FCSRMC

FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

HIPAA Privacy Policy

March 1

2016

This document includes: HIPAA Privacy Policy Statement, HIPAA Manual and HIPAA Forms

Table of Contents

PRIVACY POLICY STATEMENT

Purpose: *The following privacy policy is adopted by the Florida College System Risk Management Consortium (FCSRMC) Health Program and its member colleges. FCSRMC functioning as the Group Health Plan and the member colleges functioning as the employer/plan sponsor complies fully with all federal and state privacy protection laws and regulations. Protection of patient privacy is of paramount importance to this organization. Violations of any of these provisions may result in severe disciplinary action including termination of employment and possible referral for criminal prosecution.*

The Privacy Policy and Procedures will be reviewed periodically and revisions made when necessary based on governmental, business organization, environmental, and/or other changes.

Effective Date: *This policy is in effect as of April 14, 2003*
Revised Date: March 1, 2016

Expiration Date: *This policy remains in effect until superseded or cancelled.*

Policy Owner: *FCSRMC Privacy Officer: Executive Director*

Assigning Privacy and Security Responsibilities

It is the policy of *FCSRMC and its member colleges* that specific individuals within our workforce are assigned the responsibility of implementing and maintaining the HIPAA Privacy requirements. Furthermore, it is the policy of *FCSRMC and its member colleges* that these individuals or their designee will be provided sufficient resources and authority to fulfill their responsibilities. At a minimum, it is the policy of *FCSRMC* that there will be one individual, Executive Director as the Privacy Officer and one Privacy Contact at each member college.

Uses and Disclosures of Protected Health Information

It is the policy of *FCSRMC and its member colleges* that protected health information may not be used or disclosed except when at least one of the following conditions is true:

1. The individual who is the subject of the information has authorized the use or disclosure.
2. The individual who is the subject of the information has received the Notice of Privacy Practices developed and distributed by Florida Blue thus allowing the use or disclosure and the use or disclosure is for treatment, payment or health care operations.
3. The individual who is the subject of the information agrees with the disclosure via the authorization form or a signed copy of this Privacy Policy and the disclosure is to persons involved in the processing or assistance of health care claims.
4. The disclosure is to the individual who is the subject of the information or to HHS for compliance-related purposes.
5. The use or disclosure is for one of the HIPAA “public purposes” (i.e. required by law, etc.).

Deceased Individuals

It is the policy of *FCSRMC and its member colleges* that privacy protections extend to information concerning deceased individuals.

Notice of Privacy Practices

Florida Blue as the Group Health Plan Third Party Administrators will publish and distribute a Notice of Privacy Practices to all the Group Health Plan participants for Blue Cross Blue Shield of FL, Health Options Inc., and Delta Dental for Dental participants.

Minimum Necessary Disclosure of Protected Health Information

It is the policy of *FCSRMC and its member colleges* that (except for disclosures made for

treatment or healthcare operation purposes) all disclosures of protected health information must be limited to the minimum amount of information needed to accomplish the purpose of the disclosure. It is the policy of *FCSRMC and its member colleges* that individuals have a right to request that no disclosure be made of PHI. FCSRMC and the member colleges are not obligated to grant the request. It is also the policy of this organization that all requests for protected health information will be directed to Florida Blue as the Third Party Administrators and must be limited to the minimum amount of information needed to accomplish the purpose of the request.

Access to Protected Health Information

It is the policy of *FCSRMC and its member colleges* that access to protected health information will only be granted to authorized employee(s) or contractor(s) who require access based on the assigned job functions of the employee or contractor. It is also the policy of this organization that such access privileges should not exceed those necessary to accomplish the assigned job function.

Appropriate Human Resource, Administrative, and Security personnel will be immediately notified when the access to Protected Health Information, security systems, software, and/or facilities is no longer necessary. This includes changes in job responsibilities, employment terminations, and changes to affiliations with business associates.

Access to Protected Health Information by the Individual

It is the policy of *FCSRMC and its member colleges* that access to protected health information must be granted to the person who is the subject of such information when such access is requested. Access requests should be directed to and will be processed by Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Group Health Plan Third Party Administrators.

Amendment of Incomplete or Incorrect Protected Health Information

It is the policy of *FCSRMC and its member colleges* that all requests for amendment of incorrect protected health information will be directed to and processed by Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information.

Access by Personal Representatives

It is the policy of *FCSRMC and its member colleges* that access to protected health information must be granted to personal representatives of individuals as though they were the individuals themselves. Personal representatives may include legal designations such as Power of Attorney or parent to a minor child. It is the policy of *FCSRMC and its member colleges* that all requests for access to protected health information will be directed to and processed by Blue Cross Blue Shield of FL, for Blue Cross Blue Shield of FL, Health Options, Inc., and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information.

Alternative Communications Channels

It is the policy of *FCSRMC and its member colleges* that all requests for alternative communication channels will be directed to and processed by Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information and that alternative communications channels be used, as requested by the individuals, to the extent possible.

Disclosure Accounting

It is the policy of *FCSRMC and its member colleges* that an accounting of all disclosures subject to such accounting of protected health information be given to individuals whenever such an accounting is requested. These requests should be directed to Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental as the Third Party Administrators and maintainer of the Protected Health Information.

Judicial and Administrative Proceedings

It is the policy of *FCSRMC and its member colleges* that information be disclosed for the purposes of a judicial or administrative proceeding only when: accompanied by a court or administrative order or grand jury subpoena; when accompanied by a subpoena or discovery request that includes either the authorization of the individual to whom the information applies, documented assurances that good faith effort has been made to adequately notify the individual of the request for their information and there are no outstanding objections by the individual, or a qualified protective order issued by the court. These requests should be directed to Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information.

De-Identified Data and Limited Data Sets

It is the policy of *FCSRMC and its member colleges* to disclose de-identified data only if it has been properly de-identified by removing all the relevant identifying data. We will make use of limited data sets, but only after the relevant identifying data have been removed and then only to organizations with which we have adequate data use agreements and only for research, public health, or health care operations purposes.

Authorizations

It is the policy of *FCSRMC and its member colleges* that a valid authorization will be obtained for all disclosures that are not related to treatment, payment, health care operations, for the individual or their personal representative. A signed copy of this Privacy Policy will serve as authorization for FCSRMC and/or the member colleges to provide assistance in resolving healthcare claims issues. If a signed copy of this Privacy Policy is not on file, the individual requesting assistance will be asked to sign the Privacy Policy. An individual will also need to submit a signed Authorization Form in the event that they want to grant authorization to a third party (e.g. a spouse or parent). When the college is requesting claim assistance, on behalf of an employee, from FCSRMC, a copy of the employee signed policy statement or authorization form must be forwarded to FCSRMC.

