I. POLICY

This Policy is implemented in order to safeguard and protect the personally identifiable information (PII) that the County collects, stores, and transmits. This policy hereby incorporates all other applicable County policies, including but not limited to Policies 4.23, 4.24 and 4.25. Nothing herein shall be interpreted to contravene applicable State or Federal law. If there is a provision herein which conflicts with State or Federal Law the applicable State or Federal law as same may be updated from time to time shall govern.

All new major applications, general support systems, and external connections, as well as any major applications, general support systems, and external connections in development, or undergoing substantive changes, are required to undergo a security assessment by the Cumberland County Department of Information Technology to ensure adequate security controls are implemented, and risks managed to acceptable levels, prior to placement into an operational status.

II. KEY TERMS

A. Data - A subset of information in an electronic format that allows it to be stored, retrieved or transmitted.

B. Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

C. Non-Sensitive Personally Identifiable Information (PII) - is information that is available in public sources the disclosure of which cannot reasonably be expected to result in personal harm.

D. Personally Identifiable Information (PII) - any information about an individual maintained by an agency, 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.

E. Privacy – Freedom from unauthorized intrusion or disclosure of information about an individual.

F. Sensitive Personally Identifiable Information (SPII) – is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

III. GOVERNANCE AND PRIVACY

The County shall:

A. Maintain accountability for developing, implementing, and maintaining an agency privacy program to ensure compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by agency information systems;

B. Monitor State and Federal privacy laws for changes that affect the agency's privacy program;

C. Allocate resources to implement and operate the organization-wide privacy program;

D. Develop and implement privacy training and awareness aimed at ensuring users understand their privacy responsibilities;

E. Update the privacy plan, policies, and procedures, at least annually.

IV. PRIVACY IMPACT ASSESSMENT

The County shall implement a privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII. The County Chief Information Security Officer will be accountable for developing, implementing, and maintaining an agency privacy program to ensure compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by agency information systems;

A. The County shall conduct Privacy Impact Assessments (PIA) for new information systems, systems under development, systems undergoing changes or upgrades, or other activities that pose a privacy risk;

B. The County shall ensure a PIA is conducted prior to any new collection of PII, or upon significant changes in the architecture, information flow, or use of PII within existing systems;

C. The Privacy Impact Assessment shall be documented and used by the agency to identify and implement appropriate controls necessary to protect PII in accordance with all applicable State and Federal laws, regulations, and internal agency policies; and

D. The County shall determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally, or in support of a specific program or agency information system need.

V. MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION

The County shall:

A. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

B. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice, and for which the individual has provided consent;

C. As technically feasible, identify, redact, anonymize, or dispose of PII that is not necessary for the authorized purpose; and

D. Conduct periodic reviews of the agency's PII holdings to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the authorized purpose.

VI. INTERNAL USE AND DISPLAY OF PERSONALLY IDENTIFIABLE INFORMATION

The County shall:

A. Use PII internally only as authorized by law, or for the authorized purpose(s) described in the privacy notice; and

B. Mask Sensitive Personally Identifiable Information (SPII) that is displayed or printed. This includes, but is not limited to:

1. Financial account numbers;
2. Social Security Numbers (SSN); and
3. Credit or debit Primary Account Numbers (PANs) (no more than the first six (6) and last four (4) digits allowed to be displayed).

VII. PRINCIPLE OF LEAST PRIVILEGE

The County shall employ the principle of least privilege in order to limit access to personally identifiable information to only those users who have a business need and require access to carry out their duties and responsibilities.

A. Authorized individuals performing functions requiring privileged access must use designated privileged accounts only for administrative activities, and use standard user accounts for all other purposes;

B. The principle of least privilege is also to be applied to programs and processes; and

C. The principle of least privilege is extended to the display of SPII.

VIII. INFORMATION SHARING

The County shall:

A. Share PII with third parties, only as authorized by law, or for the authorized purposes identified and described in the privacy notice, or in a manner compatible with those purposes;

B. Where appropriate, enter into Information Sharing Agreements, Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, Service Level Agreements, Business Associate Agreements, or similar agreements, with third parties that specifically describe the PII covered, and specifically enumerate the purposes for which the PII may be used, and offers the same level of protection as documented in this policy;

C. Monitor, audit, and train agency staff on the authorized sharing of PII with third parties; and

D. Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new privacy notice is required.

