

HEALTH INFORMATION PRIVACY POLICIES AND PROCEDURES

I. USE AND DISCLOSURE POLICIES AND PROCEDURES

1. Fundamental Policies on Use and Disclosure of Protected Health Information.

Short Summary: There are certain common situations in which a plan enrollee's protected health information can be disclosed. For example, the plan (or its third party administrator) can send a \$500 check to a hospital and note on the check that the payment was for a particular enrollee's (e.g., "John Smith's") medical expense. This is a disclosure of protected health information but it is for "payment" purposes (discussed further in Section 1(b)(i)).

a) **POLICY—No Use or Disclosure.** You must not use or disclose protected health information except as these Privacy Policies and Procedures permit or require.

b) **Treatment, Payment, Health Care Operations.**

i) **POLICY—Our Activities.** We may use and disclose protected health information, without the individual's permission, for our own payment activities and our own health care operations. As a group health plan, we do not ourselves engage in treatment, though we may be included in the coordination of treatment activities for individuals by health care providers. We may disclose protected health information, without the individual's permission, for any health care provider's treatment activities. We may disclose the minimum necessary protected health information, without the individual's permission, for the payment activities of another covered entity or any health care provider. Special rules apply for disclosures related to another covered entity's health care operations. If this occurs, we will consult our legal counsel.

ii) **POLICY—Organized Health Care Arrangement's Health Care Operations.** When we participate in an organized health care arrangement, we may disclose the minimum necessary protected health information to other covered entity participants in the organized health care arrangement for the health care operations of the organized health care arrangement. This generally allows us to share protected health information with other health plans of our sponsors.

iii) **POLICY—Underwriting and Other Insurance Function Health Care Operations.** We may use and disclose the minimum necessary protected health information for underwriting, premium rating or other activities relating to creation, renewal or replacement of a contract of health insurance or health benefits. We may also use and disclose the minimum necessary protected health information to cede, secure or place a contract for reinsurance of risk for health care claims (including stop-loss and excess loss coverage).

c) **POLICY—Individual or Personal Representative.** We may disclose protected health information to the individual who is the subject of the protected health information and to that individual's personal representative as relevant to the scope of the representation.

d) **POLICY-No Sale, Marketing, Fundraising, Research or Uses of Genetic Information for Underwriting.** We will not directly or indirectly receive remuneration in exchange for any protected health information of an individual, except as otherwise allowed by applicable law. We will not engage in marketing of protected health information, except if such marketing is permissible under HIPAA and does not require an authorization. We will not use or disclose

protected health information for fundraising purposes. We will not use or disclose genetic information which is protected health information for underwriting purposes. We will not use or disclose protected health information for research purposes.

- e) **POLICY - Identify Verification.** We will verify the identity and/or authority of someone prior to making a disclosure, if we are uncertain of either.
- f) **PROCEDURE.** Document how you verify the identity and authority of any person, unknown to you, requesting protected health information. Provide the documentation to the Privacy Official, who will retain it for at least six years.

2. **Informal Permission for Certain Uses and Disclosures.**

Short Summary: Releasing a plan enrollee's protected health information to that enrollee's family member or friend is not allowed unless you satisfy an exception (described further in this Section 2).

- a) **POLICY—Informal Permission for Certain Uses and Disclosures.** We may use with, and disclose to, an individual's family members, other relatives or close personal friends, and any other person that the individual identifies, the individual's minimum necessary protected health information directly relevant to that person's involvement with the individual's health care or payment related to that health care if we follow all applicable procedures.
- b) **PROCEDURE—Individual Present or Not Present.** If the individual is present or available and has the capacity to make health care decisions, you must inform the individual of your intent to disclose the protected health information. You may make the use or disclosure if:
 - The individual agrees; or
 - The individual does not object after a reasonable opportunity to do so; or
 - You infer from the situation that, in your professional judgment, the individual does not object.

If the individual is not present we may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes.

3. **Authorization for Use or Disclosure.**

Short Summary: If we believe we need to make a use or disclosure of protected health information but cannot find any relevant exception, we will ask the plan enrollee to complete an authorization to approve the use of disclosure.

