Pennsylvania Justice Network

PRIVACY POLICY

5 Technology Park
Harrisburg, PA 17110
January 15, 2013

Table of Contents

JNET Purpose Statement

The Pennsylvania Justice Network (JNET) is an integrated, secure justice portal providing an online environment for authorized users and systems to access public safety and criminal justice information. JNET is the Commonwealth's primary public safety integration service provider.

JNET is a result of a collaborative effort of municipal, county, state, bordering states and federal justice agencies to build a secure integrated justice system. While each agency maintains ownership and control of their data, JNET allows authorized criminal justice and public safety professionals to securely and safely access information from multiple providers through one interface.

Many commonwealth agencies contribute information within the JNET secure portal including the following:

- Administrative Office of Pennsylvania Courts
- Juvenile Court Judges' Commission
- Pennsylvania Board of Probation and Parole
- Pennsylvania Chiefs of Police Association
- Pennsylvania Commission on Crime & Delinquency
- Pennsylvania Commission on Sentencing
- Pennsylvania Department of Corrections
- Pennsylvania Department of Health
- Pennsylvania Department of Public Welfare
- Pennsylvania Department of Transportation
- Pennsylvania State Police

With such a large and diverse group of data providers, it is imperative that JNET develop policies and procedures to protect the use, dissemination, and protection of each agency's information. It is also important that polices related to data use be as consistent as possible between data providers when practical.

Privacy Policy Purpose Statement

The purpose of this policy is to ensure that safeguards and sanctions are in place to protect individual privacy, civil rights and liberties, and other protected interests, as well as to protect the integrity of criminal investigations and justice system processes. The JNET Privacy Policy incorporates the principles of the Fair Information Practices as outlined by the National Criminal Justice Association (NCJA) as well as Department of Justice's (DOJ) Global Justice Information Sharing initiative privacy and civil liberties guidance and resources.

Scope

JNET is primarily an information sharing framework that enables participating agencies to access and share criminal justice information. JNET serves as a technical conduit through which information is made available to authorized users for authorized purposes. Typically, all information collection and record storage remains within the purview of partner agencies ("data contributors" or "data providers"), governed and controlled by law relevant to the functions and duties of the agencies and the purpose of the collection of information by the agencies.

However, JNET also stores or retains *some* Personally Identifiable Information data (both non-criminal justice and criminal justice)—typically user and system usage data, and PII that serves the Commonwealth's criminal justice community. It does not seek and/or retain information about individuals solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders or sexual orientations.

Hence, this document is focused on Personally Identifiable Information (PII) and criminal justice information that is gathered, collected, and maintained by JNET.

The JNET privacy policy fully adheres to the Commonwealth of Pennsylvania's Privacy Policy as defined on its public portal and in no way conflicts with any of the Commonwealth's overarching privacy policies. JNET does provide policy and procedures beyond that of the Commonwealth's umbrella policy. This policy applies to all who have access within the JNET organization, both Commonwealth employees and Contractors, as well as employees of those agencies that both provide and consume PII data via JNET.

Definitions

As used in this document:

"Agency" means: any unit of government in the Commonwealth of Pennsylvania, any county or combination of counties; department; institution; board; commission; district; council; bureau; office; governing authority; other instrumentality of state, county, or municipal government; or corporation or other establishment owned, operated, or managed by or on behalf of this Commonwealth or any county or municipality, but does not include the non-administrative functions of Pennsylvania's courts.

"Authorized user" means: a person, computer process, or device granted access to certain information, services, or functionality based on verified identity or credentials.

"Commonwealth" means: the Commonwealth of Pennsylvania

"Data Provider" means: the entity or agency that possesses and is responsible for information, and willingly provides it through JNET, to other authorized agencies for approved use.

"Disclosure" means: making a government record available for public inspection or duplication.

"Dissemination" means: the release, transfer, provision of access, sharing, publication, or divulging of a government record to a secured and vetted criminal justice user in any manner—electronic, verbal, or in writing.

"JNET" means: the Pennsylvania Justice Network.

"Law" means: any local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, or court rule, decision, or order.

"Non-justice purpose" means: the use of justice information for permitted purposes other than law enforcement or criminal justice, such as criminal background checks in connection with employment and licensing.