Complaints

It is the policy of *FCSRMC and its member colleges* that all complaints relating to the protection of health information be investigated and resolved in a timely fashion. Furthermore, it is the policy of FCSRMC that all complaints will be addressed to the college Privacy Contact for research and resolution. The Privacy Contact may involve FCSRMC and/or Florida Blue as needed to resolve a complaint. All complaints will be forwarded to FCSRMC's Privacy Officer for tracking purposes.

Prohibited Activities

It is the policy of *FCSRMC and its member colleges* that no employee or contractor may engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA regulations. It is also the policy of this organization that no employee or contractor may condition payment, enrollment or eligibility for benefits on the provision of an authorization to disclose protected health information. It is the policy of FCSRMC and its member colleges that PHI will **not** be used to make employment related decisions (e.g. hiring, terminations, promotions), except as allowed by federal law and regulation.

Responsibility

It is the policy of *FCSRMC and its member colleges* that the responsibility for designing and developing procedures to implement this policy lies with the Privacy Officer and/or the Privacy Contact where appropriate.

Verification of Identity

It is the policy of *FCSRMC and its member colleges* that the identity of all persons (including Business Associates) who request access to protected health information is reasonably verified before such access is granted.

Safeguards

It is the policy of *FCSRMC and its member colleges* that appropriate physical, technical, and administrative safeguards will be in place to reasonably safeguard Protected Health Information from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy Rule. These safeguards address PHI that is held or disclosed by the member college, including PHI transmitted on an electronic network.

Physical safeguards may include, but not be limited to, locked cabinets, locked doors, building alarm, workstation security (positioning monitor or utilizing screen protectors to prevent unauthorized individuals to view ePHI), and safe device disposal measures.

Technical safeguards may include, but not be limited to, data encryption/decryption software, firewalls, antivirus software, system access controls, unique user IDs/passwords, data backup, and integrity controls.

Administrative safeguards may include, but not be limited to, policies/procedures, risk analysis/management, security awareness, password management, establishment of Privacy and Security Officers, and Business Associate Agreements. These safeguards will extend to the oral communication of PHI.

Business Associates

It is the policy of *FCSRMC and its member colleges* that business associates must be contractually bound to protect health information to the same degree as set forth in this policy. A signed Business Associate Agreement will be obtained prior to release of Protected Health Information to the contracted party. This includes subcontractors that FCSRMC may utilize to provide activities related to Protected Health Information FCSRMC has obtained from another Covered Entity. It is also the policy of this organization that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate.

Training and Awareness

It is the policy of *FCSRMC and its member colleges* that all members of our workforce with likely access to protected health information have been trained by the compliance date on the policies and procedures governing protected health information and how *FCSRMC and its member colleges* complies with the HIPAA Privacy Rule. It is also the policy of *FCSRMC and its member colleges* that new members of our workforce receive training on these matters within a reasonable time after they have joined the workforce. It is the policy of *FCSRMC and its member colleges* to provide training should any policy or procedure related to the HIPAA Privacy Rule materially change. This training will be provided within a reasonable time after the policy or procedure materially changes. Furthermore, it is the policy of *FCSRMC and its member colleges* that training will be documented indicating participants, date and subject matter.

Sanctions

It is the policy of *FCSRMC and its member colleges* that sanctions will be in effect for any member of the workforce who intentionally or unintentionally violates any of these policies or any procedures related to the fulfillment of these policies.

Retention of Records

It is the policy of *FCSRMC and its member colleges* that the HIPAA Privacy Rule records retention requirement of six years from the date the policy was created or last in effect will be strictly adhered to. All records designated by HIPAA in this retention requirement will be maintained in a manner that allows for access within a reasonable period of time. This records retention time requirement may be extended at this organization's discretion to meet with other governmental regulations or those requirements imposed by our professional liability carrier. Florida Blue as the Third Party Administrators will retain the health insurance records of Plan Participants.

Cooperation with Privacy Oversight Authorities

It is the policy of *FCSRMC and its member colleges* that oversight agencies such as the Office for Civil Rights of the Department of Health and Human Services be given full support and cooperation in their efforts to ensure the protection of health information within this organization. It is also the policy of this organization that all personnel must cooperate fully with all privacy compliance reviews and investigations.

Emergency Access

In the event of an emergency or other occurrence such as fire, vandalism, terrorism, or natural disaster, the Security Official at the member college will give temporary access to systems containing ePHI to authorized staff if other personnel authorized to access ePHI is not available.

Response to Security Incident

An incident response process is implemented to detect, respond to and report security incidents (technical and non-technical), and to minimize loss and destruction. Through the incident response process, vulnerabilities found within the system(s) will be mitigated and information system functionality will be restored as soon as possible. Personnel who may respond to a security incident will include the Privacy Officer, Privacy Contact, Security Official, Human Resource Director, Administrator, Public Relations Representative, and Legal Counsel. All documentation related to the security incident including initial assessment, impact analysis, mitigation process, and post-incident follow up will be retained for a minimum of six years.

Internal/External Audits

Internal and/or external audits will be performed periodically to ensure proper processes are in place to protect against security breaches of PHI. Audit results will be provided to the FCSRMC Risk Manager, Privacy Officer, Privacy Contact, and other FCSRMC personnel as necessary. Appropriate measures will be taken if vulnerabilities exists to current systems or processes. Audit results and follow-up activity will be documented and maintained on file for a minimum of six years.

Information Security

FCSRMC and its member colleges will have a designated Informations System security person (Security Official) who will be responsible for maintaining the security of the system(s) and software(s) that contain PHI.

It is the policy of FCSRMC and its member colleges that staff requiring access to PHI will be given unique log-ins and passwords to systems/software containing PHI. Only staff assigned a unique log-in will be able to access such systems and access will be limited to the minimum necessary for job performance. Access to these systems/software programs will be immediately terminated when an individual terminates their employment with the entity.

FCSRMC and its member colleges will provide security awareness through the HIPAA training programs and via periodic security reminders. Such reminders may be posted to college intranets if available, or via email or memos to applicable staff.

A risk analysis will be conducted at member colleges periodically to ensure accurate measures are in place to protect ePHI. A risk analysis will also be conducted if there is a change in the business organization or environment that may render ePHI vulnerable to a breach. Results of the risk analysis will be provided to the FCSRMC Risk Manager, who will distribute to the Privacy Officer and other appropriate FCSRMC personnel. Threats or vulnerabilities identified through the risk analysis, and follow up action taken to mitigate risks to ePHI, will be documented and maintained on file for six years.

It is the policy FCSRMC and its member colleges that suspected or known security incidents will be immediately responded to and any harmful effects of such incident will be mitigated to the extent practicable. The security incident will be investigated by the

Privacy Contact and Privacy Officer, and measures put into place to prevent such incidents from reoccurring. All security incidents and their outcomes will be documented and maintained on file for six years.

