CSEA LEGAL DEPARTMENT PRESENTS

HIPPA

Health Insurance Portability and Accountability Act of 1996

Privacy in Health Care

Local 1000 AFSCME, AFL-CIO
Mary E. Sullivan, President

MARCH 2019

TABLE OF CONTENTS

This booklet is intended to provide an overview of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy requirements.

I. INTRODUCTION

Title I of HIPAA protects the health insurance coverage of workers and their families in the event of a change or loss of employment. Specifically, Title I reduces the chance of losing existing health care coverage, makes it easier to switch health plans and assists employees in purchasing health care coverage if they lose their employer's plan and have no other coverage available.

Title II of HIPAA contains the Administrative Simplification provisions intended to facilitate the electronic exchange of health information and to protect the privacy and security of those electronic transactions. Specifically, Title II sets the standard for electronic data transactions so that these transactions are uniform and made with reasonable administrative, technical and physical safeguards in place to ensure the integrity and confidentiality of the health information that is transmitted.

Relatedly, and of most interest to employees and their representatives, Title II sets standards for the privacy of individually identifiable health information.

II. STANDARDS FOR THE PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

The final privacy rules establish the general standard that "covered entities" may not use or disclose "protected health information" ("PHI"), except as authorized by the individual who is the subject of the information, as is explicitly required or permitted by the regulation.

"Covered entities" include health plans, health care clearinghouses and their business associates, and health care providers who transmit health-related information in electronic form in connection with a HIPAA-covered transaction. "Group Health Plans" are covered and are considered as an employee welfare benefit plan, including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement or otherwise that (i) has 50 or more participants or (ii) is administered by an entity other than the employer that established or maintains the plan.

Included in the type of plans that are covered by the Privacy Rule are vision, dental and prescription drug plans, long term care plans, and flexible

spending accounts. Expressly excluded are disability, liability and workers' compensation plans, life and retirement plans, and cafeteria plans.

It is important to keep in mind that it is the group health plan function that is the covered entity for purposes of the privacy rules, not the employer as a whole. Thus, employers are not covered entities in their capacity as employers.

Individual's Protected Health Information ("PHI") may not be disclosed by a covered entity except if (1) the individual authorizes disclosure, or (2) the disclosure is permitted by the regulation. It is important to note that even when disclosure is permitted by the regulation, only the "minimum necessary" amount of information to achieve the goal of the use, disclosure or request may be provided.

PHI is defined as "individually identifiable health information." "Health information" is any information (whether oral or recorded in any form or medium) that: (1) is created or received by a health care provider, a health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual. (This is the same information that is covered by the administration simplification standards of the statute.) PHI is only a portion of that information.

"Health information" becomes PHI when it identifies the individual, or could reasonably be used to identify the individual. By way of example, the following information is deemed to make health information individually identifiable:

- Names;
- All geographic subdivisions smaller than a state;
- All elements of dates, except year, directly related to an individual, such as birth date, admission date, discharge date, and death date; all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone and fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers; device identifiers and serial numbers;
- Biometric identifiers, including finger and voice prints; full face images; and,

- Any other unique identifying number, characteristic, or code.

45 CFR §164.514.

Notably, PHI does **not** include certain educational records covered by the Family Educational Right and Privacy Act and certain other education related documents.

III. REQUIREMENTS OF THE FINAL PRIVACY RULE

A covered entity may only use or disclose PHI in accordance with the rules or pursuant to the consent or authorization of the individual whose information is involved. Covered entities are **required** to disclose an individual's PHI to the individual who is the subject of the PHI when that individual requests it.

According to the Final Rule, a covered entity may release PHI to a non-covered entity when the reason the information is required is for treatment, payment or health care operations of the covered entity or of another covered entity (i.e. a group health plan or health care provider).

"Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers. It also includes coordination or management of health care by a health provider and a third-party and consultation or referrals between one health care provider and another.

"Payment" includes activities undertaken by a health plan or provider to obtain or provide reimbursement or premiums for the provision of health care and other activities, such as determinations of eligibility or coverage (including coordination of benefits), risk adjustments, billing, claims management, collections, medical necessity reviews, and utilization review.

