BLS NIELSEN INC

CYBERSECURITY POLICY

DATE UPDATED
08/26/2020

DOCUMENT DEFINITIONS

"**Policy**" refers to the Security Policy for Cybersecurity and other Information Security.

"**Agency**" refers to BLS Nielsen Inc.

"**Clients**" refers to the agency's clients, former & prospective clients.

"**Information system**" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

"**Nonpublic Information**" (NPI) shall mean all electronic information that is not Publicly Available Information and is:

1. Business-related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;
2. Any information concerning an individual, which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) driver's license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;
3. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

"**Passwords**" refers to a string of characters that, when possible, is at least 8 characters long and contains at least three of the following: upper case letter, lower case letter, a number, a special character (%, &, #, etc.).

"**Person**" means any individual or non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

"**Third Party Servicer Providers**" (TPSPs) refers to a person that is not an affiliate of the agency that provides services to the agency and maintains, processes or is otherwise permitted access to NPI through its provision of services to the agency.

INFORMATION SECURITY

This Policy for BLS Nielsen Inc (hereinafter referred to as "agency") is intended to create effective administrative, technical, electronic and physical protections to safeguard the personal information of the agency's clients and employees, the agency's proprietary and confidential information, the physical security of our premises, and the integrity of our electronic systems.

This Policy sets forth the agency's procedures for electronic and physical methods of accessing, collecting, storing, using, transmitting, destroying, and protecting NPI of clients, the agency and/or agency employees and also the use of the agency's systems by agency employees and any authorized third parties, as deemed appropriate and/or required by applicable laws and regulations.

In formulating and implementing this Policy, we have:

1. Identified reasonably foreseeable internal and external risks to agency's security, confidentiality and/or integrity of electronic, paper or other records containing private information;
2. Assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the NPI;
3. Evaluated the sufficiency of existing agency policies, procedures, and other safeguards in place to minimize those risks;
4. Designed and implemented an approach that puts safeguards in place to minimize those risks, consistent with the requirements of applicable laws/regulations;
5. Included regular monitoring of the effectiveness of those safeguards.

All security measures contained in this policy shall be reviewed and re-evaluated annually or when there is a change in applicable laws or regulations or in the business activities of agency. The agency reserves the right to modify this policy at any time, with or without prior notice.

EMPLOYEE RESPONSIBILITY

It shall be the responsibility of each agency employee to carefully read, understand and adhere to this policy. Each employee with access to NPI shall receive training as necessary on this policy.

INFORMATION SECURITY COORDINATOR

The agency has designated the office Manager as the “Information Security Coordinator” to oversee implementation of this policy.

The office Manager will be responsible for:

1. Initial implementation and maintaining responsibility for implementation of this policy;
2. Appropriate testing and evaluation of this policy’s safeguards;
3. Reviewing the security measures in this policy annually or when there is a change in applicable laws or regulations or in business activities of agency; and
4. Conducting training as necessary for all agency employees with access to NPI.
5. Implementing policies and procedures to ensure the security of information systems and NPI that are accessible to, or held by, TPSPs.

DATA GOVERNANCE & CLASSIFICATION

SPECIAL PROTECTION FOR NONPUBLIC INFORMATION

NPI is to be accorded the highest level of confidentiality by the agency and employees.

Examples of NPI include, but are not limited to - first name and last name, or first initial and last name, and any one or more of the following:

1. Social Security number
2. Driver's license number, passport number, or state-issued identification card number
3. Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password
4. Personal or protected health information
5. Biometric records.

The information listed in 1-4 above, even if it is not connected with a name, should each be treated as NPI. [A] [B]

WHERE NONPUBLIC INFORMATION IS STORED

The agency and its employees recognize that the agency possesses NPI in the following places, whether in the agency’s premises or off site, and whether created or maintained by agency or third parties on behalf of agency:

1. Hard copy and electronic files on clients and employees, located at desks, in file drawers, storage areas, on computers, electronic devices and on the agency’s systems

2. Personnel files, Form I-9s, benefits information, payroll information, and direct deposit information for employees wherever located, including but not limited to hard copies at desks, in file drawers and other storage areas, and in electronic form on computers, electronic devices or on the agency's systems
3. Off-site back-ups, in any form
4. TPSPs entrusted with NPI from the agency

This policy is intended to protect NPI possessed by the agency from unauthorized access, dissemination and/or use.

NPI may not be disseminated, communicated or stored on or through any social media websites or services, at any time or for any reason. [c]

Employees will adhere to the agency document retention schedule and requirements. When it is appropriate to destroy agency records, paper and electronic records containing NPI must be destroyed in a manner in which they cannot be read or reconstructed.

