DSS Policy Bulletin #2022-001
Date: February 8, 2022

DISTRIBUTION: *ALL STAFF, CONTRACTORS AND SUBCONTRACTOS*

CONFIDENTIALITY AND DATA PROTECTION POLICY FOR DSS-HRA-DHS CONTRACTORS AND SUBCONTRACTORS

Table of Contents

I. INTRODUCTION 1
II. OVERVIEW 2
III. OWNERSHIP OF CONFIDENTIAL DATA 2
IV. DEFINITIONS 3
V. ROUTINE COLLECTIONS AND DISCLOSURES 4
VI. DATA INVOLVING HEIGHTENED EXERCISE OF CARE 5
VII. CIVIL LIABILITY, CRIMINAL PROSECUTION AND CONTRACT TERMINATION..5
VIII. DATA SECURITY INCIDENT AND REPORTING REQUIREMENTS 6

I. INTRODUCTION

This confidentiality policy is directed to all New York City Department of Social Services (DSS), Human Resources Administration (HRA) and Department of Homeless Services (DHS) contractors, vendors, contracted providers and subcontractors, hereinafter referred to as “contractors.” The purpose of this policy is to inform all contractors of their obligations and responsibilities pertaining to the collection, retention and disclosure of confidential information obtained by or on behalf of the City of New York, as well as information provided by the City to contractors. These requirements apply to all forms of collection and disclosure, including but not limited to paper and electronic forms and oral communications, and to all devices, applications, systems, and files which contain confidential information.

Contractors should be aware that DSS-HRA-DHS program areas may also have additional confidentiality policies and procedures which are applicable to contractors and which may be more specifically tailored to the needs of each program area. The purpose of this policy is to supplement any existing confidentiality policies or procedures that apply to contractors and it should be noted that this policy does not replace or render any existing policies or agreements obsolete. Contractors should be aware of their responsibilities and obligations under all DSS-HRA-DHS confidentiality policies and procedures. Contractors should also ensure that all of their employees, subcontractors, agents, and volunteers comply with the information security standards and requirements set forth by the New York City Department of Information Technology and Telecommunications and the New York City Cyber Command and the Citywide Privacy Protection Policies and Protocols established by the New York City Chief Privacy Officer.

In accordance with this policy, Contractors agree to use and ensure the use of appropriate safeguards to prevent misuse or unauthorized disclosure of the data. Contractors are required to implement administrative, physical, and technical safeguards consistent with industry standards that reasonably and appropriately protect and secure the confidentiality, integrity, and availability of any electronic or hard copy individually identifiable information that is created, received, maintained, uploaded, exchanged or transmitted.

II. OVERVIEW

The collection, retention, use and disclosure of confidential information should be consistent with and limited to the terms provided under the City contracts, and in accordance with all applicable local, state, and federal statutes and regulations and any attached Identifying Information Law Riders. At no time during or after the term of the contract, shall contractors use Agency confidential information for the benefit of itself or any third party in any manner inconsistent with the terms and conditions of any contract or data sharing agreement.

III. OWNERSHIP OF CONFIDENTIAL DATA

In general, confidential information provided to any contractor by the Agency for purposes of the performance of services on behalf of the Agency shall remain the exclusive property of New York City, with the exception of confidential information obtained by contractors from clients in the course of providing contracted legal services to such clients. Unless otherwise specified under the terms of their contracts, confidential information provided by the Agency to contractors and maintained in connection with contractor services are owned by the City and no right, title, or interest in any material developed therefrom is transferred to the contractor.

IV. DEFINITIONS

A. "Record" means any paper or electronic file or document which contains Confidential Information.

B. “Confidential information” means any information that is private, or not for public dissemination. For purposes of this policy, information is considered confidential when a federal, state, or local law or regulation, or directive, memorandum, judicial decree, order, stipulation, settlement, or some type of pre-existing agreement deems it confidential. Most Agency records and all client records are confidential.

