



## Office of Information Technology Services

State Capitol P.O. Box 2062  
Albany, NY 12220-0062  
[www.its.ny.gov](http://www.its.ny.gov)

<b>New York State Information Technology Standard</b>	<b>No:</b> NYS-S17-003
<b>IT Standard:</b>  <b>Notification Standard for Certain Types of Regulated Data</b>	<b>Updated:</b> 03/10/2017
	<b>Issued By:</b> NYS Office of Information Technology Services  <b>Owner:</b> Division of Legal Affairs

### 1.0 Purpose and Benefits

---

The primary objective of this standard is to provide State Entities (SE) with breach notification and reporting requirements for some specific types of data that are subject to various legal and regulatory requirements. Please note that this standard does not address *all* regulated data types, so each SE must consult with its legal counsel to determine applicable requirements.

### 2.0 Authority

---

*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 with 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 policy/standard 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”), their employees; and all others, including third parties of State Entities (such as 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. Where a conflict exists between this policy/standard and a State Entity’s policy/standard, the more restrictive policy/standard will take precedence

This standard does not apply to individual members of the State workforce who, pursuant to the Acceptable Use Policy, NYS-P14-001, must immediately report suspected computer security incidents to the appropriate manager and the Information Security Officer (ISO)/designated security representative.

## **4.0 Information Statement**

---

The Cyber Incident Response Standard, NYS-S13-005, identifies Incident Response Stakeholder Roles and Responsibilities and the Incident Response Process Flow. Each SE must assign responsibility for a central point of contact to coordinate identification of an incident and reporting an incident to the Enterprise Information Security Office.

In addition, the Information Security Policy, NYS-P03-002, details that SE executive management is responsible for: complying with notification requirements in the event of a breach of private information; adhering to specific legal and regulatory requirements related to information security; and communicating legal and regulatory requirements to the ISO/designated security representative.

The standards below set forth external notification and reporting requirements for some data types as required by the specific entities referenced herein, and are intended to assist SE executive management in meeting the responsibilities. Each SE should have documented procedures that reflect their compliance with applicable notification requirements, and should include specific names, titles, or functions of the individuals responsible for each stage of the notification process. The document should include detailed instructions for how, and to whom each employee, contractor, or agent should report the incident. Any external notification and reporting from a SE to an external entity should only occur pursuant to their SE incident response protocol and after proper coordination with SE executive management, legal counsel, EISO, and other stakeholders as appropriate.

### **4.1 Notification and Reporting Requirements for Specific Data Types**

#### **[Social Security Administration \(Personally Identifiable Information\)](#)**

The State Agency will comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. 552a), related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), and related National Institute of Standards and Technology guidelines. In addition, the State Agency will comply with Data Protection Provisions set forth in its Information Exchange Agreement with the SSA as the State Transmission/Transfer Component.”

If an employee of the State Agency or an employee of the State Agency’s contractor or agent becomes aware of suspected or actual loss of Personally Identifiable Information (PII) or a security incident which includes SSA-provided information, he or she must **immediately** contact the State Agency official within the SE who is named in the SSA agreement as being responsible for Systems Security. That State Agency official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact identified in the SSA agreement. If, for any reason, the responsible State Agency official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the responsible State Agency official or delegate must report the incident by contacting SSA’s National Network Service Center (NNSC) at 1-877-697-4889 (select “Security and PII Reporting” from the options list). The responsible State Agency official or delegate will use an SSA PII Loss Reporting Worksheet, to quickly gather and organize information about the incident. The responsible State Agency official or delegate must provide to SSA timely updates as any additional information about the loss of PII becomes available.

### **Internal Revenue Service (Federal Tax Information)**

#### **Reporting Unauthorized Accesses, Disclosures or Data Breaches**

Local, state and federal agencies receiving federal tax information must follow Section 10 of [Publication 1075](#) upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents. Agencies must contact Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards **immediately**, but no later than 24-hours after identification of a possible issue involving federal tax information.