- a) **POLICY—Authorization.** We must have written authorization from the individual (or the individual's personal representative) before we may use or disclose an individual's protected health information for any purpose, except for the following:
 - For treatment, payment or health care operations.
 - To the individual, the individual's personal representative or HHS.
 - As permitted for public interest or benefit activities.
 - As permitted with a business associate.
 - Incidental to otherwise permitted or required uses and disclosures.
 - **Use FORM 3 – Authorization.**
- b) **POLICY—Authorization Revocation or Expiration.** We may not rely on an authorization we know has been revoked or has expired. An individual may revoke an authorization at any time.

Revocation of an authorization does not affect actions we may have undertaken in reliance on the authorization before we learned of its revocation.

4. Public Interest or Benefit Use and Disclosure.

Short Summary: There are a few unusual situations where the plan can use and disclose protected health information even though the use or disclosure is not for the Plan's payment or health care operations and even though the health plan enrollee has not signed an authorization. These situations are generally noted in this Section 4. For example, a court may order us to disclose the enrollee's protected health information.

- a) **POLICY—Public Interest or Benefit Use and Disclosure.** We may use or disclose an individual's protected health information for the public health, public interest, public benefit, and law enforcement activities listed in this Section 4, without the individual's permission.

Use FORM 6 - Disclosure Log/Minimum Necessary to assist with and document your determination of the minimum necessary use or disclosure and to log each disclosure for accounting.

- b) **Workers' Compensation.** We may disclose the minimum necessary protected health information authorized by and needed to comply with workers' compensation or similar programs established by law that provide benefits for work-related injury or illness without regard to fault.
- c) **Required by Law.** We may use or disclose protected health information as required by law.
- d) **Health Oversight Activities.** We may disclose the minimum necessary protected health information to a health oversight agency as needed for legally authorized health oversight activities, such as audits, civil, criminal or administrative actions or proceedings, inspections, licensure, certification, disciplinary actions, and appropriate oversight of the health care system or government benefits programs (e.g., Medicare and Medicaid) for which health information is relevant to beneficiary eligibility or entities subject to government regulatory programs or civil rights laws.
- e) **Judicial and Administrative Proceedings.** We may disclose the minimum necessary protected health information in the course of a judicial or administrative proceeding:
- i) **Order.** In response to a court or administrative tribunal order, provided we disclose only the expressly ordered protected health information.
- ii) **Process.** In response to a subpoena, discovery request or other lawful process not accompanied by court or administrative tribunal order, if we:
- Make a reasonable effort to provide notice to the individual sufficient to permit the individual to object to, or seek a qualified protective order from, a court or administrative tribunal; or
 - We receive "satisfactory assurance" that the information seeker has made reasonable efforts either (a) to ensure the individual has notice, or (b) to secure a qualified protective order from the court or administrative tribunal or by party stipulation that limits the parties' use or disclosure to the purpose of the proceeding, and requires return or destruction of the protected health information (including all copies) at end of the proceeding. Ask our Privacy Official if we have sufficient "satisfactory assurance".

5. Required Disclosures.

Short Summary: Sometimes we must disclose protected health information -- for example, if the U.S. Department of Health and Human Services ("HHS") is auditing our health plan for HIPAA and HHS requests the protected health information.

- a) **POLICY—Required Disclosures to Individual or Personal Representative.** We must disclose all protected health information subject to the right of access or disclosure accounting to an individual (or the individual's personal representative) requesting access or disclosure accounting. See Sections 12-14.
- b) **POLICY—Required Disclosures to HHS.** We must disclose protected health information to HHS as required for complaint investigation or compliance enforcement or review.

6. Minimum Necessary.

Short Summary: When we use or disclose protected health information, we generally can use or disclose the "bare amount" needed. This is called the "minimum necessary" amount for the use or disclosure.