E. Establish, maintain, and regularly update an inventory that contains a listing of all programs and agency information systems identified as collecting, using, maintaining, or sharing PII; and

F. Establish secure guidelines to transmit, collect and store PII.

IX. PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

The County shall:

A. Include privacy requirements in contracts to establish privacy roles and responsibilities for contractors and service providers;

B. Obtain commitments from vendors and other third parties that have access to PII processed by the system, to notify the agency in the event of actual or suspected unauthorized access to, or disclosures of, PII; and

C. Communicate privacy commitments and the associated system requirements to external users, as appropriate, to enable them to carry out their responsibilities.

X. PRIVACY INCIDENT RESPONSE

The County shall:

A. Respond to information security incidents involving PII consistent with the Cumberland County Cybersecurity Incident Response Plan;

B. If the incident involves the breach of personal information as defined in the New Jersey Identity Theft Prevention Act, provide timely notification to the New Jersey State Police, and others, in accordance with all applicable laws and regulations.

Guidelines: According to the New Jersey Identity Theft Prevention Act, *"Personal information means an individual's first name or first initial and last name linked with any one or more of the following data elements:*

1. *Social Security number;*
2. *Driver's license number or State identification card number; or*
3. *Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.*

Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data."

Based on the PII that may have been accessed or disclosed without authorization, agencies may have additional reporting requirements.

XI. PRIVACY AWARENESS AND TRAINING

The County shall:

A. Develop and implement privacy awareness and training aimed at ensuring users understand their privacy responsibilities; and

B. Administer basic privacy training annually, and targeted, role-based privacy training for agency users having responsibility for PII or for activities that involve PII.

XII. DATA CLASSIFICATION

The County shall classify data into various categories that helps with both protection and general usage of such data. The very purpose of a classification process is to make the data easily locatable and retrievable without needing to interrogate it again.

Below are the four classifications:

A. **Public data** - This type of data is freely accessible to the public (i.e. all employees/company personnel). It can be freely used, reused, and redistributed without repercussions. An example might be first and last names, job descriptions, or press releases.

B. **Internal-only data** - This type of data is strictly accessible to internal company personnel or internal employees who are granted access. This might include internal-only memos or other communications, business plans, etc.

C. **Confidential data** - Access to confidential data requires specific authorization and/or clearance. Types of confidential data might include Social Security numbers, cardholder data, M&A documents, and more. Usually, confidential data is protected by laws like HIPAA and the PCI DSS.

D. **Restricted data** - Restricted data includes data that, if compromised or accessed without authorization, which could lead to criminal charges and massive legal fines or cause irreparable damage to the company. Examples of restricted data might include proprietary information or research and data protected by State and federal regulations.

XIII. DATA CATEGORIZATION

The considerations listed below must be evaluated by agencies when assigning security categorizations to their information assets and determining the impact should a loss of confidentiality, integrity, availability, or privacy be realized.

A. **Legal, Regulatory, Contractual, and Policy Compliance -** Various federal and State laws, regulations, contracts and policies mandate the protection of personal information from unauthorized access, use, or disclosure.

B. **Personal Information** – New Jersey Revised Statutes §56:8-161 (2013) defines Personal Information as an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

C. **Personally Identifiable Information (PII)** - NIST Special Publication (SP) 800-121 defines PII as any information about an individual maintained by an agency, 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.

Examples of PII include but are not limited to the following:

a. Name, such as full name, maiden name, mother’s maiden name, or alias Personal identification number, such as social security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number;

b. Address information, such as street address or email address;

c. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well defined group of people;

d. Telephone numbers, including mobile, business, and personal numbers;

e. Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);

f. Information identifying personally owned property, such as vehicle registration number or title number and related information; and

g. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

D. **Sensitive Personally Identifiable Information (SPII)** - Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

E. **Criminal Justice Information -** is the term used to refer to all of the FBI Criminal Justice Information Services (CJIS) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data - data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

2. Identity History Data - textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

3. Biographic Data -information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. Property Data -information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

5. Case/Incident History - information about the history of criminal incidents.

F. **Federal Tax Information (FTI)** - FTI consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information

received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement.

FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

G. **Electronic Protected Health Information (ePHI)** – Electronic Protected Health Information (PHI) consists of any information about health status, provision of health care, or payment for health care that can be linked to an individual. PHI refers to all "individually identifiable information" held or transmitted by the County

H. Entities or its business associates in any form or media, whether paper, electronic or oral. "Individually identifiable health information" is information, including demographic data, that relates to:

1. The individual's past, present, or future physical or mental health or condition,
2. The provision of health care to the individual, or
3. The past, present, or future payment for the provision of health care to the individual,
4. The individual's identity or for which there is a reasonable basis to believe it can be used to identify the individual.

I. **Social Security Administration Provided Information** – is information that is obtained from the Social Security Administration (SSA). This can include a Social Security number verification indicator or other PII data.

J. **Payment Card Industry (PCI) Data Security Standard (DSS) Information** – PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personally identification numbers, passwords, and card expiration dates.

K. **Potential Harm to Individuals -** Agencies must consider any potential harm or adverse impact that the compromise of information may have on the parties to whom the information pertains.

L. **Agency Mission and Business Objectives -** Agencies must consider their mission and business objectives when assigning information classifications. Certain agencies may be obligated to share as much of their data as possible with the public or other outside agencies while others may be under the strictest constraints in ensuring that their data is protected against any exposure whatsoever. In either case, while it is incumbent on the agency to ensure that those objectives are met, adequate controls need to be in place and in effect to address confidentiality, integrity, availability, and privacy.

M. **Information System Dependencies/Connections and Aggregation/Commingling of Information -** Agencies must consider the risks associated with information system dependencies and connections

to other systems when classifying information. Low-sensitivity information protected by the minimum required controls in isolation must implement more restrictive controls when connected to systems containing high-sensitivity information. Information owners must consider the sensitivity of information types in the aggregate when assigning classifications. The confidentiality of an individual's first and last name is not considered High Impact information on an isolated system. When connected to, combined with, or commingled on, a system that includes other identifiers such as a social security number, the aggregate of the information requires classification as High Impact, highly sensitive and requires appropriate controls necessary to ensure the confidentiality of the information is maintained.

N. **Information Sharing Agreements, Memorandums of Understanding, and Contractual Requirement**s - Information Sharing Agreements, Memoranda of Understanding (MOU), grants, contracts, and other written agreements between agencies and external entities may include agreements regarding information access, sharing, use, disclosure and maintenance of information, as determined by the information classification of the information owner. The recipient organization's information risk classification must align with any such requirements.

   Additionally, if an agreement states that the recipient agency may further share the information, the subsequent recipients must adhere to the requirements of the original classification.

O. **Intellectual Property -** Property rights owned by an entity other than the County, when determining information risk classification assignments.

P. **Metadata** - Metadata is often referred to as "data about data". Metadata describes or supplements the information and may be either separate from or embedded within documents, records, or objects. Examples of metadata include filename, creation date, file size, author, etc. While metadata may not be readily readable, the sensitivity of the metadata alone or in combination with the information, needs to be considered.

XIV. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

For Personally Identifiable Information and Data Security related purposes, HIPAA is the Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information. When dealing with HIPAA Protected Health Information (PHI) must be taken into consideration.

A. Protected Health Information (PHI), is composed from two definitions in Section 1171 of Part C of Subtitle F of Public Law 104-191 (August 21, 1996): Health Insurance Portability and Accountability Act of 1996: Administrative Simplification. These statutory definitions are of health information and individually identifiable health information.

1. **Health information** means any information, whether oral or recorded in any form or medium, that:

   a. is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

   b. relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

2. **Individually Identifiable Health Information** is information that is a subset of health information, including demographic information collected from an individual, and:

   a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

   b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

   c. That identifies the individual; or

   d. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

3. **Protected Health Information means individually identifiable health information [defined above]:**

   a. Except as provided in number (b) of this definition, that is:

      1. Transmitted by electronic media;

      2. Maintained in electronic media; or

      3. Transmitted or maintained in any other form or medium.

b. Protected health information excludes individually identifiable health information in:

1. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
2. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
3. Employment records held by a covered entity in its role as employer.

B. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

C. When dealing with HIPAA, County employees must follow the guidelines as set forth in the Health Insurance Portability and Accountability Act of 1996.