"Partner Agency" means: a justice or government agency participating in secure

information sharing through JNET

“Person” means: an individual, business, government, or governmental subdivision or agency, business trust, estate, trust, partnership, association, or any other legal entity.

"Personal record" means: any item, collection, or grouping of information about an individual that is maintained by an agency. It includes, but is not limited to, the individual's education, financial, medical, or employment history, or items that contain or make reference to the individual's name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

“Personally Identifiable Information (PII)”[1] means; any information about an individual, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

“Privacy” means: freedom from unsanctioned intrusion. It refers to individuals’ interests in preventing the inappropriate collection, use, and release of personal information.

“Public” means: exposed to general view; accessible to or shared by all members of the community.

“Role-based Access” means: a type of access authorization that uses job functions to restrict access rights and privileges.

“Security” means: the process by which privacy is ensured.

"Security breach" means: an incident of unauthorized access to and acquisition of unencrypted or un-redacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person.

Compliance with Laws Regarding Privacy, Civil Rights and Civil Liberties

JNET Office Staff and JNET Users, including contractors, will comply with all applicable state and federal laws, guidelines and policies protecting privacy, civil rights and liberties in the collection, use, analysis, retention, destruction, sharing, dissemination and disclosure of information made available through the Pennsylvania Justice Network information sharing facilities.

JNET’s security policies and user access agreements include information concerning relevant laws and policies that govern access, use, and dissemination of JNET information. Prior to granting an agency and its individual users access to JNET system resources, the agency and user must acknowledge receipt of those policies and agree to comply with their terms.

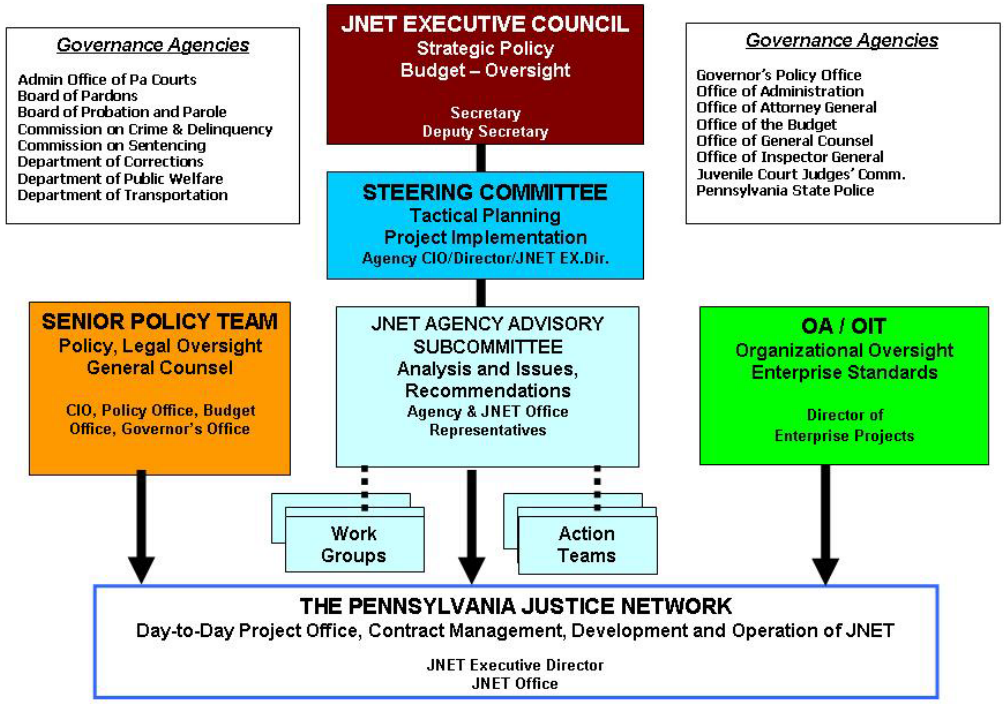
[1] This is the same definition as defined by NIST 800-122 and the federal Office of Management and Budget (OMB M-07-16)

This policy recognizes the existence of privacy policies within each participating agency, governing the collection, storage, dissemination, and destruction of statutorily protected information by the agency. Such agency privacy policies will provide greater detail than this policy and will address specific legal requirements for the protection of privacy, civil rights, and civil liberties, and will, at a minimum, be at least as comprehensive as the provisions contained within this JNET Privacy Policy.