- a) **POLICY—Minimum Necessary.** We must make reasonable efforts to use, to disclose, and to request of another covered entity, only the minimum necessary protected health information to accomplish the intended purpose. This generally will consist of the protected health information contained in a limited data set, although it can be more if needed to accomplish the intended purpose of such use, disclosure or request. There is no minimum necessary limitation for:
 - Disclosure to or a request by a health care provider for treatment.
 - Use with and disclosure to an individual (or the individual's personal representative).
 - Use and disclosure pursuant to an authorization by an individual (or the individual's personal representative).
 - Disclosure to HHS for complaint investigation or compliance enforcement or review.
 - Use and disclosure required by law.
 - Use and disclosure required for compliance with the HIPAA Administrative Simplification Rules.
- b) **POLICY—Workforce Use.** We must make reasonable efforts to limit access to and use of protected health information by our workforce members to the minimum necessary to perform their duties.

Use FORM 6—Disclosure Log/Minimum Necessary to document your compliance with the minimum necessary limitation. Include the completed Form 6 in the individual's records. Send a copy to our Privacy Official.

7. De-Identified Health Information.

Short Summary: Protected health information which has been "de-identified" (so no plan enrollee can be identified) is no longer protected health information and is not subject to HIPAA or these Policies and Procedures.

- a) **POLICY—De-Identified Health Information.** We may use and disclose de-identified health information without restriction. We will treat as protected health information any key or other means to re-identify health information that has been de-identified.

II. RELATIONSHIP RULES

8. Personal Representatives.

Short Summary: In some situations one person (e.g., a parent) is generally allowed to act on behalf of another person (e.g., a child) and receive that second person's protected health information (e.g., a parent generally can receive a child's protected health information).

- a) **POLICY—Personal Representative.** We must consider a personal representative to be the individual for all purposes under these Privacy Policies and Procedures and the Privacy Rules, unless we conclude that the personal representative may be abusive.
- b) **POLICY—Personal Representatives of Unemancipated Minors.** We will grant a parent, guardian or person acting "in loco parentis" (which generally means the parent is acting on behalf of the child) access to and control over an unemancipated minor's protected health information if, and to the extent, applicable State or other law (including case law) permits or requires us to give the parent, guardian, or person acting in loco parentis access or control. If the law is unclear we will discuss the matter with legal counsel.
- c) **Personal Representatives of Deceased Individuals.**
 - i) **POLICY—Information Protected.** We will accord the protected health information of a deceased individual all of the privacy protections of these Privacy Policies and Procedures and the Privacy Rules until at least 50 years after the death of the individual. If the individual is deceased, we may disclose to a family member, or other relative or close family friend who is involved in the care or payment for health care of the individual prior to the individual's death, the protected health information that is relevant to such person's involvement. However, we will not make this disclosure if it is inconsistent with the individual's prior expressed preference and that preference is known to us.
 - ii) **POLICY—Rights of Executors.** We will furnish an executor, administrator or other person authorized by applicable law to act for a deceased individual or the deceased individual's estate, the same rights with respect to a deceased individual's protected health information that must be accorded the individual, provided the protected health information is relevant to the scope of the representation.

9. Business Associates.

Short Summary: Our health plan (or the employer on behalf of our plan) may hire third parties who will receive protected health information and use or disclose it on our behalf. Before that occurs, we must make sure that third party has signed a contract in which it agrees to follow HIPAA. This contract is called a "business associate agreement."

- a) **POLICY—Uses and Disclosures with Business Associates.** We will not disclose protected health information to a business associate, or allow a business associate to create or receive protected health information on our behalf, unless our Privacy Official or our legal advisers confirms that the business associate has entered into a compliant written contract with us.

The business associate contract requirement does not apply to our permitted disclosures to:

- A health care provider concerning treatment.
- Our plan sponsor.

FORM—Business Associate Contract. We will use FORM 1 - Business Associate Contract Terms or another business associate agreement we find acceptable. We can verify if an agreement is acceptable by using FORM 2 -- Business Associate Agreement Checklist.

- b) **POLICY—Business Associate Compliance.** If we learn that a business associate has materially breached the business associate contract, we will require the business associate to promptly cure the breach. If the business associate fails to cure the breach to our satisfaction, we will terminate the business associate contract and our business associate relationship with that business associate.