**Call the local TIGTA Field Division Office first:** (917) 408-5640.

If unable to contact the local TIGTA Field Division, contact the Hotline Number: 800-589-3718

**Online:** <https://www.treasury.gov/tigta>

**Mailing Address:** Treasury Inspector General for Tax Administration  
Ben Franklin Station  
P.O. Box 589  
Washington, DC 20044-0589

Concurrent to notifying TIGTA, the agency must notify the Office of Safeguards by email to Safeguards mailbox, [safeguardreports@irs.gov](mailto:safeguardreports@irs.gov). To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of agency and agency Point of Contact for resolving data incident with contact information
- Date and time the incident occurred
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident occurred
- IT involved (e.g., laptop, server, mainframe)

Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. Do not include any FTI in the data Incident report.

Agencies are not to wait until after their own internal investigation has been conducted. Contacting TIGTA is critical to expedite the recovery of compromised data and identify potential criminal acts. The IRS Office of Safeguards investigation focuses on identifying processes, procedures or systems within the agency with inadequate security controls which led to the incident.

### **Federal Bureau of Investigation (Criminal Justice Information Services (CJIS))**

The SE shall promptly report incident information to the EISO and the CJIS System Agency Information Security Officer for New York State. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the SE shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact: the EISO and the CJIS System Agency (CSA) Information Security Officer for New York State.

### **Department of Health & Human Services (HIPAA/HITECH)**

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of Health and Human Services of breaches of unsecured protected health information. Covered entities will notify the

Secretary by visiting the [HHS web site](#) at: and [filling out and electronically submitting a breach report form through the HHS web portal](#). If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

### **Center for Medicaid Services**

Known or suspected security incidents involving CMS data must be reported immediately to the CMS IT Service Desk by calling 410-786-2580 or 1-800-562-1963 or via e-mail to [CMS\\_IT\\_Service\\_Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov). Even if you are not positive, but only suspect that it might be a security incident, you must still submit a report and allow the experts to determine whether or not it is a security incident. Any suspected loss or unauthorized disclosure of CMS data protected by the Privacy Act must be reported immediately.

- Provide a breach notification, without unreasonable delay, to the Department as well as individuals affected by the breach. The notification must include:
  - ✓ Source of the breach;
  - ✓ Brief description;
  - ✓ Date of discovery;
  - ✓ Type of PII involved;
  - ✓ A statement whether or not the information was encrypted;
  - ✓ What steps individuals should take to protect themselves from potential harm;
  - ✓ What the agency is doing to resolve the breach; and
  - ✓ Who affected individuals should contact for information.

### **Payment Card Industry Data Security Standards**

The PCI DSS requirements are developed and maintained by an industry standards body called the [PCI Security Standards Council](#) (SSC). The standards are enforced by the five payment card brands: Visa, MasterCard, American Express, JCB International and Discover. Each brand provides *its own* compliance guidelines, reporting and validation requirements, deadlines, brand-specific definitions and penalties for noncompliance. Service providers should therefore obtain notice and reporting requirements directly from the individual card brands.

### **Family Educational Rights and Privacy Act (FERPA; PII in Educational Record Keeping)**

There is not a notification or disclosure requirement under FERPA, however, there IS a requirement to record access and disclosures (39 CFR § 99.32). In addition,

the U.S. Department of Education considers notification a best practice. Furthermore, [New York State Education Law Section 2-d](#) includes notification requirements in the event of an unauthorized release of student data.

## 5.0 Compliance

---

This [policy or standard] 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>.

## 7.0 Contact Information

---

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

**Division of Legal Affairs**  
**Reference: NYS-S17-003**  
**NYS Office of Information Technology Services**  
**1220 Washington Avenue, Building 5**  
**Albany, NY 12242**  
**Telephone: (518) 242-5200**  
**Email: [its.sm.dla@its.ny.gov](mailto: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
01/30/2018	Original Standard Released	Division of Legal Affairs

## 9.0 Related Documents

---

[NYS Information Security Policy](#)

[NYS Cyber Incident Response Standard](#)

[NYS Cyber Incident Response Procedures](#)