"Health care operations" includes certain services or activities necessary to carry out the covered functions of the covered entity with respect to treatment or payment, such as conducting quality assessment and improvement activities, outcomes evaluation and development of clinical guidelines, population-based activities related to improving health or reducing health care costs, coordinating or managing care, evaluating provider performance, engaging in accreditation, certification or licensing activities, underwriting or premium rating for purposes of creation, renewal, or replacement of a contract of health insurance or health benefits, conducting or arranging for medical review, legal services, and auditing, business planning or development, management activities, customer service, resolution of internal grievances, and due diligence in connection with the sale or transfer of assets

to a potential successor in interest. Auditing claims and deciding claims appeals are two common plan functions that are included as part of health care operations.

In addition, the regulations specifically allow the release of PHI without an authorization when:

(a) required by law (and limited to the relevant requirements of that law);

(b) for public health activities (such as to a public health authority authorized by law to collect information to prevent or control disease or to conduct public health surveillance or to receive reports of child abuse and neglect);

(c) to a government authority authorized by law when the covered entity reasonably believes that an individual is a victim of abuse, neglect or domestic violence;

(d) for health oversight activities authorized by law (including fraud and abuse audits, investigations, and civil and administrative or criminal proceedings);

(e) for medical, judicial and administrative proceedings under certain circumstances;

(f) for law enforcement purposes to a law enforcement official (limited to information for identification and location purposes, or when reporting a crime in an emergency) (decedents: funeral directors and coroners for identification or to determine cause of death);

(g) to organ procurement organizations for cadaveric organ, eye or tissue donation purposes;

(h) for research purposes (provided that an Institutional Review Board or privacy board as described in the statute approves the absence of individual authorizations);

(i) to avert a serious threat to health or safety;

(j) for specialized government functions (such as separation or discharge from the military, to determine eligibility for veterans' health benefits, or for protective services); and

(k) required for compliance with worker's compensation and other similar laws.

All other uses and disclosures of PHI that are not specifically permitted to be made without an authorization, require the covered entity to obtain a valid authorization.

It should be noted that there are special rules for the use and disclosure of PHI when the information is contained in psychotherapy notes and for the use of PHI for purposes of marketing or in marketing materials.

IV. SPECIFIC REQUIREMENTS FOR DISCLOSURES TO EMPLOYERS AS SPONSORS OF GROUP HEALTH PLANS

An employer, as a plan sponsor of a Group Health Plan, is not a "covered entity" under HIPAA. 45 CFR §164.504. Consequently, PHI cannot be freely shared between the Group Health Plan and the employer. In order to avoid the problem that would be presented by requiring an employer to obtain individualized authorizations for each use of information, the Final Rule specifically dealt with this issue by establishing a procedure that — if followed — permits the flow of information from the Group Health Plan, health insurance issuer or HMO to the employer/plan sponsor.

In order to disclose PHI to the plan sponsor or to provide for or permit the disclosure of PHI to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, the plan documents must be amended to reflect adequate restrictions on uses and disclosures of PHI by the plan sponsor in a manner which is consistent with the Final Rule.

Specifically, this must be accomplished by ensuring that the plan documents are amended to include provisions to:

1. Establish and describe how PHI will be used by the plan sponsor;

2. Identify those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the PHI to be disclosed, and describe the circumstances under which the access will be permitted;

3. Provide an effective mechanism for resolving any issue of non-compliance by persons given access to the PHI with the plan document provisions; and

4. Provide that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and the plan sponsor agrees to:

- Not use or further disclose the PHI other than as permitted or required by the plan documents or as required by law §164.504(f)(2)(ii)(A);

- Ensure that any agents, including subcontractors, to whom it provides PHI received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information. 45 CFR §164.504(f)(2)(ii)(B);

- Not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor. §164.504(f)(2)(ii)(C);

- Report to the group health plan any use or disclosure of PHI which is inconsistent with the uses and disclosures provided for of which it becomes aware. §164.504(f)(2)(ii)(D);

- Make available PHI in accordance with the individual's right to access. 45 CFR §164.504(f)(2)(ii)((E);