10. Plan Sponsors and Third Party Administrators.

Short Summary: Under HIPAA, an employer generally cannot receive protected health information unless it has agreed to follow HIPAA's requirements. There can be a few exceptions, such as "enrollment information". This exception allows the employer to know which employees are in (or out) of the health plan and which level of coverage (e.g., single or family) those employees have selected.

- a) **POLICY—Disclosure of Protected Health Information to Plan Sponsors.** We may not disclose, and we may not permit a health insurance issuer, HMO, third party administrator, or other business associate to disclose on our behalf, protected health information to our plan sponsor—the employer, union or other entity that established and maintains our group health plan—unless we have the authorization or other sufficient permission of each plan participant and beneficiary whose protected health information is to be disclosed. There are three exceptions:
- i) **Enrollment Data to Plan Sponsor.** Our plan sponsor may receive from us, and from a health insurance issuer, HMO, third party administrator, or other business associate on our behalf, the minimum necessary information to determine whether an individual is or is not participating in our group health plan.
- ii) **Summary Health Information to Plan Sponsor.** Our plan sponsor may receive from us, and from a health insurance issuer, HMO, third party administrator, or other business associate on our behalf, the minimum necessary summary health information to enable our plan sponsor to either (a) obtain premium bids for providing coverage under our group health plan, or (b) modify, amend or terminate our group health plan. However, notwithstanding the prior sentence, we may not disclose genetic information that is protected health information as part of this summary health information provision.
- iii) **Plan Administration Functions by Plan Sponsor.** Our plan sponsor may receive from us, and from a health insurance issuer, HMO, third party administrator, or other business associate on our behalf, the minimum necessary protected health information of our plan participants and their beneficiaries to enable our plan sponsor to perform plan administration functions for us, provided that our plan sponsor furnishes written certification that the group health plan document has been amended to include “satisfactory assurance” that our plan sponsor will appropriately safeguard and limit use and disclosure of the protected health information, including not using or disclosing the protected health information for any employment-related action or decision or in connection with any other benefit or benefit plan.

FORM 4—Plan Sponsor's Group Health Plan Document Amendment contains the mandatory terms for our plan document that the Privacy Rules require to evidence the plan sponsor's “satisfactory assurance.”

FORM 5—Plan Sponsor's Certification of Group Health Plan Document Amendment is an example of the certification of “satisfactory assurance” our plan sponsor must make.

III. INDIVIDUAL'S INFORMATION RIGHTS

11. Privacy Practices Notice.

Short Summary: Our health plan is required under HIPAA to send a notice to plan participants explaining their privacy rights under HIPAA. We must send out that notice to new participants (or arrange to have another entity send it, such as our third party administrator) and then periodically send out reminders about the notice.

- a) **POLICY—Privacy Practices Notice.** As a self-funded group health plan, we will maintain a Privacy Practices Notice. That Notice must give individuals written notice of the uses and disclosures of protected health information that we may make, our legal duties with respect to protected health information, and individuals' privacy rights and how to exercise them. We must use and disclose protected health information consistently with our Notice. Use FORM 7 – Privacy Practices Notice as a template for our Privacy Practices Notice.
- b) **POLICY—Revision to Privacy Practices Notice.** We will promptly revise our Privacy Practices Notice whenever there is a material change to our uses or disclosures of protected health information, to our legal duties, to the individuals' rights or to other privacy practices that render the statements in our Notice no longer accurate.
- c) **PROCEDURE—Privacy Practices Notice Distribution.** Our Privacy Official will distribute (or cause to be distributed) the appropriate Privacy Practices Notice to each individual who is our plan participant. If there is a change to the Privacy Practices Notice and we maintain a web site, we may (in lieu of distributing the revised Notice in paper form) prominently post the change or the revised Notice on our web site. If we do this, we will post the Notice or change by the effective date of the material change. We will also provide the revised Notice or information about the material change and how to obtain the revised Notice, in our next annual mailing to individuals then covered by the plan. We will also:
 - Disseminate our Notice to each new plan participant at enrollment.
 - Notify our then current plan participants, at least once every 3 years, that our Notice is available on request, explaining how the participants may obtain it.
 - Ensure that our Notice is prominently posted and electronically available on each web site the health plan maintains (if any) that provides information about our benefits.
 - Disseminate any revised Notice to our then current plan participants within 60 days of the material change. We will not implement the material change in our privacy practices before the effective date of our revised Notice (unless earlier implementation is required by law).
 - Furnish our Notice to any person on request.
 - Email our Notice to any individual who has agreed to electronic notification and not withdrawn that agreement. We must provide a paper copy of our Notice to the individual, if you know the individual failed to get the email transmission of our Notice or if the individual requests a paper copy.

