SAMPLE DATA SECURITY INCIDENT PROTOCOL:
WHAT TO DO IN THE EVENT OF AN UNAUTHORIZED DISCLOSURE AND BREACH PREVENTION MEASURES

The purpose of this protocol is to provide guidance to program areas on how to manage and respond to a data security incident. Not all unauthorized disclosures constitute a legal breach of data security. Whether a disclosure constitutes a breach is subject to multiple statutory and regulatory legal definitions and is dependent of the type of information disclosed. The determination of whether a data breach occurred is made by the Data Privacy Officer in consultation with executive and program staff.

It is important to refrain from referring to such incidents as breaches in your oral and written communications until you receive confirmation from the Data Privacy Officer and the Office of Legal Affairs that an actual data breach has occurred. It is important to refer to such situations as data security incidents until the scope of the facts can be properly assessed. The Data Privacy Officer must be notified immediately upon discovery of an actual or suspected unauthorized disclosure so that appropriate steps may be taken.

The Data Security Incident Protocol will:

- Provide examples of what constitutes a data security incident;
- What constitutes a data security breach;
- Provide guidance on what steps need to be taken when there is a reason to believe that a data security incident has occurred;
- Provide guidance on what steps program needs to take to mitigate any harm that is a direct result of a data breach;
- Explain the requirements for breach notification;
- Provide guidance on breach prevention.

It is important to notify the Data Security Officer s immediately upon learning of the incident to determine an appropriate corrective action plan, if necessary and to ensure that such a plan is timely implemented.

Examples of possible data security incidents include, but are not limited to:

- Loss or Theft of Agency Equipment. Agency equipment includes blackberries, cell phones, cds, thumb drives, portable devices, desktop computers, laptops, photo copiers, fax machines;
- Loss, theft or improper disposal of hard copy documents that contain confidential and individually identifiable information. Individually identifiable information may relate to employees and clients;
- Misdirection of emails and faxes that contain confidential information that are sent to unintended parties of;
- Suspected instances of computer hacking or social engineering;
- The disclosure of confidential information to the internet or any social media sites;
- Unauthorized copying of confidential Agency information to personal electronic devices, such as routers, thumb drives, etc.;
- Improper disposal of Agency equipment.

**Types of Confidential Information**

The following are examples of the types of confidential information, that if disclosed without legal authorization may result in a data security incident. Please not that this not an exhaustive list:

- SSNs
- Client Names
- Client Addresses
- Client Case numbers
- Benefit Information
- Benefit Coverage dates
- Substance Abuse Treatment Records
- Records pertaining to Domestic Violence
- Protected health information maintained by the Medicaid program
- Medical/mental health information
- Office of Child Support Enforcement Records
- Adult Protective Services Records
- SDX data
- Supplemental Nutrition Assistance Program benefits
- Cash assistance Benefits
- Medicaid Records
- Reasonably identifiable HIV-AIDS related information

**Sometimes when determining whether a breach occurred, more than one statute and/regulation must be consulted, depending on the type of data that was disclosed.** Below some examples of relevant underlying statutes/regulation.

a) **HITECH**

b) **HIPAA**

c) **NYC Administrative Code**

**What Constitutes a Data Breach**

Different types of confidential information are subject to different statutory and regulatory disclosure restrictions. Certain conditions must be met to determine if a data breach occurred.

The Data Privacy Officer will review the facts connected with the disclosure and will determine whether the incident meets the legal definition of a data breach.

Determining what constitutes a breach is decided on a case-by-case basis and requires an
comprehensive analysis of the facts surrounding the incident.

Different statutes have different definitions of what constitutes a data breach. For example, the New York City Administrative Code, 10-501(a) provides the following definitions:

i) “Personal identifying information”
   (1) Shall mean any person’s date of birth, social security number, diver’s license number, non-driver photo id card number, financial services account number or code, saving account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother’s maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person. This term shall apply to all such data, notwithstanding the method by which such information is maintained

ii) “Breach of security”
   (1) Shall mean the unauthorized disclosure or use by an employee or agent of an agency, or the unauthorized possession by someone other than an employee or agent of an agency, of personal identifying information that compromises the security, confidentiality or integrity of such information. Good faith or inadvertent possession of any personal identifying information by an employee or agent of an agency for the legitimate purposes of the agency, and good faith or legally mandated disclosure of any personal identifying information by an employee or agency of an agency for the legitimate purposes of the agency shall not constitute a breach of security.

Definition of Breach under the HIPAA Omnibus Rule

The impermissible use or disclosure of Protected Health Information is considered a violation of the HIPAA Privacy Rule. Such a disclosure is presumed to be a breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that Protected Health Information Has been compromised.

The Interim Final Rule analysis, which included a subjective “Risk of Harm” analysis when Determining whether a breach has occurred, has been removed and replaced with a more objective “Risk Assessment” approach. This means that under the Final Rule, breach notification is not Required if the Covered entity can demonstrate that there is a low probability that the Protected Health Information has been compromised. The Covered Entity is no longer required to demonstrate that there is no significant risk of harm to the individual, as was required under the Interim Final Rule.
When conducting a Risk Assessment, The Data Privacy Officer will consider the following factors:

1. The Nature and Extent of the Protected Health Information Involved
2. The types of identifiers disclosed
3. The likelihood of re-identification
4. The un-authorized person who used the Protected Health Information or to whom the protected health information was disclosed
5. Whether the Protected Health Information was actually acquired or viewed
6. The extent to which the risk of the Protected Health Information has been mitigated.