Unless otherwise directed by the Chief Information Security Officer, a shredding machine at the office will be used to destroy paper documents. When computers, digital copiers, scanners and/or printers with electronic storage capacity, or portable electronic devices and media are discarded, such disposal should be coordinated with the Chief Information Security Officer, and care needs to be taken to ensure that the hard drives or other storage media are destroyed in a manner that all data becomes unreadable.

ASSET INVENTORY & DEVICE MANAGEMENT

1. Employees should keep mobile electronic communications devices (such as PDAs, smart phones, etc.) with access to NPI in their possession or in a secured location at all times, and employees will not share passwords or other access information with others. Mobile electronic devices shall be password protected when not in use.
2. Employees will not put any agency data on thumb drives, laptops or other portable media, drives and devices unless authorized by the agency. If so authorized, the thumb drives, laptops or other portable media, drives and devices should be password-protected and encrypted, and the portable mobile electronic communications devices and laptops should be password-protected and encrypted.
3. Employees whose employment with the agency is terminated for any reason must: (1) return to agency all agency information (including, but not limited to, any NPI) in any form, whether stored on computers, laptops, portable devices, electronic media, or in files, records, work papers, cloud- or web-based storage, etc. immediately prior to or at the time of departure; (2) return all keys, IDs, access codes and/or badges; and (3) not access NPI (including, but not limited to, any private information).
4. In accordance with the agency's human resources manual, access by the former employee to agency email and voice mail accounts shall be immediately disabled and access transferred to other agency staff to assure a continuity of work, and inactivated when determined appropriate by agency.

5. Employees are required to report all actual or potential unauthorized access to, use of or disclosure of NPI to the Chief Information Security Officer.

ACCESS CONTROLS & IDENTITY MANAGEMENT

INTERNAL CONTROLS

To combat internal risks to the security, confidentiality and/or integrity of records containing NPI, the following measures will be taken:

1. Agency computers will require a user ID and password and agency mobile devices should require a password (and be encrypted, if reasonably feasible). Employee log-ins and passwords should be appropriately strong (with the minimum number of characters and other elements required by the agency's systems).
2. Electronic files containing NPI will not be left unattended in an unsecured state, (e.g., computer screens must be locked when an employee using such files leaves his or her computer, even briefly). Paper and electronic files must not be removed from the agency premises or accessed remotely unless specific authorization has been provided in advance, and then, the security of that NPI must be maintained.
3. Employees are expected to log off or lock their computers when they leave them unattended (such as when on breaks, at lunch, in a meeting or out of the office). The agency will implement controls to terminate computer sessions and/or lock computers after a predetermined time of inactivity (e.g., 10 minutes).
4. Employees should not open any email attachment, link, or application where the employee does not reasonably believe the information originated from a trustworthy source, including from personal email accounts. Employees will not use agency equipment to access any application or software not approved by the agency.
5. The agency will retain only the last four digits of credit card numbers and will not retain bank routing numbers, personal bank account numbers and checks, and all credit- and banking-related information not retained will be destroyed in accordance with applicable law and agency-designated business practices.

EXTERNAL CONTROLS

In addition to the measures taken to combat internal risks, the following measures will be taken to minimize external risks to the security, confidentiality and/or integrity of records containing NPI:

1. Visitors to the agency will be escorted within the office and will not have access to agency computers or property that may contain NPI. Guests' wireless access should be fire-walled off from the agency's Systems.

2. The agency will maintain security measures so that its wireless networks cannot be accessed remotely by the public.
3. Servers and other equipment at the agency's premises containing NPI will be maintained in a secure location.

SYSTEMS & NETWORK SECURITY, OPERATIONS & AVAILABILITY

1. The agency will employ an email filter (hardware, software, or third-party provided) that works to restrict and eliminate viruses, spyware and other malware before getting to agency desktop and portable computers.
2. The agency will maintain up-to-date network and firewall protection and operating system security patches on its systems, servers and desktop and laptop computers, as well as other security measures deemed appropriate.
3. The agency will maintain security software, which includes malware protection with up-to-date patches and virus definitions, on its Systems and its servers, desktop and laptop computers, and all mobile devices, which is updated as frequently as possible, but at least daily. [D]
4. All back-ups will be password-protected and encrypted and kept in a secured location off site.
5. Agency employees should use care in communications (e.g., outgoing email and attachments) to ensure: first, that the NPI needs to be sent by email and, if so, that it is transmitted using secure email in accordance with agency policy. [E]
6. The agency will create a secure SSL tunnel between its website and the consumer before allowing the consumer to enter any NPI or to enter a password.
7. When an employee accesses agency systems and/or NPI from a remote location outside the agency internal network, the agency shall provide the employee a secure method to access the agency systems (e.g. Virtual Private Network).
8. Employees should not access agency systems or NPI using non-agency equipment (e.g., a home computer) unless authorized by the agency in writing and the agency determines such access meets the security requirements of the agency. Employees will not store, save, copy or otherwise retain any NPI on any non-agency equipment.

