LAFAYETTE COLLEGE GROUP HEALTH PLAN
HIPAA (Health Insurance Portability and Accountability Act) Security Policy

Introduction

The Lafayette College Group Health Plan ("the Group Health Plan") is a fully insured group health plan sponsored by Lafayette College (the "Plan Sponsor"). The Group Health Plan provides benefits solely through an insurance contract with a health insurance issuer or health maintenance organization ("the Insurer"). Neither the Plan Sponsor nor any member of its workforce creates, receives, maintains, or transmits electronic protected health information (as defined below) on behalf of the Group Health Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology For Economic and Clinical Health Act ("HITECH Act") and their implementing regulations and guidance require the Group Health Plan to implement various security measures with respect to electronic protected health information (electronic PHI).

Specifically, the Group Health Plan will keep the Group Health Plan's electronic PHI secure in accordance with the HIPAA security regulations. It is the Group Health Plan's policy, working together with the Insurer, to:

- ☐ Ensure the confidentiality, integrity, and availability of the Group Health Plan's electronic PHI;
- ☐ Protect against any reasonably anticipated threats or hazards to the security or integrity of the electronic PHI;
- ☐ Protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted by HIPAA; and
- ☐ Ensure workforce compliance with the HIPAA security regulations and this policy.

Electronic protected health information or electronic PHI is protected health information that is transmitted by or maintained in electronic media.

Protected health information (PHI) is the information that is subject to and defined in the Group Health Plan's privacy policies and procedures. For purposes of this Policy, PHI does not include the following, referred to this Policy as "Exempt Information":

(1) summary health information, as defined by HIPAA's privacy rules, for purposes of (a) obtaining premium bids or (b) modifying, amending, or terminating the Group Health Plan;

(2) enrollment and disenrollment information concerning the Group Health Plan which does not include any substantial clinical information; or

(3) PHI disclosed to the Group Health Plan and/or Plan Sponsor under a signed authorization that meets the requirements of the HIPAA privacy rules.

Electronic Media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

It is the Group Health Plan's policy to comply fully with the requirements of HIPAA's security regulations.

No third-party rights (including but not limited to rights of Group Health Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Group Health Plan reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Group Health Plan. This Policy does not address requirements under state law or federal laws other than HIPAA.

I. Security Official

Cristie Lazart, Director Human Resources/Benefits is the Security Official for the Group Health Plan. The Security Official is responsible for the development and implementation of the Group Health Plan's policies and procedures relating to security, including but not limited to this Policy.

II. Risk Analysis

The Group Health Plan has no employees. Except for functions performed by the Plan Sponsor using Exempt Information, all of the Group Health Plan's functions, including creation and maintenance of its records, are carried out by the Insurer. The Group Health Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit, electronic PHI relating to the Group Health Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Insurer. Accordingly, the Insurer creates and maintains all of the electronic PHI relating to the Group Health Plan, owns or controls all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Group Health Plan, and has control of its employees, agents, and subcontractors that have access to electronic PHI relating to the

Group Health Plan. The Group Health Plan has no ability to assess or modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the Group Health Plan — that ability lies solely with the Insurer.

Because the Group Health Plan has no access to, or control over, the Insurer's employees, equipment, media, facilities, policies, procedures, or documentation affecting the security of electronic PHI relating to the Group Health Plan, and the Insurer is a covered entity that is responsible under HIPAA to implement security measures with respect to electronic PHI (including electronic PHI relating to the Group Health Plan), the Group Health Plan's policies and procedures (including this Policy) do not address the following standards (including the implementation specifications associated with them) established under HIPAA and set out in Subpart C of 45 CFR Part 164:

- security management process;
- workforce security; information access management; security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- business associate contracts and other arrangements; facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

The Insurer's own security policies and procedures for electronic PHI of the Group Health Plan are adopted by the Group Health Plan.

Because the Plan Sponsor has no access to electronic PHI relating to the Group Health Plan, the Group Health Plan is not required to include provisions regarding security in its plan document.

III. Risk Management

The Group Health Plan manages risks to its electronic PHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level, taking into account the following:

- ☐ The size, complexity, and capabilities of the Group Health Plan;
- ☐ The Group Health Plan's technical infrastructure, hardware, software, and security capabilities;
- ☐ The costs of security measures; and
- ☐ The criticality of the electronic PHI potentially affected.

Based on risk analysis discussed in Section II, the Group Health Plan made a reasoned, well-informed and good-faith determination on the implementation of the HIPAA security regulations that it need not take any additional security measures, other than the measures of the Insurer, to reduce risks to the confidentiality, integrity and availability of electronic PHI.

IV. Business Associates

To the extent that the Group Health Plan has Business Associates, it obtains signed Business Associate Contracts from all Business Associates in full compliance with HIPAA, the HITECH Act, and their implementing regulations and guidance. Business Associates must agree to use appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of the Group Health Plan's electronic PHI and otherwise meet all requirements under HIPAA, the HITECH Act, and their implementing regulations and guidance. The Group Health Plan does not, and will not, disclose electronic PHI to a Business Associate unless a Business Associate Agreement has been duly executed.

If the Security Official knows of acts or patterns of activity by a Business Associate that arc material violations of the Business Associate Agreement, the Security Official will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Security Official will determine, in consultation with legal counsel, whether termination of the Business Associate Agreement is feasible. If not feasible, the Security Official will report the violation to the US Department of Health and Human Services (HHS).

V. Breach Notification Requirements

The Group Health Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Group Health Plan or one of its business associates discovers a breach of unsecured PHI.

VI. Documentation

Except to the extent controlled by the Insurer, the Group Health Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of Group Health Plan electronic PHI and any changes in the HIPAA regulations. All changes to these policies or procedures will be documented promptly.

Except to the extent controlled by the Insurer, the Group Health Plan shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented.

Policies, procedures, and other documentation controlled by the Group Health Plan, may be maintained in either written or electronic form and will be maintained for at least six years from the date of creation or the date last in effect, whichever is later.

The Group Health Plan will make its policies, procedures, and other documentation available to the Security Official, the Insurer, and the Plan Sponsor, as well as other persons responsible for implementing the procedures to which the documentation pertains.