Please provide an overview of the project/program. *The overview provides the context and background necessary to understand the project/program's purpose and mission and the justification for operating a privacy sensitive project/program. Include the following:*

- *Describe the purpose of the system, technology, pilot or project/program; the name of the department that owns or is funding the project/program and how it the project/program relates to the department's mission;*
- *Describe how the project/program collects and uses personal information, including a typical transaction that details the life cycle from collection to disposal of the information;*
- *Describe any routine information sharing conducted by the project/program both within City of Seattle departments and with external partners. Describe how such external sharing is designed with the original collection of the information.*
- *Identify any major potential privacy risks identified and briefly discuss overall privacy impact of the project/program on individuals*
- *Identify the technology used and provide a brief description of how it collects information for the project/program.*

By giving patrol officers ready access to information that enables them to provide better service to residents in mental health crises, this program directly relates to SPD's core mission of protecting and serving its residents. The application makes contact information for case managers, guidelines tailored for interacting with specific individuals, plus background information to aid in those interactions readily available to officers in the field. The metrics for success of the program include lower rates of recidivism and incarceration, lower use of force rates, increased referrals to mental health service providers, and increased communication between patrol officers and the CRU. The initial funding for the project comes from a combination of the Seattle Police Foundation and money raised by Code for America through private foundations.

The application contains information about individuals with Crisis Response Plans and individuals with seven or more Crisis Incident Templates in the last year. Currently there are about forty people with Crisis Response Plans. There are about eighty additional people with Core Profiles in the app as those individuals have had seven or more Crisis Incident Templates in the last year, but who do not have Crisis Response Plans.

The project is designed to provide patrol officers easier and direct access to the Crisis Response Plans and crisis incident information at the point of the encounter with individuals. The underlying goal is to improve the service provided to those who suffer with mental health issues resulting in safer interactions for both individuals and officers. A Lieutenant and two Sergeants oversee the CRU and are responsible for developing Crisis Response Plans.

Typically, a patrol officer with the CRU will write a response plan about a person who has a mental health issue and who has had multiple interactions with SPD as a direct result of those issues. The response plan will be approved by the CRU Sergeant. After approval, it will be available for all patrol officers to access on their Mobile Data Terminals (MDTs), at an internal Department desktop computer, or on Department-issued smart phones and laptops that can access the SPD Network via Virtual Private Network (VPN). It will be available for dispatch personnel to use in responding to crisis calls from or about the individual. Supervisory personnel will also have access to plans. Having direct access to the response plan will assist SPD personnel in referring individuals in crisis to appropriate care with the goal of avoiding future crises and eventually diminishing the need for an individual to have a plan. Once individuals receive the help they need, their calls to SPD should decrease and even stop.

The CRU is responsible for writing, updating, and removing response plans from active view in the application. In creating plans, CRU focuses on “actionable” information from the case workers/social services. It does not focus on diagnostic information but rather on observable symptomatic behavior and best practices regarding how to interact with those behaviors in the middle of a behavioral crisis. Since the information reflects actual observed behavior from previous experiences with the person in crisis, it tends to be more specific and reliable.

The CRU does not enter unnecessary information into the plan. The application has a technical constraint built in with an “editor/ supervisor” function for approval before publication of a plan: a CRU Sergeant must approve a plan prior to publishing to ensure compliance with the required criteria. A Crisis Response Plan will not be disseminated prior to approval by CRU staff, thus helping to ensure that officers and dispatchers have access to accurate, relevant and appropriate information.

The RideAlong Response program has a built-in feedback option for patrol officers to provide the CRU with updated information related to a specific individual’s plan. The CRU reviews this information, applying the same standards used in creating the plan, and must approve it before it is entered a plan.

The RideAlong Response program will flag plans for a mandatory review every six month. During the review, the CRU will assess whether the plan should be kept or removed, make necessary edits to details within the plans, verify the contact information of people included in the plans (i.e. case managers), and determine if the plan is still needed; e.g., has it been three years since the last incident.

If a plan is ‘retired’ from active view, then it will remain in the system for the same retention period as the corresponding General Offense Reports. For example, low-level interactions or crimes remain in the system for six years, so inactive response plans will also be kept for that time. Additionally, if a person who only has a Core Profile falls below seven Crisis Incident Templates in the last 365 days, the Core Profile will be automatically removed from the app’s active view.