- Make available PHI for amendment and incorporate any amendment to PHI in accordance with the Privacy Rules. 45 CFR §164.504(f)(2)(ii)(F);

- Make available the information required to provide an individual with an accounting of disclosures. 45 CFR §164.504(f)(2)(ii)(G);

- Make its internal books, records and practices relating to the use and disclosure of PHI received from the group health plan available to the Secretary of Health and Human Services for the purposes of determining whether the group health plan is in compliance with the Privacy Rules. 45 CFR §164.504(f)(2)(ii)(H);

- If feasible, return or destroy all PHI received from the group health plan that the sponsor still maintains in any form and retain no copies thereof when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit such uses and disclosures to those purposes that make the return or destruction of the PHI not feasible. 45 CFR §164.504(f)(2)(ii)(I); and

- Ensure that adequate separation exists between the group health plan and the plan sponsor. 45 CFR §164.504(f)(2)(iii) (J).

In addition, the Final Rule specifically permits the health plan, health insurance issuer or HMO to disclose "summary health information" to the plan sponsor if the plan sponsor requests such information for the purpose of: (1) obtaining premium bids from health plans for providing health insurance

coverage under a group health plan; or (2) modifying, amending or terminating the group health plan.

Finally, the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the group health plan.

V. INDIVIDUAL RIGHTS CREATED BY THE FINAL PRIVACY RULE

Restrictions on Uses and Disclosures: The individual has the right to request a restriction on the manner in which PHI is disclosed for purposes of treatment, payment and health care operations. The covered entity does not have to agree to any such restriction, but it must permit the individual to make the request. 45 CFR §164.522(a)(1).

Request for Confidential Communications: The individual has the right to request that the covered entity communicate PHI to the individual by an alternative method or at an alternative location. The covered entity must agree to any such request which is reasonable. 45 CFR §164.522(b)(1).

Access to PHI: The individual has the right to request access to or a copy of his or her PHI. The covered entity may deny this request for certain reasons set forth in the Privacy Rules. In some instances, the individual has the right to have the denial of his or her requested access reviewed. 45 CFR §164.524.

Amendment of PHI: The individual has the right to request that his or her PHI be amended. The request for amendment may be denied for certain reasons. Upon denial, the individual has the option to write a statement disagreeing with the denial and the covered entity may write a statement rebutting the individual's statement of disagreement. 45 CFR §164.526.

Request for an Accounting: An individual may request an accounting of all disclosures made during a period of up to six (6) years. The covered entity need not account for the following disclosures (45 CFR §164.528):

1. Disclosures made for treatment, payment or health care operations;

2. Disclosures made to the individual;

3. Disclosures made pursuant to a valid authorization;

4. Disclosures made for use in a facility directory or to people involved in the individual's care;

5. Disclosures incident to a use or disclosure permitted by the Privacy Rules;

6. Disclosures made for national security or intelligence purposes;

7. Disclosures made to a correctional institution or to law enforcement officials;

8. Disclosures made as part of a limited data set; and

9. Disclosures that occurred prior to April 14, 2003, the compliance date for the covered entity. 45 CFR §164.534.

VI. ADMINISTRATIVE OBLIGATIONS OF THE COVERED ENTITY 45 CFR §164.530 (unless otherwise noted)

Policies and Procedures: Every covered entity must have policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications and other requirements of the Final Rule. These policies and procedures must exist in written or electronic format and must be reasonably designed, taking into consideration the size and type of activities that relate to PHI undertaken by the covered entity.

Notice of Privacy Practices: Every covered entity must have a Notice of Privacy Practices that places individuals on notice of their rights and of the covered entity's responsibilities with regard to PHI. 45 CFR §164.520.

Personnel Designations: Every covered entity must designate a Privacy Officer who is responsible for the development and implementation of the policies and procedures of the covered entity. Additionally, the covered entity must designate a Contact Person, to whom an individual may complain regarding a privacy violation.

Training: Every covered entity must provide the necessary training on covered entity policies and procedures as is necessary to allow each employee to perform his or her function. This training must be provided to each existing employee no later than the April 14, 2003 compliance date (45 CFR §164.534), and to each new employee within a reasonable period of time from his or her date of hire.