It is the policy of FCSRMC and its member colleges that all electronic files containing PHI will be backed up on a daily basis. Any PHI lost through system errors, power outages, disasters, etc. will be restored via the backup tapes. The colleges shall acquire appropriate network-based and host-based intrusion detection systems. The IT Department shall be responsible for installing, maintaining, and updating such systems. To prevent transmission errors as data passes from one computer to another, the entity will use encryption, as determined to be appropriate, to preserve the integrity of data.

It is the policy of FCSRMC and its member colleges to take appropriate measures to remove the electronic protected health information (ePHI) stored on the computers, laptops, PDAs, or other media before its reuse. Depending on the circumstances, appropriate methods for removing ePHI from electronic media prior to reuse may be by clearing (using software or hardware products to overwrite media with non-sensitive data) or purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) the information from the electronic media.

It is the policy of FCSRMC and its member colleges that if the college removes or disposes of machines holding ePHI, including but not limited to computers, laptops, copiers, printers, scanners and fax machines, the college must retain or wipe the hard drive to ensure all PHI has been removed prior to disposal.

Acknowledgment of Receipt of Privacy Policy

I understand that this Privacy Policy will expire when I am no longer an employee covered by the health plan and all of my healthcare claims have been finalized.

I further understand that my ability to obtain treatment, my eligibility for benefits, etc. will not depend in any way on whether I sign this Privacy Policy or not. I understand however that FCSRMC and its member colleges may be limited in their ability to provide assistance if I do not sign this form.

I understand that I have a right to inspect and to obtain a copy of any information disclosed pursuant to this authorization.

Please sign and date below that you have received and had an opportunity to read the HIPAA Privacy Policy adopted by FCSRMC and its member colleges.

_____ _____

Employee Name Date

_____

Employee Signature

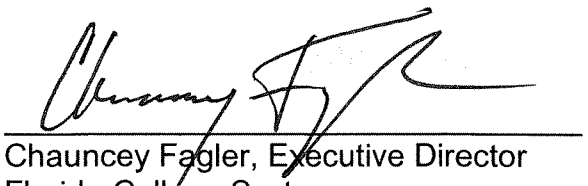
HIPAA PROCEDURES MANUAL

FCSRMC and its Member Colleges

This document contains the procedures to be followed by all workforce members and contractors of FCSRMC and its Health Plan member colleges to comply with privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Questions concerning the contents of this document should be referred to FCSRMC, Executive Director – Chauncey Fagler

THESE POLICIES AND PROCEDURES HAVE BEEN APPROVED AND ARE REVIEWED ANNUALLY BY THE FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM AND THE COMPLIANCE OFFICER AT EACH COLLEGE LOCATION.

2016

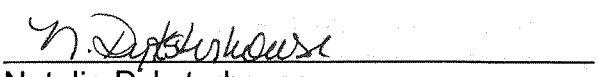


Chauncey Fagler, Executive Director
Florida College System
Risk Management Consortium

6/9/2016
Date

Robert Pralle, Associate Director
Compliance Officer's Signature

6/1/2016
Date



Natalie Dyksterhouse
Back–up Compliance Officer's Signature

6/1/16
Date

ACCESS REQUEST PROCESSING

Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc., Delta Dental for Dental as the Third Party Administrators for FCSRMC will process employee requests for access to protected health information for health and claims.

Actions To Be Taken For All Access Requests

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. If a college employee contacts FCCMRC and requests access to or copying of protected health information, the employee should be directed to Florida Blue as the Third Party Administrator. This is a service that will be provided by Florida Blue.

3. If a college employee contacts the college requesting access to or a copy of the protected health information, the college representative should inform the employee that the request should be directed to Florida Blue.

4. If one of the college contacts FCSRMC on behalf of an employee that is requesting access to or a copy of the protected health information, FCSRMC should inform the college representative that the request should be directed to Florida Blue.

5. In the event that an employee contacts Florida Blue and is not successful in obtaining access or a copy, the employee should notify the college Privacy Contact and inform them of the problem. The Privacy Contact will in turn notify FCSRMC of the problem.

AMENDMENT REQUEST PROCESSING

Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators for FCSRMC will process employee requests for amendments to protected health information for health and claims.

Actions To Be Taken For All Amendment Requests

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. If a college employee contacts FCSMRC and requests an amendment to protected health information, the employee should be directed to Florida Blue as the Third Party Administrators. This is a service that will be provided by Florida Blue.

3. If a college employee contacts the college requesting an amendment to the protected health information, the college representative should inform the employee that the request should be directed to Florida Blue.

4. If one of the college contacts FCSRMC on behalf of an employee that is requesting an amendment to protected health information, FCSRMC should inform the college representative that the request should be directed to Florida Blue.

5. In the event that an employee contacts Florida Blue and is not successful in obtaining an amendment, the employee should notify the college Privacy Point of Contact and inform them of the problem. The Privacy Point of Contact will in turn notify FCSRMC of the problem.

COMPLAINT PROCESSING

Actions To Be Taken For All Complaints

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. If FCSRMC receives a complaint directly from a college employee, a copy should be sent to the college Privacy Contact. The complaint must be submitted on the Complaint Form and have all of the required information noted.

3. If the complaint is about an incident that occurred at Florida Blue, the Complaint Form should be sent to FCSRMC for submission to Florida Blue for research and resolution. Florida Blue will research the complaint and keep FCSRMC informed as to the resolution.

4. If the complaint is about an incident that occurred at the college, the college Privacy Contact should research the complaint and generate the Response to Complaint Form and the Compliant Tracking Information Form. Copies of all forms (Complaint Form, Response to Complaint Form and Complaint Tracking Information Form) should be sent to the FCSRMC Privacy Officer.

5. If the complaint is about an incident that occurred at FCSRMC, the Privacy Officer or their designee will research the issue and generate the Response to Complaint Form and the Complaint Tracking Information Form.

Actions To Be Taken When No Compliance Violation Is Found

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. If you determine that, there has been no violation of FCSRMC and its member colleges' privacy policies, then document these findings on the complaint form.

3. Contact the employee and explain your findings; also provide the individual with a written record of the complaint resolution.

4. Document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the complaint form.

5. If the individual is dissatisfied with the disposition of his or her complaint, refer this matter to FCSRMC Privacy Officer.

6. Copies of all complaints processed by the colleges should be sent to FCSRMC.

Actions To Be Taken When A Compliance Violation Is Found

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. If you determine that a violation of FCSRMC and its member colleges' privacy policies has occurred, document this fact on the complaint form.

3. If the violation took place at FCSRMC and its member colleges and is an employee violation, the employee should be sanctioned according to the policies outlined in the HIPAA Privacy Training document.

4. Contact the individual who filed the complaint and explain your findings; also provide the individual with a written record of the complaint resolution.