Governance and Oversight

Organizationally, the JNET Office, including its Executive Director, reports to the Chief Information Officer (CIO) of the Commonwealth. However, it takes its direction from a Steering Committee comprised of members from 16 Commonwealth agencies who are appointed by each respective agency head. Each steering committee member has a voice in the strategic direction of JNET, how and what data is shared, and how policy and technical issues affecting their organizations and integrated justice are addressed. Steering Committee members chair and staff the JNET Agency Advisory Subcommittee (JAAS), and are advocates for JNET in each of their respective agencies. The JAAS has been charged with routinely reviewing changes to this Privacy Policy, and recommending approval to the Steering Committee.

JNET Governance Structure



The individual who serves as JNET's security and privacy officer is a Commonwealth employee who is responsible for overseeing the implementation of privacy protections. More specifically, this individual is responsible for:

- enforcing the Commonwealth Privacy Policy as defined in ITB-PRV001 *CoPA Electronic Information Privacy Policy*
- ensuring that all applicable federal, state, and other mandates specific to electronic privacy concerns that pertain to JNET are enforced.
- updating the JNET Privacy Policy and coordinating JAAS review

Public Access

JNET is not used as a mechanism for the general public to directly access, inspect, validate and/or duplicate justice information. Consequently, the JNET Privacy Policy does not address information privacy and protection from the public. Members of the general public who seek access to justice information are referred to the appropriate data-contributing agency for permission to access. Data-providing agencies' privacy policies are required to address privacy considerations and limitations on the public access to and dissemination of information retained by that agency.

JNET provides information exchange between participating agencies only. Policy regarding such exchanges (see *Information Sharing section for more information*) is described below.

Information Analysis

JNET provides data querying and reporting tools for those authorized users who want to perform statistical analysis of some of the data collected and retained at JNET. Currently, analysis is performed on JNET system and services usage data, automated warrants records transfer system statistics, county prison and probation/parole reporting transactions, and pre-sentence investigations statistics.

It is the policy of JNET to conform to the mandates of the Criminal History Record Information Act 18 Pa. C.S.A. §9101 et seq. (CHRIA), and to Chapter 601 of The Pennsylvania Code, 37 Pa. Code 601.1 et. seq. Criminal Justice Information Systems Act, as applicable, when allowing access to criminal justice information for research and statistical analysis.

Information Quality and Maintenance

A. Best Practices

Participating agencies have processes in place to ensure and periodically review the quality (accuracy, completeness, currency, and reliability) of the information they collect, maintain and share through JNET.

JNET will make every reasonable effort to ensure that information collected from participating agencies (data providers) as well as information that it collects and maintains, is derived from dependable and trustworthy sources. However, JNET makes

no warranty or representation, either express or implied, with respect to the quality, performance, merchantability or fitness for a particular purpose of the data.

B. Audits

JNET uses technologies and procedures to ensure that all of its services and systems are authorized for official purposes, that all information shared through its framework is relevant and appropriate for such authorized uses, and that safeguards are in place to actively monitor and historically record access and use of its services and systems., identifying authorized users and the nature of information exchange.

Periodic audits of the use of JNET information resources shall be conducted in order to maintain effective security, ensure privacy, and to assess ongoing operations. These audits are held every three (3) years, and are conducted by an individual (or individuals) authorized to see such information. Additionally, JNET services and systems that process or store confidential or sensitive information undergo technical security reviews to ensure compliance with implementation standards and for vulnerabilities to subsequently discovered threats. Such technical security reviews are conducted at least once a year or when the systems or services undergo major modifications.

C. Error Reporting and Error Correction

Individual JNET users are encouraged to use its User Provisioning System to correct errors with user data that is collected and stored in JNET-maintained repositories. Errors with CHRIA-protected (criminal justice) data are to be reported to the Pennsylvania State Police, who are responsible for dealing with those errors. Finally, JNET refers individuals who report errors with non-criminal justice data to the appropriate data-contributing agency.

Merging Records

JNET does not merge information about individuals.

Information Sharing

Participating agencies are encouraged to use only JNET for information sharing to ensure compliance with requirements of data privacy, security, and protection.