Complaints: Every covered entity must provide a process by which an individual may file a complaint about the covered entity's policies and procedures or its compliance/non-compliance with those policies and procedures.

Mitigation: A covered entity must, to the extent possible, mitigate any harmful effect(s) resulting from use or disclosure of PHI in violation of the covered entity's policies and procedures or the Privacy Rules.

Business Associate Agreements: A covered entity may disclose PHI to a business associate and may allow a business associate to create or receive PHI on behalf of the covered entity, provided that the covered entity receives reasonable assurances from the business associate that it will adequately safeguard the PHI by signing a Business Associate Agreement. This standard does not apply to: (a) disclosures made by a covered entity to a health care provider concerning the treatment of the individual; or (b) certain disclosures by a group health plan or health insurance issuer or HMO with respect to a group health plan to the plan sponsor. 45 CFR §164.308(b)(I).

Sanctions: The covered entity must have and apply appropriate sanctions against members of its workforce that violate the covered entity's policies and procedures.

VII. SPECIFIC EXCLUSIONS

The Final Rule specifically exempts from the definition of PHI "employment records held by the covered entity in its role as an employer." 45 CFR §160.103.

In the Final Rule, Health and Human Services intentionally failed to define the term "employment records." HHS was concerned that defining the term "employment records" would lead to the misconception that certain records would never constitute PHI and would wrongly place the focus of such an inquiry on the nature of the information in question rather than on the reason for which the covered entity obtained the information.

HHS did clarify that information needed for an employer to carry out its obligations under FMLA, ADA and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance and fitness-for-duty employee tests may be part of the employment records maintained by the covered entity in its role as an employer.

For example, drug screening test results will be PHI when a provider administers the test to the employee. Those same drug test results, however, will not be PHI in the hands of an employer when, pursuant to a valid authorization, the provider discloses the test results to the employer and the employer places them in the employee's employment record. The same result is reached even if the drug testing is administered by an employee health clinic operated by the employer, and the health clinic discloses the results of the

testing, pursuant to a valid authorization, to the employer.

Employers should note that just because certain employment records are not subject to the Privacy Rules, those records remain subject to all privacy protections that currently protect employment records.

VIII. QUICK REFERENCE GUIDE FOR UNIONS

Q: What do the HIPAA Privacy Rules do?

A: The HIPAA Privacy Rules create national standards for the protection of individuals' medical records and health-related information through which an individual might be identified (protected health information or "PHI"). Specifically, it gives individuals more control over their health information, sets limits on the use and release of health records, establishes safeguards to protect the privacy of that health information, and institutes criminal and civil penalties to hold violators accountable for improper disclosure of records or information.

Q: What are an individual's privacy rights under the statute?

A: Generally, individuals have the right to make informed choices when seeking health care and/or reimbursement for care, with respect to how personal health information may be used. Specifically, individuals have the right to:

- consent to treatment, payment and health care operations;
- agree or object to a use or disclosure of protected health information for non-treatment, non-payment, or non-healthcare operations;
- receive a Privacy Notice from health care providers and insurers;
- access and amend protected health information;
- request a restriction on the use and disclosure of protected health information;
- obtain an accounting of disclosures of protected health information; and,
- request alternative communication methods regarding protected health information.

Q: What is the impact on health information in the context of workers' compensation and disability?

A: Several situations where personal health information is utilized for benefits purposes are explicitly exempt from the HIPAA privacy requirements, including workers' compensation carriers, disability insurers, and life insurance carriers. When the information is obtained by these entities for purposes of providing benefits coverage, the use and storage of the information will not be limited by the HIPAA privacy rules. This means that authorizations and

consents are not needed to obtain this information. Of course, the information is still required to be kept confidential by an employer.

Q: Does HIPAA apply to a sick leave bank and is the bank itself, or is an employee who sits on the bank, a "business associate" of the employer?

A: A sick leave bank is not a "covered entity" under HIPAA. Thus, HIPAA's provisions do not apply. Nor is a sick leave bank a "business associate" of a covered entity because it does not undertake to perform functions for or provide services to or on behalf of a covered entity.