5. Document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the complaint form.

6. If the individual is dissatisfied with the disposition of his or her complaint, refer this matter to FCSRMC Privacy Officer.

7. Copies of all complaints processed by the colleges should be sent to FCSRMC.

DISCLOSURE ACCOUNTING REQUEST PROCESSING

Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators for FCSRMC will track disclosures of protected health information for health and claims.

Actions To Be Taken For Disclosure Accounting Requests

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. If a college employee contacts FCSRMC and requests an accounting of disclosures of protected health information, the employee should be directed to Florida Blue as the Third Party Administrators. This is a service that will be provided by Florida Blue.

3. If an employee, contacts the college requesting an accounting of disclosures of protected health information, the employee should be directed to Florida Blue as the Third Party Administrators. This is a service that will be provided by Florida Blue.

4. If one of the colleges contacts FCSRMC on behalf of an employee that is requesting an accounting of disclosures of protected health information, FCSRMC should inform the college representative that the request should be directed to Florida Blue.

5. In the event that an employee contacts Florida Blue and is not successful in obtaining an accounting of disclosures, the employee should notify the college Privacy Contact and inform them of the problem. The Privacy Contact will in turn notify FCSRMC of the problem.

INDIVIDUAL PERMISSION

Actions To Be Taken When Obtaining Written Authorization

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. All employees will be sent a copy of the Privacy Policy by the Colleges and will be asked to sign the policy and return it to the Privacy Contact at each college.

3. If an employee contacts their Privacy Contact at the college to request assistance with a healthcare claim issue and PHI access will be required by the college representative, there must either be a signed copy of the Privacy Policy on file or the employee will be asked to sign the Privacy Policy granting authorization for access to PHI.

4. If an employee contacts FCSRMC to request assistance with a healthcare claim issue and PHI access will be required by FCSRMC, FCSRMC will contact the college and request a copy of the Privacy Policy (with the individual's signature).

5. If the college contacts FCSRMC on behalf of an employee, a copy of the signed Privacy Policy or the authorization form (for third party authorizations) whichever is appropriate will be forwarded to FCSRMC by the member college.

INFORMATION DISCLOSURES

Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators for FCSRMC or the individual's physician will likely be the primary contacts for PHI information disclosure required by law enforcement. These procedures will apply under circumstances where FCSRMC or the colleges is contacted directly by Law Enforcement.

Actions To Be Taken When Disclosing Information to Law Enforcement

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. If a law enforcement agency contacts FCSRMC and/or a member college and requests disclosures of employee protected health information, the agency should be directed to Florida Blue as the Third Party Administrators or to the individual's physician.

3. If one of the colleges contacts FCSRMC on behalf of a law enforcement agency requesting a disclosure of protected health information, FCSRMC will advise the college representative that the request should be directed to Florida Blue or to the individual's physician.

4. In the event that a law enforcement agency contacts Florida Blue and is not successful in obtaining a disclosure of PHI, the agency should notify the college Privacy Point of Contact and inform them of the problem. The Privacy Point of Contact will in turn notify FCSRMC of the problem.

Actions To Be Taken When Disclosing Information For A Judicial Or Administrative Proceeding

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

    2. If FCSRMC and/or a member college is presented with a court order, grand jury subpoena, or administrative order, with a request for

disclosures of employee protected health information, the agency should be directed to Florida Blue as the Third Party Administrators or to the individual's physician.

3. If FCSRMC and/or a member college is presented with a lawyer's subpoena or discovery request, the firm should be directed to Florida Blue as the Third Party Administrators or to the individual's physician.

4. If one of the colleges contacts FCSRMC, for a judicial or administrative procedure, requesting a disclosure of protected health information, FCSRMC will advise the college representative that the request should be directed to Florida Blue or to the individual's physician.

5. In the event that a firm contacts Florida Blue, for a judicial or administrative procedure, and is not successful in obtaining a disclosure of PHI, the firm should notify the college Privacy Point of Contact and inform them of the problem. The Privacy Point of Contact will in turn notify FCSRMC of the problem.

Actions To Be Taken When Disclosing Information To The Individual

This procedure is documented in the Procedures for Access Request section of this manual.

Actions To Be Taken When Disclosing Information To The Department Of Health and Human Services as Part Of A Compliance Review

FCSRMC and its member colleges must cooperate fully with the Department of Health and Human Services (DHHS) when conducting compliance reviews. Answer all questions put to you by DHHS compliance investigators. Provide access to DHHS personnel to all requested records.

Actions To Be Taken When Disclosing Information About Deceased Individuals

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. Disclose information about deceased individuals to law enforcement only when they are suspected to be victims of a crime (or required to by court order or for purposes of identifying the perpetrator of a crime).

3. In all other cases, treat deceased individuals exactly as living individuals for purposes of information disclosures.

Actions To Be Taken When Disclosing Information About Minors To Their Parents Or Guardians.

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. Determine if the parent or guardian is a personal representative. See the privacy official or the Personal Representative section of this manual to make that determination. If so, treat the parent or guardian as any other personal representative. If not, continue with the rest of this procedure.

3. Determine if state, local, case, or other applicable law requires that the information be disclosed to the parents or guardians. (See your privacy official, who may then consult an attorney) If so, disclose the information

4. Determine if state, local, case, or other applicable law explicitly permits the information to be disclosed to the parents or guardians. (See your privacy official, who may then consult an attorney) If so, disclose the information as necessary.

5. Determine if state, local, case, or other applicable law forbids the information to be disclosed to the parents or guardians. (See your privacy official, who may then consult an attorney) If so, do *not* disclose the information.

If state, local, case, or other applicable law is completely silent on the issue, our legal counsel must make a professional judgment whether to allow, disclose, or forbid the information.

NOTICE AND ACKNOWLEDGEMENT

Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators for FCSRMC will produce and distribute the Notice of Privacy Practices for all FCSRMC enrollees.

Personal Representatives

Actions To Be Taken When Dealing With Personal Representatives

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. Recognize the circumstances when a personal representative relationship exists. These circumstances include:

    - If the person has the authority to act on behalf of the individual in making health care decisions (See FCSRMC's Privacy Officer and/or the Privacy Contact at the member college if you have any questions). The privacy official will contact an attorney if necessary.
    - The executor or Administrators of a deceased person's estate is automatically a personal representative of the deceased individual.
    - A parent, guardian, or other person acting *in loco parentis* of an un-emancipated minor is automatically a personal representative unless:

3. Validate the personal representative relationship. This can be done by requesting the last four digits of the social security number of the individual enrollee. Otherwise, obtain verification of the relationship between the two (such as a power of attorney).

4. Personal representatives should be indicated on the Authorization Form.

TRAINING

Actions To Be Taken For Initially Training The Workforce

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. Complete an up to date listing of staff and their job descriptions. This will include independent contractors and temporary office staff.