12. Access.

Short Summary: Plan enrollees generally have the legal right to access their protected health information and obtain copies of it. Some new HIPAA rules from 2013 also allow the person to obtain an electronic copy of their protected health information in some situations.

- a) **POLICY—Right to Inspect and Copy.** We will allow an individual to inspect and to obtain a copy of his or her protected health information for as long as we or our business associates maintain that protected health information in designated record sets. We may withhold from an individual only that protected health information specified in Section 12(b) below. We may

charge a fee as allowed by law. We generally must respond to the individual's request for access within 30 days of us receiving the request.

If an individual makes an access request with respect to protected health information which is maintained electronically in our designated record set, the following rules shall apply:

- The individual shall have a right to obtain a copy of such information electronically and, if the individual requests, provide it in the form and format requested by the individual if it is readily producible in such form and format. If it is not so readily producible, we will provide it in a readable electronic form and format as agreed to by us and the individual.
 - The individual shall have a right to direct us to transmit the copy of protected health information directly to another person designated by the individual. We will follow such a direction if the individual's request is in writing, signed by the individual and clearly identifies the designated person and where to send the copy of protected health information.
 - Any fee that we may impose for providing the individual a copy of such information shall not be greater than our direct or indirect labor costs, supply costs or postage costs in responding to the request for the copy or for an explanatory summary of the protected health information.
 - We will send the information to an individual in an unencrypted email only if we warn the individual of the risks of unencrypted emails and the individual prefers the unencrypted email. We will provide the information on the individual's own external portable media only if we perform a risk analysis related to the potential use of the media and we conclude that there is an acceptable level of risk.
- b) **POLICY—Protected Health Information We May Withhold.** We may deny access to, and a copy of, protected health information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding. Other exceptions may also apply. We will consult our legal counsel if needed.
- c) **POLICY—Designations.** We must identify in writing each designated record set we maintain or that is maintained on our behalf by our business associates, and the titles of persons or offices responsible for receiving and processing access requests.

Use FORM 9 – Designated Personnel and Record Sets to identify our designated record sets.

13. **Amendment.**

Short Summary: Plan enrollees generally have the legal right to modify their protected health information that we (or our business associates) hold, if that protected health information is incorrect. We must promptly respond to such a request.

- a) **POLICY—Right to Amend.** We will allow an individual to request to amend his or her protected health information for as long as we or our business associates maintain the protected health information in designated record sets. We may deny an amendment request only as specified in Section 13(b) below. We will generally respond to the individual's request within 60 days of its receipt. If we make an amendment, we will notify our business associates that may have and rely on the unamended records.
- b) **POLICY—Bases for Denying Amendment Request.** We may decline to amend protected health information if:
- We did not create the information (unless the originator is no longer available to act on the request).

- The information to be amended is not part of a designated record set maintained by us or by a business associate on our behalf.
- The information is accurate and complete.

14. **Disclosure Accounting.**

Short Summary: Plan enrollees generally have the legal right to understand how their protected health information has been disclosed. However, as a practical matter, the vast majority of the disclosures do not need to be tracked by us or our business associates.