In addition to the response plans, the application pulls and displays information from the Crisis Incident Templates into the same view, giving officers a quick synopsis of the police incident history with that person. This includes the behaviors shown on past incidents, the nature of the crisis, disposition of past calls, and the template narrative. The following data is also pulled from the Records Management System

(REPOSIT): verified name, date of birth, physical characteristics, and address. Only information from the Crisis Incidents Templates and Records Management System is entered in the application for individuals who do not have Crisis Response Plans but have had seven or more Crisis Incident Templates in the last year.

There is currently no ability to share an individual's information in the app with individuals outside of the police department through the app directly. All users logging into the application must have valid SPD Active Directory credentials. Information about contacts with persons in crisis will be shared in the same manner currently shared as part of the SPD's internal work flow; the information could also be used in the Office of Public Affairs (OPA) complaint investigations, Use of Force investigations, or similar internal oversight processes. The information in the application could also be used by police officers to communicate externally with case managers, prosecutors, defense attorneys, and care givers. The actual contents of the RideAlong Response will not be disseminated proactively. SPD must comply with the disclosure requirements of the Public Records Act (PRA), Chapter 42.56 RCW. SPD will apply all applicable PRA exemptions, including other confidentiality statutes to prevent unauthorized disclosure of information, to maintain the confidentiality of the identity of individuals entered in the app. Anonymized aggregate data from the app will be used to track successes and other metrics related to crisis calls. This anonymized aggregate data and analyses will be shared with the DOJ Monitor and may be shared publicly with others.

NOTIFICATION

1. ***How does the project/program provide notice about the information that is being collected?*** *Our Privacy Principles and Statement require that we provide notice to the public when we collect personal information, whenever possible.*
    - *Describe how notice will be provided to the individuals whose information is collected by this project/program and how it is adequate.*
    - *If notice is not provided, explain why not. (For certain law enforcement or other project/programs, notice may not be appropriate.)*
    - *Discuss how the notice provided corresponds to the purpose of the project/program and the stated uses of the information collected.*

    The response plans are developed based on an imminent safety concern, repeated and escalating behavior, and extremely high-utilization of 911 services as the result of symptomatic behavior of individuals in crisis. No specific notice is given to individuals at the time of an encounter with an individual in crisis that their information has been entered in the application. Individuals generally are aware of their contacts with police. Most of the information in the application is pulled from information entered on the Crisis Incident Template from previous encounters with police.

    If the person has a response plan, it means the CRU has worked with the case manager to get input on the information for the response plan and the case manager is aware of the response plan.

2. ***What opportunities are available for individuals to consent to the use of their information, decline to provide information, or opt out of the project/program?*** *Describe how an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use?*

If notice is provided explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. Note: An example of a reason to not provide an opt-out would be that the data is encrypted and therefore unlikely available to identify an individual in the event of a data breach.

The individuals in the application do not have the ability to opt out during a crisis response, just as they generally have no ability to opt out of interaction with the police when in crisis. Individuals have the right to inspect criminal history record information maintained by the department and to seek correction of any incorrect information (RCW 10.97.030, SPD Policy 12.050).

Ensuring the accuracy of information in the application is key to its success. When researching and working with the case managers, the CRU will work to correct and update information as needed. Additionally, patrol officers can send the CRU an email through the application to correct any erroneous information they observe. If the CRU finds any incorrect information through patrol officer feedback, following up with the case manager, or other means, including input from the subject, the information will go through the editor/supervisor approval process and the plan will be updated or removed as approved, applying the same standards used in creating the plan.

COLLECTION

3. ***Identify the information, including personal information, that the project/program collects, uses, disseminates, or maintains.*** *Explain how the data collection ties with the purpose of the underlying mission of the department.*

Information from REPOSIT is pulled to allow officers to search in the application by the following components: name, date of birth, age, race, gender, eye color, hair color, weight, and height. Additionally, officers will view the person's scars, marks, and tattoos.