3. Identify the staff positions that will require HIPAA privacy training.

4. Create a training program that will adequately train the staff and train each member of the staff in the topics which they must learn. Record each training session in a workforce training log

Actions To Be Taken For Training New Workforce Members

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. Give new staff as well as temporary staff a basic orientation in the policies and procedures related to their job function.

3. Ensure that new FCSRMC and member college staff completes training within 30 days of their start date.

4. Make entries for each training session in the work force training log.

Actions To Be Taken For Ongoing Training Of The Workforce

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. FCSRMC's PRIVACY OFFICER AND LEGAL COUNSEL HAVE REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE PRIVACY POLICY ADOPTED BY FCSRMC AND ITS HEALTH PLAN MEMBER COLLEGES. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT FCSRMC PRIVACY OFFICER OR THE COLLEGE PRIVACY CONTACT BEFORE CONTINUING.

2. Keep up to date a quick training reference guide.

3. Include a HIPAA awareness-training component in periodic staff meetings.

4. FCSRMC's Privacy Officer will maintain the workforce-training log. The member college's Privacy Contact will forward copies of the colleges training logs to FCSRMC's Privacy Officer.

AUTHORIZATION FOR THE USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

Florida College System Risk Management Consortium (FCSRMC) and it's Member Colleges

As required by the Health Insurance Portability and Accountability Act (HIPAA) of 1996, FCSRMC and its member colleges may not use or disclose your health information except as provided in our Notice of Privacy Practices without your authorization. The Notice of Privacy Practice was sent to you from Blue Cross Blue Cross Blue Shield of FL. Your signature on this form indicates that you are giving permission for the uses and disclosures of Protected Health Information described herein. You may revoke this authorization at any time by signing and dating the revocation section on your copy of this form and returning to this office.

EMPLOYEE INFORMATION:

EMPLOYEE'S NAME

_____

Last **First** **M.I.**

ADDRESS

_____

BIRTHDATE _____/_____/_____ **DAYTIME TELEPHONE NUMBER** _____

Month **Day** **Year**

SOCIAL SECURITY NO. _____

AUTHORIZATION:

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that treatment, payment, enrollment or eligibility of benefits may **not** be conditioned on my signing this authorization except as provided by law.

RELEASE FROM LIABILITY:

I FURTHER UNDERSTAND THAT IF THE ENTITY/PERSON AUTHORIZED TO RECEIVE THE INFORMATION IS NOT A HEALTH PLAN OR HEALTH CARE PROVIDER, THE RELEASED INFORMATION COULD POTENTIALLY BE RE-DISCLOSED AND MAY NO LONGER BE PROTECTED BY FEDERAL PRIVACY REGULATIONS. THEREFORE, I RELEASE FCSRMC AND IT'S MEMBER COLLEGES FROM ANY AND ALL LEGAL LIABILITY THAT MAY ARISE FROM WHAT THE PARTY NAMED BELOW DOES WITHIN THE PHI.

ENTITY/PERSON RECEIVING INFORMATION:

(NAME OF PERSON OR ENTITY RECEIVING INFORMATION)

STREET ADDRESS

CITY **STATE** **ZIP CODE**

INFORMATION TO BE DISCLOSED:

☐ All records containing PHI **OR**

☐ Demographic/Insurance Information ☐ Lab/Diagnostic Test Reports ☐ FMLA Forms

☐ Physician Notices/Reports ☐ Other (please specify):_____

PURPOSE OF DISCLOSURE:

☐ Second Opinion ☐ Continuing Medical Treatment ☐ Employee Request

☐ Marketing Promotion: I have been informed that FCSRMC __is __ is not receiving direct or indirect compensation from a third party as a result of disclosing information for this purpose.

☐ Other (please specify):

_____

I understand that this authorization will expire one (1) year from the date of signature on this form.

RIGHT TO REVOKE AUTHORIZATION:

I MAY REVOKE THIS AUTHORIZATION AT ANY TIME, IN WRITING TO THE PRACTICE, BEFORE THE INFORMATION HAS BEEN RELEASED. I FURTHER UNDERSTAND THAT I HAVE A RIGHT TO RECEIVE A COPY OF THIS AUTHORIZATION UPON REQUEST.

Authorization Copy Received: ☐ Yes ☐ No

SIGNATURE:

BY SIGNING THIS AGREEMENT, I ACKNOWLEDGE THAT I HAVE CAREFULLY READ, UNDERSTAND AND AGREE TO THE ABOVE TERMS AND CONDITIONS.

Date: _____

Employee Signature: _____

Parent, Guardian or Legal Representative Signature:_____

Printed Name of Parent, Guardian or Legal Representative:_____

Relationship to Employee:_____

Legal Representative's Authority to Act for Patient (Power of Attorney, Healthcare Surrogate, etc.):

_____

Witness Signature:_____

Rev. 3/1/16

Complaint Form

FCSRMC and its Member Colleges

As required by the Health Information Portability and Accountability Act of 1996 (HIPAA) you have a right to complain about our privacy policies, procedures or actions. Florida College System Risk Management Consortium (FCSRMC) and its member colleges will not engage in any discriminatory or other retaliatory behavior against you because of this complaint. Please be as thorough and forthright as possible, and return it to our Privacy Officer listed above.

Please complete the sections below:

Name:
Address:
Phone:
E-mail Address:
What is the best way to reach you?
What are the best hours to reach you?

Details of your complaint: *(Please be as specific as possible with dates, times and the specific policy, procedure or action taken; include the names, if any, of any one in the office with whom you discussed this. Use the other side of this form if you need more room. Attach any relevant documents.)*

Documents attached include:

Signed: _____ Date: _____

Print Name: _____ Telephone: _____

If not signed by the individual, please indicate:

Relationship:

- ☐ parent or guardian of minor
- ☐ guardian or conservator of an incompetent member
- ☐ beneficiary or personal representative of deceased member
- ☐ other (specify)

Name of individual member:

Please return this form to the colleges Privacy Officer.

Response to Complaint

FCSRMC and its Member Colleges

Dear_____:

Action on your complaint, dated _____ (attached) has been completed.

We have investigated your concern and have concluded that your concern is: (*Choose one of the following*)

☐ Not warranted, for the following reason:

_____

_____

_____

_____

☐ Warranted. We have taken the following steps to reduce any harm you may have suffered: _____

_____

We have taken the following steps to reduce the likelihood this will happen again:

_____

_____

Sincerely,

_____

Signature

_____ _____

Print name *Date*

NOTE: *If you believe your rights have been violated, you may file an appeal with FCSRMC or file a complaint the Secretary of the Department of Health and Human Services. You will not be penalized for filing an appeal or a complaint.*

Complaint Tracking Information

Name of Individual:

_____

Address:

_____

_____

For Office Use Only:

Date received:	Processed by:
Review Date:	Response Date:
Follow-up: ☐ Yes ☐ No	Date of Follow-up:

Reviewer's Comments:

_____

_____

Action Taken:

_____

_____

_____

_____

FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM (FCSRMC)

BUSINESS ASSOCIATE AGREEMENT

THIS **BUSINESS ASSOCIATE AGREEMENT** (this "Agreement") is made as of _____, 2014 (the "Effective Date") by and between **Florida College System Risk Management Consortium (FCSRMC)** ("Covered Entity") and _____ ("Business Associate"), each individually a "Party" and collectively the "Parties."

