



Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

| | |
|---|--|
| New York State Information Technology Policy | No: NYS-P10-004 |
| IT Policy: Guidance for the Use of SSNs by State Government Entities | Updated: 10/02/2020 |
| | Issued By: NYS Office of Information Technology Services Owner: Division of Legal Affairs |

1.0 Purpose and Benefits

Social Security numbers (SSNs) are highly sensitive personal identifying information. SSNs are commonly used in identity theft and fraud. Changes to the New York State Labor Law and Public Officers Law in 2009 and 2010 implemented controls on the collection and transmission of SSNs by the State and its political subdivisions. These changes to the Labor Law and Public Officers Law reduce the potential for SSNs from being subject to unauthorized disclosure.

Since 1983, the New York State Personal Privacy Protection Law (PPPL), codified in Article 6-A of the Public Officers Law, has required State agencies to maintain in their records only the personal information relevant and necessary to accomplish a purpose of such agencies: (1) as required to be accomplished by statute or executive order, or (2) as required to implement a program specifically authorized by law. Further, the PPPL obligates agencies to ensure the integrity and security of personal information maintained in their records. Chapter 279 of the Laws of 2008 amended the PPPL and the Labor Law to extend to public entities certain prohibitions already applicable to commercial entities and to establish specific requirements applicable for the use and transmission of SSNs. More specifically, Chapter 279 added Section 96-a of the Public Officers Law and Section 203-d of the Labor Law.

This policy describes these requirements as they are applicable to State government entities, providing guidance to ensure that the deployment of technology in government is coordinated with consistent approaches for compliance. This guidance was originally issued by the Office of Information Technology Services (ITS) after consultation with the former New York State Consumer Protection Board, the New York State Department of Labor, and the former New York State Office of Cyber Security and Critical

Infrastructure Coordination (now a part of ITS). These agencies, or their successors, have certain responsibilities concerning the privacy and security of personal identifying information, such as SSNs, used by State government entities. Per statute, an employer's failure to establish policies or procedures to safeguard against privacy breaches may be presumptive evidence of a violation. State government entities may wish to adopt agency level policies not inconsistent with these guidelines to avoid allegations of breach and imposition of authorized penalties.

2.0 Authority

Chapter 279 of the Laws of 2008 contained changes to the New York State Labor Law which went into effect on January 3, 2009, and changes to the New York State Public Officers Law, Article 6-A (Personal Privacy Protection Law), which went into effect January 1, 2010, governing the use of SSNs by state agencies and political subdivisions. Many of these changes concern the use of SSNs in technology systems, including the Internet, websites, and electronic mail.

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. Section 2 of Executive Order No. 117 provides the State Chief Information Officer the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security, and business re-engineering. Details regarding this authority can be found in [NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines](#).

3.0 Scope

This guideline applies to all "State Government" entities as defined in Executive Order 117 or "State Agencies" as defined in Section 101 of the State Technology Law ("State Entities" or "SE"), their employees, and all others, including third parties (such as local governments, consultants, vendors, and contractors), that use or access any ITS Information Technology Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. This guideline also applies to SE "technology" "systems," as defined in the [NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary](#).

4.0 Information Statement

NYS LABOR LAW SECTION 203-d

Section 203-d of the NYS Labor Law, effective January 3, 2009, prohibits all New York State employers, including the State in its capacity as an employer, from:

- Unless required by law:
 - Publicly posting or displaying an employee’s SSN;
 - Visibly printing a SSN on any identification badge or card, including a timecard;
 - Placing a SSN in files with unrestricted access; or
 - Communicating an employee’s “personal identifying information” to the general public. “Personal identifying information” means any of the following elements alone or in combination with other elements: an employee’s home address or telephone number, personal electronic mail address, Internet identification name or password, parent’s surname prior to marriage, drivers’ license number, or SSN; or
- Using a SSN as an identification number for purposes of any occupational licensing.¹

Labor Law Section 203-d: (i) states it shall be presumptive evidence of a knowing legal violation of this section if an employer has not put into place policies or procedures to safeguard against such violations, including provisions to notify employees; and (ii) provides the Commissioner of Labor authority to impose monetary civil penalties for such knowing violations.