SYSTEMS & NETWORK MONITORING

1. The agency will monitor its systems and equipment for any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such

information system, including but not limited to implementing hardware, software and/or procedural mechanisms to record and report activity for the systems and equipment.

2. The agency will exercise due diligence in making sure TPSPs that are provided NPI have the requisite security controls and written policy in place, provide the agency a written commitment to safeguard and store NPI with at least the same level of security controls as the agency maintains (as outlined in this policy), and advise the agency as to any actual, suspected or potential breaches of private information. [F]

BUSINESS CONTINUITY & DISASTER RECOVERY

IF A BREACH OF NPI (CYBERSECURITY EVENT) OCCURS OR IS SUSPECTED

A security breach occurs when there is an unauthorized acquisition, dissemination, use or loss of NPI. Each employee shall be responsible for notifying the office manager whenever he or she learns there has been or may have been a security breach that may have compromised NPI or other agency information about clients, employees or agency business.

The agency will take the following actions in the event of a security breach:

a. assess the security breach
b. consult counsel
c. review the requirements of the applicable state laws and regulations
d. notify the carriers whose policyholders insured through the agency may have been affected by the event
e. notify the carrier for the agency's cybersecurity coverage
f. notify individuals, regulatory and law enforcement authorities (if and as required and further as deemed appropriate by agency management) [G]
g. take and document corrective actions to contain and control the problem
h. identify who will address any media inquiries
i. draft the content of all communications regarding the event for potentially affected individuals and, if appropriate, the public. [H]

THIRD PARTY SERVICE PROVIDER SECURITY POLICY

This policy defines the minimum cybersecurity standards for Third Party Service Providers (TPSPs) and describes the process and procedures the agency will utilize to identify and assess risk of doing business with TPSPs.

The agency will adhere to the following policy to secure Nonpublic Information (NPI) held or accessed by TPSPs.

The agency shall identify TPSPs that hold or have access to agency's NPI. Once TPSPs are identified, the agency shall conduct periodic due diligence through Third Party Risk Assessments to determine the adequacy of the TPSPs' cybersecurity program. Third Party Risk Assessments shall accomplish the following:

1. Identify potential cybersecurity risks of doing business with identified TPSPs;
2. Assess and categorize the identified risk according to the agency's adopted risk assessment criteria;
3. Decide whether to do business with the TPSP based on the assessment and categorization of risk by the agency;
4. The TPSP Risk Assessments shall be documented in writing.

All TPSPs must adhere to the following minimum cybersecurity practices. The agency may impose additional requirements as it deems necessary.

1. Use of appropriate access controls to limit access to agency's NPI;
2. Notification to the agency within 72 hours of a cybersecurity event directly impacting the agency's information systems or NPI held by the TPSP;
3. Regular cybersecurity awareness training of TPSP personnel;
4. Any other standards or practices required by state or federal laws;

For TPSPs that are Covered Entities under the 23 NYCRR 500 Cybersecurity Regulation, these additional minimum requirements may apply:

1. Encryption of agency's NPI while at rest or in transit;
2. Use of multi-factor authentication when accessing agency's NPI;

Due Diligence Process to Evaluate Adequacy of Third Party Service Provider Cybersecurity Practices and Adherence to Minimum Standards:

To conduct business with the agency, the agency shall establish through its own due diligence that the TPSP employs practices and procedures designed to protect the agency's NPI. The agency's due diligence process may include all or parts of the following until the agency is satisfied that the TPSP meets or exceeds the minimum required cybersecurity practices defined in this policy:

1. Certification by the TPSP that its cybersecurity program meets or exceeds one or more of the following published standards of information/cyber security:
    a. **23 NYCRR 500** (New York State Cybersecurity Requirements for Financial Services Companies)[1]
    b. **ISO/IEC 27000 Family of Standards** (International Organization for Standardization systematic approach to managing and securing sensitive company information)[2]

[1] See https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf
[2] See https://www.iso.org/isoiec-27001-information-security.html

c. **SOC2/3 and/or SOC for Cybersecurity** (Service Organizations Controls for Certified Professional Accountants)[3]
d. **NIST 7621r1** (National Institute of Standards and Technology - Small Business Information Security: The Fundamentals)[4]
e. **NIST CSF** (NIST Cyber Security Framework)[5]
f. **OWASP** (Open Web Application Security Project)[6]
g. **GDPR** (European Union General Data Protection Regulation)[7]