C. “Employee” means any person employed by a contractor or subcontractor whether employed full time, part time or on a temporary or seasonal basis, as well as any officers, representatives, consultants, researchers, agents or any other person or entity given access to Agency confidential or identifying information.

D. “Identifying information” means any information obtained by or on behalf of the City that may be used on its own, or with other information, to identify or locate an individual. Note that information from various or seemingly unrelated sources that may not have been identifiable or specific on its own may rise to the level of “identifying” when combined with other available information. Examples of identifying information include: name, full or partial social security number, photographs, current or previous home address, gender identity, citizenship or immigration status, employment status, eligibility for or receipt of public assistance, scheduled appointment times, location and internet protocol address.

E. “Identifying Information Law” shall refer to the New York City Local Laws 245 and 247 which set forth new requirements concerning the collection, retention, and disclosure of identifying information by City agencies and health and human services contractors, technology services contracts and certain types of outreach contracts. The Citywide Privacy Officer has the authority to expand the applicability of the Identifying Information Law to other types of contractors over time.

F. “Health and Human services” means any services provided to third parties, including social services such as day care, foster care, home care, homeless assistance, housing and shelter assistance, preventive services, youth services, and senior centers; health or medical services including those provided by health maintenance organizations; legal services; employment assistance services, vocational and educational programs; and recreation programs.

G. “Technology Services Contracts” means contracts and subcontracts for technology services involving sensitive identifying information collected by the contractor or subcontractor on behalf of the City. Such contractors and subcontractors collect, access, store, process, analyze, transmit, or otherwise handle sensitive identifying information, even if access to sensitive information is not the express purpose of the contract.

H. “Outreach services” means certain contracts and subcontracts for outreach services services involving identifying information. These are contracts or subcontracts where the contractor or subcontractor collects, uses, or discloses identifying information (except for routine business contact information) on behalf of the City for projects designed to help clients of other City agencies or offices (or members of the public) access information about City services, resources, or events through any means. This designation does not include agency contracts with a vendor to perform outreach services to the agency’s own clients.

I. “Data security incident” refers to the suspected or actual disclosure of any confidential information to a third party without authorization, whether the disclosure is intentional or accidental, or when confidential information is used, acquired, or accessed for improper purposes.

V. ROUTINE COLLECTIONS AND DISCLOSURES

The Identifying Information Law which applies to health and human services contractors, technology services contracts and certain outreach services contracts required each City agency to appoint an Agency Privacy Officer charged with assessing compliance and designating certain types of collections and disclosures of identifying information as “routine”. Disclosures for functions or purposes designated as routine generally do not require further approval from the DSS Agency Privacy Officer (APO) prior to the disclosure of identifying information. The DSS APO has designated a number of routine collections and disclosures, for example, responding to subpoenas, court orders, audits, and program eligibility determinations.

It is the Contractor’s responsibility to review the APO’s routine designations to ensure that all collections and disclosures of identifying information are made in accordance with the APO’s prior approval. Please note that the APO’s designations were made with current Agency and contractor operations in mind. If legal review was required for a particular disclosure prior to enactment of the law, such review is still required.

Except under emergency circumstances, Contractors must seek approval from the APO prior to any collection, retention, use or disclosure of identifying information for any purpose that has not been designated as routine or is outside of the scope of their respective agreements. Collections or disclosures of any identifying information that have not been designated as routine must be approved by the DSS APO on a case-by-case basis. If a collection or disclosure is made under emergency circumstances, this should be reported to the DSS APO using the contact information at the bottom of this communication.

Additionally, contractors must fully cooperate with audits and investigations to the extent permitted by law when formal requests for confidential information are made for these purposes. If confidential information is sought from Contractors by subpoena, court order or FOIL request, Contractors shall consult with the DSS Office Legal Affairs prior to the disclosure and unless legally prohibited from doing so, provide reasonable written notice and a copy of the request to DSS Office of Legal Affairs. No Confidential Information may be disclosed without authorization from the DSS Office of Legal Affairs unless such disclosure is required by law.