Accordingly, SEs should have policies in place to comply with the requirements of section 203-d. These policies should include:

- an outline of the prohibitions of section 203-d; and
- procedures instituted by the SE to safeguard against unlawful disclosure, including as applicable notice to and training of its workforce.

To the extent a SE is using technology systems to accomplish any of the purposes described above (e.g. using the entity’s employees’ SSNs as identification numbers in its technology systems) it should modify its IT systems to comply with these requirements.

NYS PPPL SECTION 96-a

1. **Section 96-a of the PPPL**, effective January 1, 2010 (hereinafter “Section 96-a”), extends the prohibitions of Section 399-dd of the General Business Law to the context of the State and its political subdivisions (hereinafter “the State”). These restrictions fall into two main groups: (a) prohibitions against what the State can do; and (b) limitations on what the State can require individuals to do.

Section 96-a defines a “social security account number” to “include the nine-digit account number issued by the federal social security administration and any number derived therefrom” but not “any number that has been encrypted.” Under Section 96-a: **Unless required by law, the State shall not:**

¹ A State Government entity should consult with its Counsel’s Office concerning the requirements of section 203-d of the Labor Law and its applicability to its specific circumstances.

- Intentionally communicate to the general public or otherwise make available to the general public in any manner an individual's social security account number.
- Print an individual's social security account number on any card or tag required for the individual to access products, services, or benefits provided by the state and its political subdivisions.
- Include an individual's social security account number, except for the last four digits, on any materials that are mailed to the individual, or in any electronic mail that is copied to third parties, unless:
 - state or federal law requires the social security account number to be on the document to be mailed; or
 - the State chooses to include the social security account number in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security account number (but social security account numbers permitted to be mailed under this exception may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened).
- Encode or embed a SSN in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the SSN.

Unless required by law, the State shall not require an individual to:

- Transmit the individual's social security account number over the Internet unless the connection is secure or the social security account number is encrypted; or
- Use the individual's social security account number to access an Internet website, unless a password or unique personal identification number (PIN) or other authentication device is also required to access the Internet website. Such passwords and PINS should be unique to the individual and based on information which is private and not generally available to others.²

2. Concerning NYS PPPL section 96-a, all SEs should:

- a. Make checklists concerning their use of social security account numbers and SSNs and consult with their attorneys to confirm they are in compliance with the law.

² The statute contains limited exceptions for the collection, use, or release of SSNs for fraud investigations, internal verification or other administrative purposes. The existence of these exceptions does not obviate the State government entity's obligation to otherwise ensure the security and integrity of SSNs. A State government entity should consult with its Counsel's Office concerning the requirements of section 96-a and their applicability to its specific circumstances.

b. Review the guidance below which was developed to assist SEs to comply with the law.

c. With regard to documents:

i. **Make a list of all the documents which the SE provides to individuals**, such as employees or members of the public, which show or contain an individual's SSN. These can include cards, tags, letters or forms where the SSN appears on the face of the document and cards or documents where the SSN is embedded or encoded in or on the item.

ii. **Divide this list into two types of documents**, i.e., those which are sent by postal or electronic mail for the individual's personal review only, and those which are intended for public use (e.g., a badge).

iii. **For documents intended for the individual's personal review only:**

- SEs may only use the full SSN:
 - if required by state or federal law, or
 - in applications or forms sent by mail that include documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the SSN

--but--

- for either of the above, only if no portion of the SSN is printed on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.
- Otherwise, SEs may only use the last four digits of the SSN, refraining from doing even that when possible.

--and--

- unless required by state or federal law, not intentionally communicate or otherwise make available to any third party an individual's SSN.

iv. **For documents intended for public use**, SEs should not use any printed SSNs either in part or in full.