- a) **POLICY—Right to Disclosure Accounting.** We will allow an individual to request an accounting of each disclosure that we make of the individual's protected health information for up to 6 years prior to the request. We do not have to account for disclosures that are exempt from accounting as specified in Section 14(b) below. We will respond to the individual's request within 60 days. However, we will not provide a disclosure accounting if a law enforcement official asks us to temporarily not provide it.
- We may not charge for an individual's first accounting in any 12-month period. We may charge a reasonable, cost-based fee for other accountings within that same 12-month period.
 - **Use FORM 6** – Disclosure Log/Minimum Necessary to document each accountable disclosure.
 - The best way to respond to this request is to gather all the required disclosure accounting information from our records and from our business associates' records, then provide all this information to the individual. Alternatively, we may also be able to provide all of the disclosure accounting information we hold, then provide a list of all our business associates, including contact information for those business associates (such as work address, phone number and e-mail address). Before we do this, we would need to ensure the business associate has agreed to directly respond to the individual's request.
- b) **POLICY—Exempt Disclosures.** We do not have to account for the following:
- Disclosures made before our Privacy Rules compliance date (generally April 14, 2003 or April 14, 2004). Disclosure relating to an electronic designated record set generally all must be accounted for as of the date specified by HHS.
 - Disclosures made to the individual or the individual's personal representative.
 - Disclosures made for a payment related to that person's health care, or for health care operations.
 - Disclosures made pursuant to authorization.
 - Disclosures made in a limited data set.
- c) **POLICY—Accounting Information.** We will track accountable disclosures. The information that must be tracked to fulfill our disclosure accounting obligations is as follows:
- The disclosure date;
 - The name and, if known, address of each person or entity that received the disclosure;
 - A description of the protected health information disclosed; and
 - A statement of the purpose of the disclosure, or a copy of any written request for the disclosure from HHS or another government agency or organization to which the protected health information was disclosed pursuant to a public interest or benefit activity.

We will hold this information for 6 years.

15. Restriction Requests.

Short Summary: Plan enrollees generally have the legal right to request that we put restrictions on how their protected health information is used or disclosed. Except in very rare situations, we do not have to agree to this request (that is, we can deny the request). If we accept the request, we should inform our business associates of the new restriction.

- a) **POLICY—Restriction Requests.** We will allow an individual to request that we restrict our use or disclosure of his or her protected health information for treatment, payment, health care operations, or with specified family members or others. Except as noted below, we have no obligation to agree to such request. We will comply, and notify our business associates to comply, with any such agreement we make (except in an appropriate medical emergency). We will document any agreed-upon restriction request.

We will comply with a restriction request, and notify our business associates to comply, if:

- i) the disclosure is to a health plan for purposes of carrying out payment or health care operations and is not otherwise required by law; and
 - ii) the protected health information pertains solely to a health care item or service for which the individual or another person (other than a health plan on behalf of the individual) has paid the covered entity in full.
- b) **POLICY—Restriction Termination.** We may terminate a restriction agreement (other than a restriction agreement described in the prior sentence) either (i) with the concurrence of the individual or (ii) unilaterally by written notice of termination to the individual. When we terminate a restriction agreement unilaterally, we will continue to comply with the restriction with respect to protected health information we created or received subject to the restriction.

16. Confidential Communication.

Short Summary: Sometimes, plan enrollees may be in physical danger if we disclose protected health information in a certain way. For example, suppose our health plan wants to send an explanation of benefits ("EOB") to an employee's home. Suppose the EOB contains sensitive information that an employee is trying to keep from the employee's spouse. The employee may inform us that the employee fears for his / her physical safety if the spouse finds out the employee is being treated for a particular condition (and the EOB would reveal this). So, the employee requests that we (or our third party administrator) send the EOB to the employee's work. We generally must accommodate this type of request.

- a) **POLICY—Confidential Communication.** We will allow an individual to request confidential communications (that is, the use of alternative means or alternative locations when we communicate protected health information to the individual), if the request is reasonable and in writing, and the individual gives us a clear statement that all or part of the protected health information could endanger the individual if not communicated by the requested alternative means or to the requested alternative location.

IV. ADMINISTRATIVE REQUIREMENTS

17. Privacy Policies and Procedures.

Short Summary: Under HIPAA, our health plan must adopt these policies and procedures. You, as someone who works for the health plan (even if you are employed by the employer) must follow these policies and procedures.