Information access and sharing between participating agencies through JNET is only permitted for authorized purposes, as defined by law, court order, or for business practices that are a necessary component of the requesting agency's duties and functions, and is compatible with the purpose and expectations of use under which the information was collected.

Authorized access is determined in the context of the agency's privacy policy governing the information system that is the source of the information to be exchanged. Implementation of restrictions on access within the context of JNET will be role-based.

Information exchanges brokered by JNET will identify the data source and provide descriptive labels to the information being exchanged and provided, where possible, to aid

in handling the information. At a minimum, the federated queries and subscription/notification capabilities of JNET will feature such source-based identification.

JNET will not provide bulk record dissemination. For purposes of properly authorized research and statistical analysis, such bulk dissemination must be requested from the agency or agencies which are considered the data provider.

The Privacy Policies of those agencies that regularly share information with or through JNET will be reviewed to ensure that they address the legal requirements for collection, secure storage, data quality assurance and maintenance, permissible dissemination, and removal or destruction of PII.

Information Security Safeguards

JNET has adopted policies, procedures, and practices and has implemented technology tools and physical security measures, to ensure that PII in exchanges between participating agencies and PII retained at JNET are secure from unauthorized access, use or dissemination, modification, theft, or sabotage resulting from natural disasters or human-caused intrusions. JNET adheres to the management directives, administrative rules, and Information Technology Bulletins (ITBs) listed on page 5 (above)—all dealing with various aspects of handling, storing, and disposing personally identifiable information. An example of JNET's compliance is that it encrypts all databases that contain PII with Transparent Data Encryption Technology (TDE).

JNET's data sharing partners also must confirm that they have established and implemented comparable security measures, and must agree to comply with JNET's established security policies—particularly those that establish protections for PII and criminal justice data--before requests to consume and use JNET web services are approved by JNET's Web Services Governance Team. Any agency that requests data through JNET's web services must establish a procedure for adding, maintaining and removing user accounts that uniquely identify individual users. Information acquired or received through JNET shall be used only for authorized purposes as stated within this policy, and as stated within policies established by individual data providers.

Users may not confirm the existence or nonexistence of specific records contained within JNET to persons who are ineligible to receive information. However, general information concerning data sources accessible through JNET is available on JNET's public portal.

Expectations Regarding Accountability, Enforcement and Sanctions

Although JNET also logs usage of its systems and services by users and systems, it expects that agencies that are granted authority to use its messaging and web services will also maintain computerized logs of queries performed by users under their authority. Participating agencies must also make reasonable attempts to cooperate with audits and misuse investigations performed by JNET or by another partner agency.

In accordance with the Breach of Personal Information Notification Act (73 P.S. §. 2301 et seq.) (the "Breach Act"), any agency, upon discovery of a "breach of the security of the system" (as defined by the Breach Act) which originates with that agency and is related to that agency's use of JNET and/or data accessed through JNET, shall notify JNET and all affected individuals in accordance with the Breach Act and any other applicable law.

JNET will promptly investigate incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, and data bases. An incident is defined as a violation or imminent threat of violation of privacy policies, security policies, acceptable use policies, or standard security practices.

JNET shall treat all privacy and security incidents as a misuse of JNET, whether or not the cause of the incident was accidental or intentional. As a counter measure, JNET shall implement misuse investigation procedures to: establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and, track, document, and report incidents to the appropriate agency officials and/or authorities.

JNET and participating agencies are to promptly report incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, services, and data bases to the agency sponsor, point-of-contact or JTAC. JNET users shall adhere to the *JNET Policy and Procedure: Misuse Investigation Procedures*, and *OA/OIT ITB SEC024 Information Technology Security Incident Reporting Policy*.

Details on the incident reporting structure, responsibilities and procedures are contained in the *JNET Misuse Investigation Procedures*, *PSP CLEAN AR Information Security Procedures* and *Commonwealth ITB SEC024*.

Agencies that use JNET also must ensure that users under their authority who have violated the terms of this JNET Privacy Policy are subjected to appropriate sanctions. Non-compliance with this policy by a participating agency or its authorized users may result in suspension of access to JNET or other administrative sanctions, as defined and approved by JNET's Steering Committee.