The application pulls all information from the Crisis Incident Templates (also on REPOSIT) and relevant information is available for patrol officers to see. This information includes the behaviors shown on past incidents, the nature of the crisis, disposition of past calls, known veteran status, and the template narrative. This information is used for different parts of the patrol-facing and CRU-facing purposes of viewing key information and analyzing impact of the application. For example, the common behaviors displayed by the person as collected in the Crisis Incident Templates will be included in the officer-view. Whether reportable use of force was used will only be used by the CRU as part of assessing whether the application has helped to foster safer interactions between police and residents.

Interacting with a person in behavioral crisis is a complex and demanding endeavor which requires a high level of skill and technique. It is so complicated that officers are often required to respond to clinical settings and assist clinical staff and Mental Health Professionals (all of whom have specific, years-long training working with persons in crisis) in de-escalating persons in crisis. Additionally, SPD and police agencies in general are seeking alternative means of bringing a situation to non-custodial outcomes. Information is essential to exploring and achieving other more appropriate options for individuals in crisis. The RideAlong Response enables officers to see previously exhibited behaviors, existing case management, previously attempted diversion attempts, officer safety information (if applicable), and best practices for working with the historically identified behaviors. This should lead to a reduction in use of force, jail bookings, and unnecessary emergent detention (ERs)—all of which are better outcomes for individuals, the police, and service providers.

4. ***Is information being collected from sources other than an individual, including other IT systems, systems of records, commercial data aggregators, publicly available data and/or other departments?*** *State the source(s) and explain why information from sources other than the individual is required.*

   All information is collected, stored, and maintained on the City of Seattle network. The CRU manually enters certain information into the application; i.e., response plan, emergency contacts, background information, demeanor of the person in behavioral crisis, notable officer safety concerns, plus hooks, and triggers. The CRU meets with current service providers, family, or any other existing support structure to inform the process of developing response plans. Information regarding current case management (services) is relayed from county databases.

   (2018 Update: RideAlong has been moved to the Microsoft Azure platform.)

   The following information is drawn from REPOSIT: full name, date of birth, gender, race, height, weight, eye color, hair color, scars/marks/tattoos, address, and all data from existing Crisis Incident Template submissions.

   The information is required from observant sources other than the individual to fully develop the response plan.

USE

5. ***Describe how and why the project/program uses the information that is collected****. List each use (internal and external to the department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used.*

   All information is collected, stored, and maintained on the City of Seattle network. The CRU manually enters certain information into the application; i.e., response plan, emergency contacts, background information, demeanor of the person in behavioral crisis, notable officer safety concerns, plus hooks, and triggers. The CRU meets with current service providers, family, or any other existing support structure to inform the process of developing response plans. Information regarding current case management (services) is relayed from county databases.

   The following information is drawn from REPOSIT: full name, date of birth, gender, race, height, weight, eye color, hair color, scars/marks/tattoos, address, and all data from existing Crisis Incident Template submissions.

   The information is required from observant sources other than the individual to fully develop the response plan.

6. ***Does the project/program use technology to:***
   a. ***Conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly or***
   b. ***Create new information such as a score, analysis, or report?***

If so, state how the City of Seattle plans to use such results. Some project/programs perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Explain what will be done with the newly derived information. Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data?

The application pulls information from REPOSIT, allowing an officer to search in the application by the following components: name, date of birth, age, race, gender, eye color, hair color, weight, and height. Additionally, officers will view the person’s scars, marks, and tattoos. This enables the officer to identify a person in crisis who will not or cannot provide identifying information so that the officer can provide the appropriate response.

There is no component of the application that finds patterns and predicts future behavior. The information in the application compiles past behavior to give officers context for the present encounter. The application also auto-generates ‘best practices’ from the Crisis Intervention Training based on those past behaviors shown. The application does create new information about the individual by compiling existing information automatically. One example is that it shows the percentage of times that an individual has exhibited a specific behavior. The derived information is used by the responding officers to better inform their immediate decision making when interacting with an individual in crisis.