SEs should not, unless required by law, require individuals to choose their SSN as an account ID for the purposes of identification on printed communications.

d. With regard to e-mail:

- i. SEs may not include full SSNs in any electronic mail (including in any attached documents) that is copied to third parties, unless state or federal law requires it.
- ii. Otherwise, SEs may only use the last four digits of the SSN, refraining from doing even that when possible.

e. With regard to Internet communications:

- i. Make a list of all Internet-related communications where the SE requires an individual to transmit his/her full SSN over the Internet in order to register for or file a claim for benefits or services, or where an individual is required to use his/her SSN to access the SE's Internet website.

- ii. **Divide this list into two types of communications**, i.e., SSN form submissions and SSNs used for website access.

iii. **For these types of communications:**

- For both types of communications, unless required to do so by law, SEs are not permitted to require the transmission of the SSN unless the transmission is via a secure (i.e., https) connection or the SSN is encrypted.
- Unless required to do so by law, a SE is not permitted to require SSNs to be used to access internet websites unless a password, unique personal identifier, or other authentication device is also required. In those cases, in which SSNs are currently used for this purpose, a SE must:
 - implement multi-factor authentication requiring a password, unique personal identifier, or other authentication device (e.g., a token) to establish the unique identity of the user; or
 - provide users with a means of changing their user IDs from an SSN to an identifier that will not identify them personally and is not derived from the SSN. This notice could be provided to all current users of the SE's services in the next general postal or online mailing. For prospective users of the SE's services, any registration screen that asks for the creation of a user ID should contain a prominent disclaimer warning the individual to exercise care in the selection of a user ID with language such as "*Choose an alias to protect your identity. Do not choose any information that identifies you personally (e.g., a Social Security number).*"

Note that the NYS PPPL does not prevent the collection, use or release of a social security account number as required by state or federal law, or the use of a social security account number for internal verification, fraud investigation or administrative purposes.

A worksheet is attached to the end of this policy to further assist SEs complying with these laws. See Attachment A.

5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

| Term | Definition |
|--------------------------------|---|
| State Government Entity | shall have the same meaning as defined in Executive Order No. 117, first referenced above, and shall include all state agencies, departments, offices, divisions, boards, bureaus, commissions and other entities over which the Governor has executive power and the State University of New York and City University of New York; provided, however, that universities shall be included within this definition to the extent of business and administrative functions of such universities common to State government. |

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Division of Legal Affairs
Reference: NYS-P10-004
NYS Office of Information Technology Services
State Capitol, PO Box 2062
Albany, NY 12220-0062
Telephone: (518) 473-5115
Email: its.sm.dla@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: <http://www.its.ny.gov/tables/technologypolicyindex>

8.0 Revision History

This policy shall be reviewed at least once every two years to ensure relevancy.

| Date | Description of Change | Reviewer |
|-------------|---|---------------------------|
| 07/07/2010 | Original Policy Release | CIO/OFT |
| 07/07/2012 | Scheduled Policy Review | CIO/OFT |
| 09/12/2012 | Reformatted and updated to reflect current CIO, agency name, logo and style. | CIO/OFT |
| 12/20/2013 | Revised to update language and outdated links, after reviewing current status of the law. | ITS-DLA |
| 12/20/2014 | Scheduled Review | ITS-DLA |
| 06/28/2017 | Reformatted logo and style. Updated language after review. | ITS-DLA |
| 10/02/2020 | Minor grammatical changes. | Division of Legal Affairs |

9.0 Related Documents

ATTACHMENT A: Worksheet

Under provisions of section 96-a of the Personal Privacy Protection Law, Public Officers Law, Article 6-A (the "PPPL"), as amended by chapter 279 of the Laws of 2008 and effective January 1, 2010, state agencies and political subdivisions were subject to new restrictions on the collection and use of Social Security numbers (SSNs). This Worksheet is intended to assist state agencies in complying with the PPPL. Instructions and examples of responses are provided below. The Worksheet is suggestive only and does not constitute legal advice.