The Covered Entity is only required to engage in this risk assessment when the Covered Entity wants to demonstrate that notification is not required. If it is clear from the facts that a breach occurred, then the Covered Entity may take immediate steps to provide notification of the breach to the appropriate parties.

Examples of Possible Data Breaches
- Taking a file on the train or bus and inadvertently leaving it on a seat or dropping it.
- Improper disposal of sensitive records, accidentally throwing out a cd or thumb-drive.
- A computer virus has compromised your terminal making you vulnerable to hackers.
- An employee took confidential files home (whether authorized or not) and they were accessed by a third party.
- Accidental e-mail, fax, or postal dispatch to the wrong person.

1) DETECTION—What Steps Must Be Taken Upon Discovery of an Unauthorized Disclosure?

a) DOCUMENTATION

i) Making a report

When there is reason to believe that a data incident has occurred, the first step is to Notify the Data Privacy Officer or the person within your organization responsible for investigating data security incidents. You will be asked to complete an incident report. A blank copy of the Data Security Incident Form is attached to this Protocol as Appendix “A.” The form shall be completed by the manager or supervisor for the unit upon consultation with all parties apprised of the facts and shall include a description of the chronological sequence of events. Consultation may also require discussions with your organization’s IT team.
If an incident is believed to have affected more than one program area, each program area affected should be consulted. Depending on the nature of the incident, more than one form may need to be completed, however, most incidents will only necessitate the completion of one incident form, even if the incident extends across multiple program areas.

The form asks about the nature of the incident—how the disclosure was discovered, the type of information disclosed, the number of records involved and the number of individuals affected.

At first, you may not have all the information the form asks you to complete. The program area may have to conduct interviews with involved parties during the fact gathering process.

b) REPORTING
   i) Who to report to?
      (1) When an unauthorized disclosure has been discovered, the program should inform the Data Privacy Officer of the incident and complete the Data Security Incident Form.
      (2) One of them will be assigned to your incident and guide you through whether you need to disclose to affected parties, the NYPD, or other authorities.
      (3) If the data breached was protected health information, The Secretary of Health and Human Services must be notified in accordance with HIPAA.
      (4) If more data was protected health information and more than 500 individuals were affected, you are also required to notify the media.

2) RISK ASSESSMENT

Depending on the sensitivity of the information, the risk of a data breach may be deemed high or low. A risk assessment will be conducted to determine what the appropriate corrective action shall be.

Mitigation of Harm

Once a breach is discovered certain steps must be taken to mitigate the harm. Examples of such steps include:

- Taking precautionary measures to ensure that electronic and physical information is secured.
- Investigate whether it is possible to recover the information that information that was disclosed.
- Require that un-intended recipients provide written assurances that they will not re-disclose the data to third parties.
- Train employees about the importance of protecting confidential information and the restrictions on disclosure.
- Develop policies and procedures that provide staff with guidance on what administrative and physical safeguards must be adopted to protect confidential information.
• Notify all affected individuals who are subject to a data breach. Individuals must be informed of what happened, what steps the Agency has taken to mitigate the harm and the individual shall be provided with instructions on how to protect themselves from further harm, i.e. information about credit reporting services.

3) ESCALATION
   a) Who else needs to know?
      i) Based on the risk assessment, the Data Privacy Officer will decide who else needs to be made aware of the suspected unauthorized disclosure.
      ii) It is important to note that in some instances, the data breach may not belong to the party responsible for the disclosure. In those instances, the owner of the data must be notified so that investigation efforts may be coordinated.
      iii) People involved in the detection of the disclosure or who are responsible for the incident should expect to fill out the Form and may be questioned by other authorities, depending on the situation.

4) BREACH NOTIFICATION

Questions to keep in mind:

   a) Do the affected parties need to be notified?
   b) What manner of notification is sufficient to satisfy statutory burden?

Different types of information are subject to different breach notification requirements. The HIPAA Breach Notification Rule applies when Protected Health Information has been compromised.

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule did not exist before HITECH. Section 13402 of the HITECH Act requires a Covered Entity to provide notification to affected individuals and to the Secretary of HHS following a discovery of a breach of unsecured Protected Health Information. If the breach affected more than 500 individuals, notification of the breach to the media is also required. Under 45 C.F.R. 164.408(c) Covered Entities must provide notification to the HHS Secretary and affected individual no later than 60 days after the end of the calendar year in which the breaches were discovered, not when the breaches occurred.

If the breach was caused by a Business Associate, the rule also requires the Business Associate to notify the Covered Entity.

5) BREACH PREVENTION

Below are some examples of breach prevention measures

• Organizations should employ a Data Privacy Officer and a Data Security Officer
• Staff should receive routine training on confidentiality
• Safeguard measures should be implemented to protect electronic and physical data.
• Staff should adopt the “minimum necessary” standard regarding data access.
• Organizations should implement policies and procedures that govern the protection of confidential data and provide guidance on the proper disposal of physical data and equipment that contains confidential data.
• Organizations should be aware that data privacy issues require both legal and technical expertise.
• Organizations should enter into Memoranda of Understanding (MOUS) and Data Sharing Agreements, and/or Business Associate agreements prior to the disclosure of confidential information and or protected health information with third parties.