7. ***How does the project/program ensure appropriate use of the information that is collected?*** *Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

The program ensures appropriate use of information in several ways. First, by policy only the Crisis Response Unit can edit the plans and Core Profiles directly. Second, only approved users with an appropriate business need are included within a specific Lightweight Directory Access Protocol (LDAP) group that controls access to sign into the application and view the information. The users and the information they view are monitored by the application and this activity log information can be exported as a Comma Separated Variable (CSV) for DATA to view and audit.

Access to RideAlong Response is governed by SPD Policy 12.050 “Criminal Justice Information Systems” (CJIS) which is the standard applied to all other CJIS technology. The policy states, “For the purposes of this policy, the RideAlong Response application is considered a criminal justice record system that contains criminal history record information.” SPD Policy 12.050 was implemented using E-Directive 16-00024 and the RideAlong Response application will be covered in greater detail in the 2017 SPD Crisis Intervention Team (CIT) training block.

RETENTION

8. ***Does the project/program follow the City records retention standard for the information it collects?*** *Departments are responsible for ensuring information collected is only retained for the period required by law. City departments are further responsible for reviewing and auditing their compliance with this process. For more information, please see the internal retention schedule, here, and records retention ordinance, here.*

In addition, please provide answers to the following questions:

- *How does it dispose of the information stored at the appropriate interval?*
- *What is your audit process for ensuring the timely and appropriate disposal of information?*

The CRU is responsible for writing, updating, and removing response plans from patrol officer view in the application. The application automatically sends an email to the CRU with a list of plans and people that need review. This is set up so that plans will be reviewed every six months. The CRU will assess whether a plan should be kept or removed, edit details within the plans, and verify the accuracy of contact information of people included in the plans (i.e. case managers). A plan may be retired from active view because there have been no new incidents related to the observed previous behavior. Due to the complex nature of these types of events, these assessments will be made on a case by case basis and in conjunction with communication with case management staff (if appropriate).

If a plan is 'retired' from active view for patrol officers, then it will remain in the system for as long as the corresponding General Offense Reports. For example, low-level interactions or crimes remain in the system for six years, so inactive response plans will also be kept for that time. Additionally, if a person who only has a 'Core Profile' falls below seven Crisis Incident Templates in the last 365 days, then they will automatically be removed from the app's view for patrol officers.

SHARING

9. ***Are there other departments or agencies with assigned roles and responsibilities regarding the information that is collected?*** *Identify and list the name(s) of any departments or agencies with which the information is shared and how ownership and management of the data will be handled.*

CRU personnel have full ownership and control of the Crisis Response Plan content. Content for 'Core Profiles' is controlled by the source systems from which that data originates. Only SPD and City IT personnel with specific authorization may access the application directly.

Information contained in the application may be used by police officers to communicate with case managers, prosecutors, defense attorneys, and caregivers to the extent those individuals have the appropriate authorization to access the information. Case managers, prosecutors, defense attorneys, and caregivers are subject to the same confidentiality provisions regarding mental health care related information as SPD.

SPD must comply with the disclosure requirements of the Public Records Act (PRA), Chapter 42.56 RCW. SPD will apply all applicable PRA exemptions, including other confidentiality statutes to prevent unauthorized disclosure of information, to maintain the confidentiality of the identity of individuals entered in the application to the extent allowed by law.

Anonymized aggregate data from the application may be shared publicly with the DOJ Monitor and others. The application itself will not be shared directly with other departments, agencies, or individuals.

10. ***Does the project/program place limitations on data sharing?***

Describe any limitations that may be placed on external agencies further sharing the information provided by the City of Seattle. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment.

Anonymized aggregate data from the application may be shared publicly with the DOJ Monitor and others. The application itself will not be shared directly with other departments, agencies, or individuals.

11. ***What procedures are in place to determine which users may access the information and how does the project/program determine who has access?*** *Describe the process and authorization by which an individual receives access to the information held by the project/program, both electronic and paper based records. Identify users from other departments who may have access to the project/program information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project/program information. Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication).*

The application login process checks authentication requests against an SPD Active Directory group that derives the authorized user membership from a collection of other SPD Active Directory groups created for the Digital Evidence Management System (DEMS). These DEMS Active Directory groups align user accounts to job role and responsibilities. The user accounts are added or removed as per normal policies within the department. The aggregate resulting set of individuals with access (patrol officers, dispatchers, and specific supervisory personnel) are thus authorized to log into the application.