2. Certification that a recent (preferably within the previous 12 months) cybersecurity vulnerability assessment / audit of the TPSP's information technology systems and/or relevant applications was conducted by a qualified party.

    a. The results of the TPSP's vulnerability assessment shall indicate that it presents no vulnerabilities that expose the agency's NPI or violate NY State law or that any such vulnerabilities have since been eliminated;

3. Agency review and acceptance of the TPSP's representations and warranties that address the TPSP's cybersecurity policies and procedures relating to the security of the agency's NPI. Such TPSP policies and procedures may include but not be limited to:

- Access controls, including its use of multi-factor authentication, to limit access to relevant information systems and NPI
- Use of encryption to protect NPI at rest and in transit
- Notice to be provided to agency in the event of a cybersecurity event directly impacting the agency's information systems or NPI

Agency acknowledges that the cyber threat landscape changes over time. Therefore, agency shall conduct periodic risk assessments of TPSPs that are identified during the periodic Agency Risk Assessment process.

Chief Information Security Officer and Use of Third Party Service Provider to Fulfill Agency's Cybersecurity Obligations

The agency may utilize a TPSP to implement and enforce the agency's cybersecurity program and polices, to serve as the agency's Chief Information Security Officer, or both. When a TPSP is utilized by the agency to perform any of the aforementioned functions, the agency shall retain responsibility for compliance with NY State Law and shall designate a senior member employed by the agency to direct and oversee the TPSP.

[3] See https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html
[4] See https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf
[5] See https://www.nist.gov/cyberframework
[6] See https://www.owasp.org
[7] See https://eugdpr.org

A Agency should carefully review security breach notification and privacy laws, as well as insurance laws/regulations, in all states where it does business, as well as in the states in which individuals of an agency hold NPI reside, to make sure this definition of NPI encompasses all of those laws/regulations. The privacy laws typically require that the business keep confidential the information that an individual gives it. The NPI identified above are the kinds of information elements that typically trigger state security breach notification laws, which require notification to the affected individuals, regulators, law enforcement, etc., as well as other statutory requirements, in the event of a breach of Private Information. Click here for a list of the state security breach notification laws, as published by the National Conference of State Legislatures.

B Note on HIPAA: Agency should also carefully review the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules to assure compliance with any requirements that are applicable, such as regarding the treatment of Protected Health Information (PHI). For further information on HIPAA and its privacy and security rules, see https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

C The agency should carefully identify every place in which it maintains NPI to make sure it is identified and thus properly handled and protected, and so it is stored and accessible only to those with a need to access it to do their jobs.

The agency should also determine whether it truly needs to keep that NPI in all the places it exists, or at all, and if not, the unneeded information should be properly destroyed (e.g., paper documents shredded, and electronic materials destroyed or securely deleted (including electronic back-ups) in accordance with the agency's policy and any applicable laws and regulations.

D Agency should set procedures that define the time frames when new software versions relating to each element of its Systems must be implemented.

E The use of TLS email encryption is strongly recommended where the carrier or client can accept it. This results in the friendliest workflow for both the sender and the receiver. Otherwise the email can be sent using a proprietary email solution (if the carrier or other party will accept it) or password-protected file (such as a password-protected PDF), where the password is delivered separately from the email containing the file and consists of information that only the end user will know. For more information on TLS email encryption, see the FAQs at

http://www.independentagent.com/Resources/AgencyManagement/ACT/Pages/policyning/SecurityPrivacy/ACT_TLSFAQ.aspx

Also note that password protecting a file may not be sufficient to avoid triggering a security breach under the state security breach notification laws and regulations if sent to the wrong place or recipient.

F These TPSP commitments need to track the requirements of applicable state security breach notification and other privacy laws and regulations, as well as the agency's policy.

G In New York under Section 899-aa of the General Business Law you must notify (3) NYS offices: the NYS Attorney General, the NYS Division of State Police and the Department of State's Division of Consumer Protection in addition to the Superintendent of the Department of Financial Services as required under Regulation 23 NYCRR 500.

H See http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx for links to the various security breach notification laws, and counsel for the agency also should be consulted to determine if other laws or regulations are applicable. Laws of the states in which the agency conducts business, as well as laws of the states in which individuals affected by a security breach reside, may apply to a particular security breach.

Agents who are subject to the HIPAA privacy and security rules should be aware of HIPAA's breach notification rule, which may apply in the event of a breach of information protected under HIPAA. A summary of the HIPAA breach notification rule can be found in a memo titled, "HIPAA Breach Notification Rule," which is available to Big "I" members who log in to http://www.independentagent.com click on "Big I Resources" & select "Legal Advocacy" and Memoranda/FAQs."