Q. 1 HOW AND WHY DOES MY AGENCY COLLECT SSNs?

| Identified instance in which SSNs are collected | In which formats are the SSNs collected? | What agency purpose is served by collecting SSNs in this instance? | What is the legal authority for collecting SSNs in this instance? | How are these SSNs transmitted? ³ | Are changes needed to comply with §96-a? | Timetable for indicated changes |
|--|---|---|--|---|--|---|
| <p>Instructions: Using a new row for each entry, identify an instance in which the agency collects SSNs from individuals.</p> | <p>Instructions: For each instance identified in the first column, identify the format for the collection, of SSNs e.g., application forms [web and/or paper], claim forms [web and/or paper], website access.</p> | <p>Instructions: For each instance identified in the first column, explain what agency purpose is served by collecting SSNs from individuals.</p> | <p>Instructions: For each instance identified in first column, identify the legal authority for the collection of SSNs. If the legal authority is Section 96-a (1) (e) of the PPPL, confirm that the instance in first column is a form or application.</p> | <p>Instructions: For each instance identified in first column, identify the manner of transmission (e.g., by web transmission; or by fax to an agency fax machine).</p> | <p>Instructions: For each specific format identified in first column, identify the necessary remediation.</p> | <p>Instructions: For each specific format identified in first column, identify target completion date and any milestone dates.</p> |
| <p>Example #1: On applications for agency benefits or services.</p> | <p>Example #1: On applications for agency benefits or services (web and paper).</p> | <p>Example #1: For personal identification and for tax calculation and reporting. State government entity needs to collect and maintain SSN in agency file for these purposes.</p> | <p>Example #1: Federal or NYS tax law; NYS Personal Privacy Protection Law (especially the "relevant and necessary" provisions).</p> | <p>Example #1: Web application form transmitted through non-secure (i.e., non-https) connection.</p> | <p>Example #1: Change page to https.</p> | <p>Example #1: Change completed by law's effective date of January 1, 2010, or as reasonably soon as possible thereafter.</p> |
| <p>Example #2: Used as an identifier for</p> | <p>Example #2:</p> | <p>Example #2: For personal identification</p> | <p>Example #2: Well-intentioned</p> | <p>Example #2: Web page transmitted</p> | <p>Example #2: Connection change same as Example #1.</p> | <p>Example #2: Connection change same</p> |

³ The changes in SSN law address transmission of SSNs. State government entities should also review and confirm with their legal counsel whether the manner in which they maintain SSNs complies with the PPPL.

| Identified instance in which SSNs are collected | In which formats are the SSNs collected? | What agency purpose is served by collecting SSNs in this instance? | What is the legal authority for collecting SSNs in this instance? | How are these SSNs transmitted? ³ | Are changes needed to comply with §96-a? | Timetable for indicated changes |
|---|--|--|---|--|--|--|
| logging in to a website. | Login credentials on website. | and to authenticate the individual's identity for web access. | but ill-advised effort to comply with laws requiring virtual access security. | through non-secure (i.e., non-https) connection. Also, authentication by one-factor, public information (i.e., SSN by itself). | Authentication change requires either non-SSN authenticator or SSN with password or other unique personal identifier. | as Example #1. Page re-design for authentication change by (milestone and completion dates). |
| Example #3: On forms and paperwork for patient admission. | Example #3: On patients admission paperwork (printable, but sent via email). | Example #3: To confirm identity of patient and for patient billing purposes. | Example #3: POL § 96-a (1)(e). Forms. | Example #3: Secured electronic mail. | Example #3: No. Agency created form for accurate identification and billing purposes. SSN sent internally through secure e-mail. System access on need to know basis- limited to Medical, Admissions/Discharge billing staff only. | Example #3: N/A |