BACKGROUND

A. **Purpose**. The purpose of this Agreement is to comply with the requirements of (i) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the associated regulations, the HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164, as may be amended (the "Privacy Rule"), the HIPAA Security Rule, 45 C.F.R. Parts 160, 162 and 164, as may be amended (the "Security Rule"), and (ii) the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH Act"). Unless otherwise defined in this Agreement, capitalized terms have the meanings given in the Privacy Rule, the Security Rule, and the HITECH Act. The Privacy and Security Rules require a Covered Entity obtain written assurances from Business Associate that Business Associate will appropriately safeguard Protected Health Information ("PHI"). The HITECH Act provides further protection for the privacy and security of PHI used and disclosed through health information technology.

B. **Relationship**. Covered Entity and Business Associate have entered into an agreement under which Business Associate may receive, use, obtain, access or create PHI from or on behalf of Covered Entity in the course of providing services (the "Services") for Covered Entity.

The Parties agree as follows:

1. **Permitted Uses and Disclosures**. Business Associate may use and/or disclose PHI only as permitted or required by this Agreement, or as otherwise required by law. Business Associate may disclose PHI to, and permit the use of PHI by, its employees, contractors, agents, or other representatives only to the extent directly related to and necessary for the performance of the Services. Business Associate will request from Covered Entity no more than the minimum PHI necessary to perform the Services. Business Associate will not use or disclose PHI in a manner (i) inconsistent with Covered Entity's obligations under the Privacy Rule, the Security Rule or the HITECH Act, or (ii) that would violate the Privacy Rule, the Security Rule, or the HITECH Act if disclosed or used in such a manner by Covered Entity. Business Associate may use PHI for the proper management and administration of Business Associate's business and to carry out its legal

responsibilities. Business Associate may disclose PHI for its proper management and administration in accordance with 45 C.F.R. § 164.504(e)(4).

2. **Safeguards for the Protection of PHI**. Business Associate will implement and maintain appropriate safeguards to ensure that PHI obtained by or on behalf of Covered Entity is not used or disclosed by Business Associate in violation of this Agreement. Such safeguards shall be designed to protect the confidentiality and integrity of such PHI obtained accessed or created from or on behalf of Covered Entity. Security measures maintained by Business Associate to protect electronic PHI shall include administrative safeguards, physical safeguards, and technical safeguards as necessary to protect such PHI. Upon request by Covered Entity, Business Associate shall provide a written description of such safeguards.

3. **Reporting and Mitigating the Effect of Unauthorized Uses and Disclosures**. If Business Associate has knowledge of any use or disclosure of PHI not provided for by this Agreement, then Business Associate will promptly notify Covered Entity in accordance with Section 10.8. Business Associate will establish and implement procedures and other reasonable efforts for mitigating, to the extent possible, any harmful effects arising from any improper use and/or disclosure of PHI of which it becomes aware. Furthermore, in the event Business Associate becomes aware of a security incident involving PHI, by itself or any of its agents or subcontractors, Business Associate shall promptly notify Covered Entity in writing, of such security incident. Business Associate shall identify the: (i) date of the security incident; (ii) scope of the security incident; (iii) Business Associate's response to the security incident; and (iv) identification of the party responsible for the security incident, if known. Covered Entity and Business Associate agree to act together in good faith to take reasonable steps to investigate and mitigate any harm caused by such unauthorized use or security incident. For these purposes, a "security incident" shall have the same meaning set forth in the Security Rule: "a security incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

4. **Data Breach Notification and Mitigation**. Business Associate agrees to promptly notify Covered Entity of any "breach" of "unsecured PHI" as those terms are defined by 45 C.F.R. §164.402 (hereinafter a "Data Breach"). The parties acknowledge and agree that 45 C.F.R. §164.404, as described below in this Section, governs the determination of the date of a Data Breach. Business Associate will, following the discovery of a Data Breach, promptly notify Covered Entity and in no event later than fifteen (15) calendar days after Business Associate discovers such Data Breach, unless Business Associate is prevented from doing so by 45 C.F.R. §164.412 concerning law enforcement investigations. For purposes of reporting a Data Breach to Covered Entity, the discovery of a Data Breach shall occur as of the first day on which such Data Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. Business Associate will be considered to have had knowledge of a Data Breach if the Data Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the Data

Breach) who is an employee, officer or other agent of the Business Associate. No later than thirty (30) calendar days following a Data Breach, Business Associate shall provide Covered Entity with sufficient information to permit Covered Entity to comply with the Data Breach notification requirements set forth at 45 C.F.R. §164.400 et seq. Specifically, if the following information is known to (or can be reasonably obtained by) the Business Associate, Business Associate will provide Covered Entity with: (i) contact information for individuals who were or who may have been impacted by the Data Breach (e.g., first and last name, mailing address, street address, phone number, email address); (ii) a brief description of the circumstances of the Data Breach, including the date of the Data Breach and date of discovery; (iii) a description of the types of unsecured PHI involved in the Data Breach (e.g., names, social security number, date of birth, address(es), account numbers of any type, disability codes, diagnostic and/or billing codes and similar information); (iv) a brief description of what the Business Associate has done or is doing to investigate the Data Breach, mitigate harm to the individual impacted by the Data Breach, and protect against future Data Breaches; and (v) appoint a liaison and provide contact information for same so that the Covered Entity may ask questions or learn additional information concerning the Data Breach. Following a Data Breach, Business Associate will have a continuing duty to inform Covered Entity of new information learned by Business Associate regarding the Data Breach, including but not limited to the information described in items (i) through (v), above.

5. **Liability.**. Business Associates are directly liable for: (a) uses and disclosures that violate its business associate agreement *or* the Privacy Rule; (b) failing to disclose to the Secretary when required to do so; (c) failing to disclose as necessary to accommodate an individual's request for electronic copy of his or her PHI; (d) failing to make reasonable efforts to limit PHI to the minimum necessary; and (e) failing to enter into business associate agreements with subcontractors.

Under the HIPAA rule, Business Associates must: (a) keep such records and submit such compliance reports as the Secretary may determine necessary to ascertain compliance; (b) cooperate with the Secretary in any compliance investigation; (c) permit access by the Secretary during normal business hours to facilities, books, records, accounts and other sources of information; and (d) comply with the HIPAA Security Rule

6. **Use and Disclosure of PHI by Subcontractors, Agents, and Representatives**. Business Associate agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information, in accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2).