VI. DATA INVOLVING HEIGHTENED EXERCISE OF CARE

Contractors should be aware that there should be a heightened exercise of care when collecting, using, and disclosing certain types of highly sensitive confidential data as required under applicable local, state, and federal statutes and regulations. There are certain types of confidential information that would pose a higher risk of harm to clients if improperly disclosed. Examples of such data include but are not limited to individually identifiable protected health information under the Health Insurance Portability and Accountability Act (HIPAA), HIV-AIDS status information under Article 27-F of the NYS Public Health Law, Domestic Violence status and Domestic Violence address information under VAWA 34 USC § 12291(b)(2) and NY Social Services Law § 459-h, drug and alcohol use information under 42 U.S.C.§290dd-2 and mental health status information under the NYS Mental Hygiene Law §33.13. Contractors are responsible for complying with all applicable local, state and federal law that govern the use and disclosure of confidential information.

Contractors whose services require receiving and maintaining Protected Health Information from the HRA covered entity which administers the Medicaid program must also enter into business associate agreements with the covered entity, in addition to their underlying agreements. The HIPAA Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associates that the business associates will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. Please note that business associates are required to report security and privacy breaches to the covered entity under 45 CFR § 164.410.

VII. CIVIL LIABILITY, CRIMINAL PROSECUTION AND CONTRACT TERMINATION

Any unauthorized access to, or disclosure of confidential information may result in civil liability, monetary civil penalties, a private lawsuit, or a criminal prosecution. Contractors should not access any active, closed or archived case record, including, but not limited to the record of a relative, acquaintance, neighbor, friend, partner, co-worker, themselves or any other individual, except in the performance of official job duties and for authorized purposes, utilizing approved processes for such access and in accordance with federal and state laws, rules, regulations, policies and agreements. Please be advised that a contract may be terminated as a result of an incident involving the unauthorized disclosure of HRA-DSS-DHS data.

VIII. DATA SECURITY INCIDENT AND REPORTING REQUIREMENTS

Data security incidents have the potential to cause harm to clients, including but not limited to financial, physical, emotional, and reputational harm. There is also a risk of reputational harm and financial liability to DSS-HRA-DHS and the City. It is important for Contractors to be aware of these risks and also be able to recognize and identify a data security incident. Examples of data security incidents may include but are not limited to:

- unauthorized access to identifying information
- disclosure of identifying information to unauthorized third parties
- loss (even temporary) or inadvertent disclosure or release of identifying information except during exigent (emergency) circumstances, collecting, retaining, or disclosing identifying information without prior routine or case-by-case approval of the Agency Privacy Officer.
- Loss, theft or improper disposal of equipment, including work-issued cell phones, CDs, thumb drives, portable devices, desktop computers, laptops, photocopiers, fax machines.
- Loss, theft, or improper disposal of hard copy documents that contain confidential and personally identifiable information.
- Misdirection of emails, mails/correspondence and faxes containing confidential information that are sent to unintended parties.
- Suspected or actual instances of computer hacking, ransomware, and phishing attacks.
  Examples of phishing attacks include situations where threat actors disguise themselves as a trusted entity to dupe individuals into opening suspicious emails or trick them into clicking on a malicious link in an attempt to gain privileged access, steal user data such as login credentials and financial information and/or install malware which can result in the freezing of the system.
- Release of confidential information in response to a fraudulent email or telephone call.
- 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, and other non-secure environments without prior authorization from DSS-HRA-DHS. etc.

Contractors shall fully cooperate with DSS-HRA-DHS regarding any investigations related to the unauthorized disclosure of confidential data.

Contractors shall immediately report to the Agency the discovery of any unauthorized use or disclosure of confidential information directly to security@dss.nyc.gov and cooperate with additional information requests.

Effective Immediately