Q. 2 HOW AND WHY DOES MY AGENCY USE SSNS?

| How does my agency use SSNs it collects? | Why does my agency use SSNs in this manner? | What is the legal authority for this use? | What are the security risks? | Are changes needed to comply with §96-a? | Timetable for indicated changes? |
|---|--|---|--|---|--|
| Instructions: In separate boxes in this column, identify the format for each use, e.g., on cards, tags or forms, on printed materials such as envelopes, letters, postcards or flyers mailed to the individual, or on e-mail messages, for fraud investigation, internal verification or | Instructions: For each specific use identified in first column, explain why your agency uses SSNs in this manner, and the justification for such use. If the manner of use is on printed or electronic materials mailed to the individual, indicate whether the purpose of the use is as part of an enrollment or | Instructions: For each specific use identified in first column, identify the legal authority for the use of SSNs in this manner. | Instructions: For each specific use identified in the first column, review how the SSNS are displayed or transmitted , e.g., would the SSN as displayed on the communication be visible to persons other than the SSN owner? | Instructions: For each specific use identified in first column, identify the necessary remediation | Instructions: For each specific format identified in first column, identify target completion date and any milestone dates. |

| How does my agency use SSNs it collects? | Why does my agency use SSNs in this manner? | What is the legal authority for this use? | What are the security risks? | Are changes needed to comply with §96-a? | Timetable for indicated changes? |
|---|---|---|---|---|--|
| administrative purposes. | application process, or to confirm the accuracy of the SSN, or to establish, amend or terminate an account, contract or policy. | | | | |
| Example #1: On tax forms mailed to the individual. | Example #1: To enable individual to report taxable benefits. State government entity is required to show SSN on tax form. | Examples #1: Federal or NYS tax law; NYS Personal Privacy Protection Law (especially the “relevant and necessary” provisions). | Example #1: If the SSN as displayed on the tax form is visible through the window of the mailing envelope. | Example #1: Tax form should always be accompanied by a cover letter which does not display the SSN. | Example #1: Cover letter should be included with next tax form mailing. |
| Example #2: As personal ID on cards, tags for customers and employees to use in order to access benefits or services. | Example #2: For personal identification. | Example #2: Well-intentioned but ill-advised effort to comply with laws requiring physical access security. | Example #2: SSN can be seen by anyone viewing the card, tag or form. Includes encoded or embedded SSNs on cards or documents. | Example #2: Phase in new personal ID program that does not allow for use of SSN as personal ID. | Example #2: For new IDs, immediately prohibit use of SSN. Phase-in conversion of existing IDs by (milestone and completion dates). |
| Example #3: Posting on publicly accessible websites or otherwise making available for public inspection <i>newly received documents containing SSNs</i> filed with the agency pursuant to court rules, commercial code laws, or other legal requirements <i>after</i> the new SSN law became effective. | Example #3: Newly received court documents; commercial code filings; clerk’s office documents. | Example #3: Collection and use made pursuant to the relevant laws pertaining to those specific filings with the requisite State government entity. Public release of the documents to adhere to those laws as well as to government transparency laws and principles. | Example #3: SSN can be seen by anyone viewing the site or document. | Example #3: SSNs should be redacted from lists prior to posting and documents prior to inclusion in open record repository. | Example #3: Immediately correct web postings. |
| Example #4: Having posted on publicly accessible websites or | Example #4: Previously received and posted court documents; | Example #4: Collection and use made pursuant to the | Example #4: SSN can be seen by anyone viewing the site or document. | Example #4: No, unless requested to do so by an individual | Example #4: For documents previously made available for |

| How does my agency use SSNs it collects? | Why does my agency use SSNs in this manner? | What is the legal authority for this use? | What are the security risks? | Are changes needed to comply with §96-a? | Timetable for indicated changes? |
|---|--|--|------------------------------|---|---|
| <p>otherwise made available for public inspection <i>previously received documents containing SSNs</i> filed with the agency pursuant to court rules, commercial code laws, or other legal requirements <i>before</i> the new SSN law became effective.</p> | <p>commercial code filings; clerk's office documents</p> | <p>relevant laws pertaining to those specific filings with the requisite State government entity. Public release of the documents to adhere to those laws as well as to government transparency laws and principles.</p> | | <p>to whom the SSN pertains. Redacting SSNs from previously posted documents wholesale without individual prompting would be an optimal practice, should resources permit doing so.</p> | <p>public inspection, redact upon request of individual to whom the SSN pertains.</p> |