- a) **POLICY—Adoption.** We will adopt and implement written privacy policies and procedures for protected health information designed to comply with our obligations under the Privacy Rules. These Privacy Policies and Procedures are intended to satisfy this obligation.
- b) **PROCEDURE—Implementation and Compliance.** Each member of our workforce with access to protected health information must, at all times, comply with the policies and follow the procedures set out in these Privacy Policies and Procedures.
- c) **POLICY—Revisions.** Only a designated person (e.g., plan administrator, plan fiduciary, Privacy Official, etc.) may change these Privacy Policies and Procedures.

18. Privacy Personnel, Training, Workforce Management, Administrative Practices.

Short Summary: There are certain administrative practices we must follow. For example, new employees who begin helping out with the plan and who will see protected health information must be trained on HIPAA. In addition, if an improper use or disclosure of protected health information occurs, we must take actions to minimize the harmful effect of that improper use or disclosure.

a) **POLICY—Privacy Personnel.**

- i) **Privacy Official.** Our Privacy Official is responsible for developing, maintaining, and implementing these Privacy Policies and Procedures, and for overseeing our full compliance with these Privacy Policies and Procedures, the Privacy Rules, and other applicable federal and state privacy law.

Our Privacy Official is:

Director of Human Resources
Telephone: 847-810-3530 Fax: 847-234-3675
E-mail: HR@cityoflakeforest.com
Office: 800 N. Field Drive, Lake Forest, IL 60045

- ii) **Contact Offices.** We will maintain contact offices for individuals to obtain our Privacy Practices Notice and other information on our privacy practices. Our contact offices will also accept complaints about our privacy practices.

Our contact offices are:

Department of Human Resources
800 N. Field Drive, Lake Forest, IL 60045

- b) **POLICY—Workforce Training.** Each member of our workforce who may have access to or use of protected health information will receive training on our Privacy Policies and Procedures, as necessary and appropriate for the member to carry out his or her job functions.

Use FORM 8 – Privacy Training Certificate to document each workforce member's completion of privacy training.

c) **PROCEDURE—Training Timing.**

- i) **New Members.** New members of our workforce must receive privacy training before they may have access to or use of protected health information.
- ii) **Retraining.** Existing workforce members must receive retraining within a reasonable period of time after there is material change in their job functions or in our Privacy Policies and Procedures that affects their access to or use of protected health information. We may also require periodic retraining even if there has not been any such change.

- d) **POLICY—Workforce Sanctions.** Workforce members who violate our Privacy Policies and Procedures, the Privacy Rules or other applicable federal or state privacy law will be subject to

disciplinary action, including employment termination, consistent with the sanctions developed, documented, and disseminated by our Privacy Official and the employer.

- e) **POLICY—Mitigation.** We will have and implement contingency plans to mitigate any deleterious effect of an improper use or disclosure of protected health information by a member of our workforce or by our business associates.
- f) **POLICY—Retaliatory Acts.** We will not attempt to intimidate, threaten, coerce, discriminate or retaliate against an individual who:
 - Exercises any right, including filing complaints, under the Privacy Rules.
 - Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by HHS or other appropriate authority.
 - Opposes any act or practice the individual believes in good faith is illegal under the Privacy Rules (provided the opposition is reasonable and does not involve illegal disclosure of protected health information).
- g) **POLICY—Waivers.** We will not require an individual to waive any right under the Privacy Rules, including the right to complain to HHS, as a condition of providing claims payment, enrollment or benefits eligibility to the individual.
- h) **POLICY—Documentation and Record Retention.** We will retain the documentation required by our Privacy Policies and Procedures and the Privacy Rules until 6 years after the later of its creation or last effective date. Our Privacy Official will be our repository of documentation regarding our privacy practices and compliance with our Privacy Policies and Procedures and the Privacy Rules.

19. **Data Safeguards.**

Short Summary: We must ensure that protected health information is kept secure. For example, any protected health information on paper generally should be kept locked up at night.