Sworn officers and personnel within precincts may also see printed-out profiles and response plans if officers choose to print out someone's information from the application. All SPD employees are backgrounded, and the information will be handled the same way that CJIS information and other confidential records are handled within SPD as governed by SPD Policy 12.050.

CRU has two levels of administrative access to the app: editor and supervisor. Editors can edit response plans and then submit them to a supervisor for approval. Supervisors approve response plans for public view, add editors and other supervisors, and can access the full set of administrative features. The two CRU Sergeants have been granted access as supervisors. The CRU patrol officers are designated as editors. IT personnel will have administrative access to the application platform but no administrative rights within the application itself.

The application may only be accessed from local endpoint devices (e.g., computers, laptops) authorized on the internal network or for remote endpoint devices deployed in the field (e.g., remote laptops, SPD smartphones). These devices are granted access through the SPD VPN via the f5 VPN client. The provisioning, use, and removal of such access follows existing SPD protocols.

Currently, only a limited number of Patrol officers have department-issued smartphones that allow VPN access (e.g., Bike Patrol Officers).

12. ***How does the project/program review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?*** *Please describe the process for reviewing and updating data sharing agreements.*

    Not applicable: the application is not shared outside of SPD.

LEGAL OBLIGATIONS AND COMPLIANCE

13. ***Are there any specific legal authorities and/or agreements that permit and define the collection of information by the project/program in question?***
    - *List all statutory and regulatory authority that pertains to or governs the information collected by the project/program, including the authority to collect the information listed in question.*
    - *If you are relying on another department and/or agency to manage the legal or compliance authority of the information that is collected, please list those departments and authorities.*

    The information collected is pulled from the Records Management System (RMS) and the Crisis Incident Templates completed in connection with SPD officers' law enforcement duties. Additional information is collected in compliance with SPD Manual 16.110.

14. ***How is data accuracy ensured?*** *Explain how the project/program checks the accuracy of the information. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. If the project/program does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project/program.*

    The SPD master name index assigns each individual a Personal Identification Number (PIN) to differentiate between individuals who may, for example, have similar names but different dates of birth. The information automatically pulled into the application goes through an import script. This script pulls information from REPOSIT and finds matching GO numbers between the Crisis Incident Template and the full GO report. From there, it compares the first and last name of the person on the Crisis Incident Template with those involved in the GO report. It then uses that person's PIN number to their physical characteristics and address location from REPOSIT into the application. This ensures the application contains accurate information about the correct individuals.

    If there is no match on the initial name, then that entire Crisis Incident Template is not used. The application also keeps audit logs of all the imports from RMS which the application makes, including why information was and was not included in the import. If a person's information is updated in

    RMS (i.e. change of address), then on future imports the data will automatically synchronize with the application. Additionally, the form to create a plan and edit information both allows CRU officers to locally update information from RMS (i.e. more updated weight), and requires information to be listed in a standard data format (e.g., someone cannot be 5' 13").

    The CRU reviews every plan in the application at least every six months. The CRU also reviews a plan when officers in the field submit feedback if they suspect any information in the application is incorrect. These measures help to ensure accuracy within the application, which is essential to its effective use.

15. ***What are the procedures that allow individuals to access their information?***
Describe any procedures or regulations the department has in place that allow access to information collected by the system or project/program and/or to an accounting of disclosures of that information.

Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request. The CRU will provide a point of contact on the SPD website for individuals who wish to inquire about a Crisis Response Plan or Core Profile.

16. ***What procedures, if any, are in place to allow an individual to correct inaccurate or erroneous information?*** *Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If none exist, please state why.*

Individuals cannot directly access their information, so they cannot update it. Individuals have the right to inspect criminal history record information maintained by the department and to seek correction of any incorrect information (RCW 10.97.030, SPD Policy 12.050). If the CRU finds any incorrect information through patrol officer feedback, following up with the case managers, or other means including input from the subject, the plan will go through the editor/supervisor approval process and information will be updated or removed as approved.

17. ***Is the system compliant with all appropriate City of Seattle and other appropriate regulations and requirements?*** *Please provide details about reviews and other means of ensuring systems and project/program compliance.*

The project pre-dates the new stage gate process currently being refined by Seattle IT, and thus the artifacts that would have been created as part of that process (e.g., formal business case) do not exist.