Sick bank committees presumably do not disclose the information received to anyone else. Moreover, the Department of Health and Human Services clarified that information needed for an employer to carry out its obligations under FMLA, ADA, or other similar laws, as well as records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance and fitness-for-duty employee tests are part of employment records. Consequently, where information is provided in order to substantiate an employee's request for sick leave, it constitutes an employment record to which HIPAA does not apply.

Q: What impact will HIPAA have on employer-sponsored Flexible Spending Accounts?

A: Employers sometimes provide flexible spending account plans ("FSAs") to employees. These plans may be self-administered and self-insured or administered by a third-party administrator. So long as there are fifty or more participants in the plan, it will be a "Group Health Plan" and HIPAA provisions will apply.

The burden of compliance with HIPAA privacy provisions falls on the employer or the plan administrator if it is someone other than the employer. In either case, employers/plan administrators who offer such plans will need to amend their written flexible benefit policies to indicate compliance with HIPAA privacy provisions. In addition, employers/plan administrators must distribute a Notice of Privacy Practices to employees with regard to flexible benefits plans.

There are numerous administrative and physical plant changes that employers need to make as well. These include:

- appointing a Privacy Official and a Contact Person for employees;
- training Human Resources staff on how to request, protect, and provide Protected Health Information ("PHI");
- implementing physical and technological privacy safeguards;

- creating a firewall where necessary between "health plan" functions and Human Resources functions to ensure that PHI is not used or disclosed for employment or other benefit plan purposes;
- creating a process for receiving complaints about HIPAA policies and procedures, or compliance; and,
- determining how they will mitigate any harmful effects from wrongful disclosures under HIPAA, including establishing sanctions to be applied for violations.

In short, FSAs are required to keep employee health information confidential and establish procedures by which employees may access and change their own information.

Q: Are unions or employees with specific responsibilities "business associates" under HIPAA?

A: Unions and individual employees typically are not business associates of an employer under HIPAA. Some employers are choosing to interpret HIPAA to require a "business associate" contract with either the union or its employees who deal with personal health information. This is not what the statute requires. As defined by HIPAA, a "business associate" is someone who **performs** or **assists** a **covered entity** to perform its job using protected health information ("PHI").

For example, a claims adjuster at an HMO is a business associate of a doctor's office because the adjuster will utilize PHI of a patient to determine whether a procedure is covered, thus allowing the doctor to provide treatment and/or obtain payment. CSEA's dealings with employers, even with health care industry employers, do not put the union in the role of performing functions on behalf of the employer by using PHI. (Note that even in the example set forth above, the employee-claims adjuster is not him/her self a business associate of either the doctor's office or the HMO. He or she is simply an employee of a covered entity.)

Q: How does HIPAA affect the union's ability to assist members with benefit problems or appeals?

A: Generally, union representatives will need a written authorization to obtain PHI from a covered entity such as an HMO or employer-insurer. Remember that it is not problematic for a union representative to possess PHI that has been given to them by the member. The member has consented to the use of this information on his or her behalf. It is the insurer or other covered entity that will decline to share PHI with a union representative in the absence of an authorization from the member. In addition, where a spouse reveals the PHI to a union rep, this is also not a violation of HIPAA. The bottom

line is that a union representative is not covered under HIPAA and is therefore not constrained by its provisions.

Q: What effect does HIPAA have on the union's ability to negotiate health benefits for members?

A: A union has a more difficult time amassing medical information about its members in order to analyze health plans. However, HIPAA excludes certain kinds of information: "summary health information" is not considered PHI and is census-type information that can be presented to plan sponsors in order to obtain premium bids for health insurance coverage or to modify, amend or terminate a Group Health Plan.

Q: Are all records that contain medical information covered by the privacy regulations?

A: No. An employer is not, in and of itself, a covered entity. In most cases, only the employer's health insurance related activities are covered. Employment related activities and records are not covered under HIPAA. If an employer has properly obtained medical information (for example, medical information received from the employee in connection with a work place issue such as returning to work, the need for accommodation in work assignments, or the need for leave), that information is not PHI falling within HIPAA privacy protections. This information is an "employment record" held by a non-covered entity. (Non-HIPAA confidentiality and non-discrimination requirements still apply, however.) If the employer has used this information to make employment-related decisions, that use is not regulated by HIPAA. Moreover, the employer may not cite HIPAA as a basis to refuse to provide the information if requested.