7. **Individual Rights**. Business Associate will comply with the following individual rights requirements as applicable to PHI used or maintained by Business Associate:

7.1. Right of Access. Business Associate agrees to provide access to PHI maintained by Business Associate in a Designated Record Set, at request of Covered Entity and in the time and manner designated by Covered Entity, to Covered Entity or, as directed, to an individual in order to meet the requirements under 45 C.F.R. §164.524.

7.2. Right of Amendment. Business Associate agrees to make any amendment(s) to PHI maintained by Business Associate in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. §164.526 at the request of Physician or an individual, and in the time and manner designated by Covered Entity.

7.3. Right to Accounting Disclosures. Business Associate agrees to document such disclosures of PHI as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528. Business Associate agrees to provide to Covered Entity or an individual, in the time and manner designated by Covered Entity, such information collected in order to permit Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528.

8. **Inspection of Books and Records**. Business Associate will make its internal practices, books, records, and policies and procedures relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the federal Department of Health and Human Services ("HHS"), the Office of Civil Rights ("OCR"), or their Agents or to Covered Entity for purposes of monitoring compliance with the Privacy Rule, the Security Rule and the HITECH Act.

9. **Term and Termination**

9.1. Term. This Agreement will commence on the Effective Date. Unless terminated sooner pursuant to Section 9.2, this Agreement shall remain in effect for the duration of all Services provided by Business Associate and for so long as Business Associate shall remain in possession of any PHI received by Business Associate on behalf of Covered Entity, unless Covered Entity has agreed in accordance with Section 9.3 that it is infeasible to return or destroy all PHI.

9.2. Termination. Covered Entity may immediately terminate this Agreement if Covered Entity determines that Business Associate has breached a material term of this Agreement and Business Associate has failed to cure the material breach within 30 days after receipt of written notice from Covered Entity. Covered Entity may also report the material breach to the Secretary of HHS or OCR.

9.3. Effect of Termination. Upon termination of this Agreement, Business Associate will recover any PHI relating to this Agreement in possession of its subcontractors, agents, or representatives. Business

Associate will return to Covered Entity or destroy all such PHI plus all other PHI relating to this Agreement in its possession, and will retain no copies. If Business Associate believes that it is not feasible to return or destroy the PHI as described above, Business Associate shall notify Covered Entity in writing. The notification shall include: (i) a written statement that Business Associate has determined that it is infeasible to return or destroy the PHI in its possession, and (ii) the specific reasons for such determination. If the Parties agree that Business Associate cannot feasibly return or destroy the PHI, Business Associate will ensure that any and all protections, requirements and restrictions contained in this Agreement will be extended to any PHI retained after the termination of this Agreement, and that any further uses and/or disclosures will be limited to the purposes that make the return or destruction of the PHI infeasible. Notwithstanding anything in this Agreement to the contrary, Business Associate shall not be required to return to Covered Entity the medical records of Business Associate that document services even though such records contain PHI.

10. **Miscellaneous**.

10.1. Survival. The respective rights and obligations of the Parties under Section 8 (Inspection of Books and Records), Section 9.3 (Effect of Termination), and Section 10 (Miscellaneous) will survive termination of this Agreement indefinitely.

10.2. Amendments; Waiver. This Agreement constitutes the entire agreement between the Parties with respect to its subject matter. It may not be modified, nor will any provision be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one (1) event will not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

10.3. Compliance with Privacy Rule. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule. The Parties agree to amend this Agreement from time to time as necessary for Covered Entity to comply with the requirements of the Privacy Rule and HIPAA.

10.4. Compliance with the Security Rule. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Security Rule. The Parties agree to amend this Agreement from time to time as necessary for Covered Entity to comply with the requirements of the Security Rule and HIPAA.

10.5. Compliance with the HITECH Act. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HITECH Act. The Parties agree to amend this Agreement from time to time as necessary for Covered Entity to comply with the requirements of the HITECH Act.

10.6. Governing Law; Venue. This Agreement shall be governed by and construed in all respects by the laws of the State of Florida.

10.7. No Third Party Beneficiaries. Except as provided in Section 4, nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors and permitted assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

10.8. Notices. Any notice to be given under this Agreement to a Party shall be made via U.S. Mail, commercial courier or hand delivery to such Party at its address given below, and/or facsimile to the facsimile telephone number listed below, or to such other address or facsimile number as shall hereafter be specified by notice from the Party. Any such notice shall be deemed given when so delivered to or received at the proper address.

If to Covered Entity:

Florida College System Risk Management Consortium (FCSRMC)
4500 NW 27th Avenue, Suite D2
Gainesville, FL 32206
Attn: Natalie Dyksterhouse

If to Business Associate:

_____

_____

_____

Attn:_____

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement effective as of the date first above stated.

Covered Entity:	**Business Associate:**
Florida College System Risk	_____
Management Consortium	
By:_____	By:_____
Its: Office Manager	Its: Administrator

PRIVACY OFFICER/PRIVACY CONTACT

Purpose: *The Privacy Officer/Privacy Contact role and responsibilities are established pursuant to the Privacy Policy Statement adopted by the Florida College System Risk Management Consortium's (FCSRMC) Health Program and its member colleges. FCSRMC functioning as the Group Health Plan and the member colleges functioning as the employer/plan sponsor complies fully with all federal and state privacy protection laws and regulations. Protection of patient privacy is of paramount importance to this organization.*

Role

It is the policy of *FCSRMC and its member colleges* that specific individuals within our workforce are assigned the responsibility of implementing and maintaining the HIPAA Privacy requirements. Furthermore, it is the policy of *FCSRMC and its member colleges* that these individuals or their designee will be provided sufficient resources and authority to fulfill their responsibilities. At a minimum it is the policy of *FCSRMC* that there will be one individual, Executive Director as the Privacy Officer and one Privacy Contact at each member college.

The role addressed herein applies to the Privacy Officer; and, to a lesser degree, the Privacy Contact. Under the role of Privacy Officer, accountability extends across the entire consortium as applicable. However, under the role of Privacy Contact, accountability is restricted to the individual member college.

Privacy Officer/Executive Director

1. The Privacy Officer serves in a leadership role for Privacy Oversight activities.
2. The Privacy Officer will Chair and/or provide leadership to *FCSRMC and its member colleges'* Operations Committee.
3. The Privacy Officer serves as information privacy consultant to *FCSRMC and its member colleges*.
4. The Privacy Officer will serve *FCSRMC and its member colleges* as a liaison to regulatory and accrediting bodies for matters relating to privacy at the Consortium level.

Responsibilities

The responsibilities addressed herein apply to the Privacy Officer and extend across the Consortium.