- a) **POLICY—Data Privacy Protection.** We will implement and comply with reasonable and appropriate administrative, physical, and technical safeguards to secure the privacy of protected health information against any intentional or unintentional use or disclosure in violation of these Privacy Policies and Procedures or the Privacy Rules. These safeguards will include reasonable limits to incidental uses or disclosures of protected health information made as a result of otherwise permitted or required uses or disclosures.
- b) **PROCEDURE—Data Privacy Protection.** Our Privacy Official, in conjunction with our legal advisers, will augment these Privacy Policies and Procedures with such additional data security policies and procedures as appropriate for our plan to have reasonable and appropriate administrative, physical and technical safeguards to ensure the integrity and confidentiality of the protected health information we maintain against any reasonably anticipated unauthorized use or disclosure, intentional or unintentional, or any reasonably anticipated threat or hazard to the privacy, security or integrity of the protected health information. These additional data security policies and procedures will ensure compliance by our workforce members with these Privacy Policies and Procedures, the Privacy Rules, and such other policies and procedures as may be adopted to implement our compliance obligations under the Privacy Rules.

20. **Complaints and HHS Enforcement.**

Short Summary: Plan enrollees have the legal right to complain if we are not following HIPAA. We must take those complaints seriously and try to resolve them. In addition, the federal government (usually the

Office for Civil Rights, a division of the U.S. Department of Health and Human Services) may audit the health plan to verify that we are following HIPAA.

- a) **POLICY—Complaints.** We will timely investigate and appropriately respond to each complaint received by our contact offices or a workforce member regarding our compliance with these Privacy Policies and Procedures or the Privacy Rules.
- b) **POLICY—HHS Enforcement and Compliance Cooperation.** We will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of our plan.

V. STATE LAW POLICIES AND PROCEDURES

21. State Privacy Law.

Short Summary: In some situations state privacy laws may go beyond what HIPAA requires. We should carefully consider whether we need to follow those additional requirements. We may take the position that other laws (such as ERISA, a federal law governing many health plans) supersede those state laws, so that we do not need to follow the state laws. If we do need to follow them, we will modify these Policies and Procedures to reflect those state laws.

- a) **POLICY—State Law Compliance.** We will comply with state privacy laws to the extent we are required to do so. If our group health plan is subject to ERISA, certain state privacy laws may be preempted. Our Privacy Official and legal advisers will determine which state privacy laws apply to our group health plan, whether those laws conflict with the Privacy Rules and, if so, whether those laws are more stringent than the Privacy Rules and therefore are not preempted by the Privacy Rules. A state law is more stringent than the Privacy Rules if it provides greater protections or rights to individuals or imposes greater restrictions on our use or disclosure of protected health information than the Privacy Rules.

VI. BREACH RULES

22. Identifying a Breach.

Short Summary: Sometimes we (or a business associate) may experience a "breach" of protected health information (e.g., a former employee takes protected health information with him or her and misuses it). The City must promptly report any such breach to the Privacy Official so we can act quickly.

- a) **POLICY – Identifying a Breach.** We will identify any suspected breach of protected health information and report a suspected breach to our Privacy Official.

FORM – Breach Identification. We will use **FORM 10**, Breach Identification, to identify a breach. We will record all individuals affected by a breach. We will record the list electronically or by using FORM 11, Log of Individuals Affected by Breach.

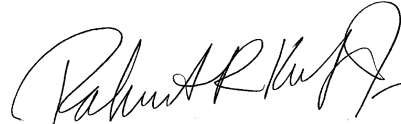
23. Notification Regarding Breach.

Short Summary: If there was a "breach" of protected health information (as discussed in Section 22), the health plan generally must notify the plan enrollees who were affected. The plan (generally, us, on behalf of the plan) must inform the U.S. Department of Health and Human Services of the breach.

- a) **POLICY – Notification Regarding Breach.** We will notify all relevant parties of a breach of protected health information, in accordance with HIPAA's rules. Relevant parties include the U.S. Department of Health and Human Services, affected individuals and, for certain large breaches affecting 500 or more individuals, local media.

FORM - Breach Notification. We will use **FORM 10** – Breach Identification and **FORM 12** – Notification to Affected Individuals of Breach when notifying relevant parties. We will create a separate notice to the media if so required. **FORM 13** – Media Notice. If a law enforcement official requests that we delay notice of a breach, we will document our consideration and, where applicable, acceptance of such delay. **FORM 14** – Law Enforcement Delay.

7. **Distribution.** Human Resources Website, www.citylf.org.



Robert R. Kiely, Jr.
City Manager