18. ***Has a system security plan been completed for the information system(s) supporting the project/program?*** *Please provide details about how the information and system are secured against unauthorized access.*

An SRC review was completed and relevant security controls were identified and implemented.

The application stores police data on servers owned and managed by the City of Seattle. The individual application components and communication between them are not visible from outside the docker container, effectively firewalling off the internal components from external users and systems.

As previously mentioned, the application will make outbound LDAP calls to determine if a user is authorized to access the application by membership in the appropriate LDAP group. If the user is an authorized member, the actual rights are authorized based on that user's role designation within the application layer itself. Thus, if the user is authorized to access the application for any reason, the actual capabilities are limited to those assigned by the application administrators.

19. ***How is the project/program mitigating privacy risk? G****iven the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.*

    Privacy risk mitigation includes secure input and use of the data on SPD-only networks, limiting access to the data entry portion of the application to CRU staff, limiting access to the active application to patrol officers, dispatchers, and identified supervisory personnel, providing officer training on how and when to use the information in the application, specifying that the application contains CJIS information (SPD Policy 12.050), and applying the appropriate legal standards for disclosure of information in the application.

MONITORING AND ENFORCEMENT

20. ***Describe how the project/program maintains a record of any disclosures outside of the department.*** *A project/program may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project/program keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the project/program must be able to recreate the information noted above to demonstrate compliance. If the project/program does not, explain why not.*

    A record of disclosure of any information in the application pursuant to a Public Records Act Request or subpoena would be maintained in the business records of the Legal Unit. Information in the application may be discussed with the subject. It may also be discussed as part of a care management conference with the appropriate authorization from the individual for release of confidential information.

21. ***Have access controls been implemented and are audit logs are regularly reviewed to ensure appropriate sharing outside of the department?*** *Is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies? Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

    The application automatically logs and tracks the use of the application, the import of information into the application, and the edits made to each plan. These are available within the application to be exported by data base administrators. This does not require an external party to remove the information.

22. ***How does the project/program ensure that the information is used in accordance with stated practices of the project/program?*** *What auditing measures are in place to safeguard the information and policies that pertain to them? Explain whether the project/program conducts self-audits, third party audits or reviews.?*

    After every incident involving a person with mental health issues, the officer must fill out a Crisis Incident Template (CIT). A CRU staff member reviews every report that includes a CIT to ensure that officers are acting in compliance with CIT training and best practices. The Sergeant personally reaches out to officers to offer feedback. This will continue with the application, including monitoring how the application is used within each incident.

As previously mentioned, there are logs to audit and track the use of the application, the import of information into the application, and the edits made to each plan. These are available within the application to be exported by data base administrators. This does not require an external party to remove the information.

23. ***Describe what privacy training is provided to users either generally or specifically relevant to the project/program.*** *City of Seattle offers privacy and security training. Each project/program may offer training specific to the project/program, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to personal information are trained to handle it appropriately. Explain what controls are in place to ensure that users of the system have completed training relevant to the project/program.*

An e-module (web-based learning) has been developed for mandatory review by users and compliance prior to the launch of the application itself. This training provides basic instructions for use of the program for officers. The policy directive that all officers must read was released to all SPD officers on September 27, 2016 via e-Directive. The policy directive included a quiz to ensure that the officers reviewed the information. Failure to read e-Directives can result in disciplinary action.

24. ***Is there any aspect of the project/program that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?*** *Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected that is not explained in the initial notification.*

Mental health care information, criminal history records information, and other private and sensitive information are entered into the application. In addition, the application will contain triggers and de-escalation techniques specific to an individual that could be used to harm the individual if used improperly. In addition to the internal measures indicated above which maintain the accuracy and confidentiality of the information, the SPD Crisis Intervention Policy was developed by SPD in conjunction with an interagency group composed of a cross-section of stakeholders, including mental health professionals, clinicians, community advocates, academics, non-SPD law enforcement, and representatives of the judiciary. SPD consulted with and will continue to work collaboratively with these groups as we move forward with the application.