Q: How is it possible for someone other than the individual him or herself to obtain medical information about that individual?

A: Generally, information may be obtained using an authorization or consent form (depending on the circumstances) or through a health care power of attorney. (This must be a **health care** power of attorney rather than a general power of attorney.) However, certain individuals (referred to as "personal representatives") are entitled, under HIPAA, to have access to the information and make decisions on behalf of another individual. For adults, a health care power of attorney is needed. For children, a parent, guardian, or anyone acting *in loco parentis* may make health care decisions on behalf of the minor child and, consequently, have access to medical information about that child. This means that a parent is generally permitted access to a child's medical records **unless otherwise prohibited by law**. The parent may always agree to allow the child to have a confidential relationship with a health care

provider. Where an individual is deceased, someone with legal authority to act on behalf of the decedent or the estate may do so (e.g., executor of the estate, next of kin or other family member, someone holding a durable power of attorney).

Q: What can an individual do if he or she believes his or her privacy rights have been violated?

A: HIPAA enforcement is intended to be "complaint driven." Privacy notices issued by health plans and other covered entities must include information about filing complaints directly with the entity about violations. Each covered entity must establish a system for taking complaints, acting to minimize wrongful disclosures of information, and disciplining or penalizing its employees for violating the privacy rules. In addition, a written complaint must be filed with the federal Office for Civil Rights (OCR) within 180 days from when the individual knew or should have known that the violating act occurred. However, the Secretary may waive the 180-day time limit if good cause is shown. See, www.hhs.gov/hipaa/filing-a-complaint/index.html for more information.

APPENDIX
45 CFR §164.508(c)

Authorization To Disclose Protected Health Information

Please complete the following information. This authorization will not be valid until all sections are completed.

I *(print your name)* _____ hereby request and authorize the release of the information described below.

Fill in the name of the person whose Protected Health Information you are authorizing to be disclosed:

Name: _____ ID Number: _____

Address:_____ Date of Birth:_____

_____

_____

_____

What is your relationship to this person?

_____Self _____ Parent _____Guardian _____ Personal Representative (Please provide documentation such as a Court Order, Power of Attorney Health Care Proxy, etc.)

Please identify the person(s) or organization(s) you are authorizing to release the information (e.g. name of insurance carrier, health plan administrator, etc.):

_____

_____

_____

Purpose of this authorization: please note that by signing this form you will authorize CSEA to obtain your protected health information for the following purposes. **Please check one:**

_____ Any purpose
_____ Specific medical condition or service date(s): _____
_____ Other (briefly describe): _____

Protected Health Information to be Disclosed: Please indicate the specific protected health information you authorize us to obtain for the purposes stated above. Please check all that apply:

_____**Claim/Benefit Information** (i.e., status, type of service, diagnosis, provider, dates of service, benefits available, benefits used, contract limits, etc.)

_____ **Membership Information** (i.e., coverage information, enrollment dates, eligibility, address, dates of birth, etc.)

_____ **Other** (briefly describe) _____

Entity Authorized to Request and Receive:

_____, **CSEA (i.e., Labor Relations Specialist, Health Benefits Associate, etc.)**

Expiration: This authorization will remain in effect for twelve (12) months from the date of your signature unless you specify a different date or an event that will cause the authorization to expire. You may specify an expiration date or event for this authorization: _____

Acknowledgements: This Authorization may be revoked in writing at any time, except to the extent that the entity disclosing the information has already relied upon it. Signing this Authorization is not a condition for treatment, payment, enrollment, or eligibility benefits. Information disclosed in reliance upon this Authorization may not be redisclosed by the recipient except in accordance with law or as otherwise authorized. In the event of such redisclosure, the information may no longer be protected under the HIPAA Privacy Rule.

Signature: Date Signed:

_____ _____

Prepared by the
CSEA Legal Department
LOCAL 1000, AFSCME, AFL-CIO
143 Washington Avenue
Albany, New York 12210

Mary E. Sullivan, President