1. The Privacy Officer provides leadership in the planning, design, and evaluation of FCSRMC and its member colleges' privacy and security related projects.
2. The Privacy Officer provides development guidance and assists in the identification, implementation, and maintenance of FCSRMC

and its member colleges' Protected Health Information (PHI) privacy policies and procedures in coordination with member colleges, Consortium Compliance Officer, Legal Counsel and Florida Blue as the Third Party Administrators.

3. The Privacy Officer initiates, facilitates and promotes activities to foster information privacy awareness within *FCSRMC and its member colleges*.
4. The Privacy Officer establishes an internal privacy audit program to ensure Consortium-wide compliance to *FCSRMC and its member colleges'* privacy policies.
5. The Privacy Officer periodically revises the privacy program in light of changes in laws, regulations, or *FCSRMC and its member colleges'* policy.
6. The Privacy Officer maintains current knowledge of applicable Federal and State privacy laws to ensure *FCSRMC and its member colleges'* adaptation and compliance.
7. The Privacy Officer cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
8. The Privacy Officer works with *FCSRMC and its member colleges,* Legal Counsel, Consortium Compliance Officer, Cross Blue Shield of Florida as the Third Party Administrators and other related parties to represent the Consortium's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.
9. Privacy Officer is responsible for reviewing all privacy complaints and making a determination.

Role

Under the role of Privacy Contact, accountability is restricted to the individual member college.

Privacy Contact - Member Colleges

1. The Privacy Contact serves in a leadership role for Privacy Oversight activities of the *individual member college.*
2. The Privacy Contact serves as information privacy consultant to the *individual member college*.
3. The Privacy Contact will serve the *individual member college* as a liaison to regulatory and accrediting bodies for matters relating to privacy at the entity level.

Responsibilities

The responsibilities addressed herein apply to the Privacy Contact and extend across the *individual member college.*

1. The Privacy Contact provides leadership in the planning, design, and evaluation of *its member college's* privacy and security related projects.
2. The Privacy Contact will implement and maintain *FCSRMC's* Privacy Program and associated policies.
3. The Privacy Contact must maintain compliance with federal and state laws related to privacy, security, confidentiality, and protection of information resources.
4. The Privacy Contact is required to produce periodic reports to *FCSRMC* as to the status of information privacy.
5. The Privacy Contact collaborates with other departments such as legal counsel, corporate compliance, human resources, accounting, and with Business Associates as required to ensure compliance with *the FCSRMC's* specific privacy requirements.
6. The Privacy Contact develops administrative, technical and physical safeguards to protect the privacy of protected health information from accidental or intentional use or disclosure. Such safeguards will include policies regarding:
    a. Minimum necessary use of PHI
    b. Shredding of documents containing PHI
    c. Locked accesses to areas that contain PHI, such as doors and drawers; and ensure only the appropriate personnel have keys to locked areas.
7. The Privacy Contact monitors *its member college's* departmental systems development and operations for security and privacy compliance.
8. The Privacy Contact coordinates with *FCSRMC's Privacy Officer* regarding its complaint and information program for:
    a. Receiving complaints and/or questions related to any aspect of *its member college's* privacy program;
    b. Providing information in response to internal and external inquiries regarding *its member college's* privacy policies and procedures or notice of information practices;
    c. Ensuring that *its member college's* notice of information practices include the method for contacting the program or individual for privacy related matters;
    d. Recording and documenting all complaints/questions and their resolution;
    e. Ensuring investigation of all allegations of non-compliance with *its member college's* privacy policies or notice of information practices.
    f. Submitting a copy of all complaints to FCSRMC.
9. The Privacy Contact develops and implements *its member college's* privacy training program and, in conjunction with the Security Officer or other individual charged with security oversight, a cyber security awareness and training program that includes the following components:
    a. Initial training of all employees relating to the privacy and cyber security program;

b. Privacy and cyber security training for all new employees;
c. Upon changes in *FCSRMC* and/or *its member college's* privacy policy or procedure, retraining of directly affected employees;
d. Mandated privacy retraining for all employees on a periodic basis, but at a minimum, every three years;
e. Privacy training to all members of the workforce -including all contract employees, volunteers, trainees, and other persons under their direct control on an unpaid basis, who are not business partners but are likely to have contact with PHI.

10. The Privacy Contact coordinates with HR to develop appropriate sanctions for failure to comply with *its member college's* privacy policies and procedures by all members of the workforce, business partners or associates.
11. The Privacy Contact coordinates with the HR to ensure no intimidating, discriminatory, or other retaliatory actions occur against a person who files, testifies, assists or participates in any investigation, compliance review, proceeding or hearing related to a *its member college's* privacy violation or opposed any unlawful act or practice.
12. The Privacy Contact establishes an internal privacy audit program to ensure organization-wide compliance to *its member college's* privacy policies.
13. The Privacy Contact coordinates the development of privacy risk assessment policies and procedures designed to measure the performance and quality of *its member college's* privacy program.
14. The Privacy Contact periodically revises the privacy program in light of changes in laws, regulations, or *FCSRMC and its member colleges'* policy.
15. The Privacy Contact coordinates with HR regarding the development of procedures for documenting and reporting self- disclosures of any evidence of privacy violations to legal counsel, and if appropriate to the appropriate government regulatory body according to *its member college's* policy.

SECURITY OFFICIAL

Purpose: *The Security Official role and responsibilities are established pursuant to the Privacy Policy Statement adopted by the Florida College System Risk Management Consortium's (FCSRMC) Health Program and its member colleges. FCSRMC functioning as the Group Health Plan and the member colleges functioning as the employer/plan sponsor complies fully with all federal and state privacy protection laws and regulations. Protection of patient privacy is of paramount importance to this organization.*

Role

It is the policy of *FCSRMC and its member colleges* that specific individuals within our workforce are assigned the responsibility of implementing and maintaining the HIPAA Privacy and Security requirements. Furthermore, it is the policy of *FCSRMC and its member colleges* that these individuals or their designee will be provided sufficient resources and authority to fulfill their responsibilities. At a minimum it is the policy of *FCSRMC* that there will be one individual assigned as the Security Official at each member college. The Security Official will act as a focus and resource for the college's information security matters and will work closely with the Privacy Contact to achieve the goals of the organization. The Security Official will be responsible for coordinating and implementing security measures to protect Protected Health Information (PHI) received and processed for our employees as outlined by Federal and State rules and regulations.

Responsibilities

The Security Official:

1. Has an in-depth understanding of network and system security technology and practices across all major-computing areas (mainframe, client/server, PC/LAN, telephony) with a special emphasis on Internet related technology.

2. Has knowledge of HIPAA, state and federal guidelines on privacy, transactions and security.

3. Maintains a working knowledge and understanding of all hardware and software applications applicable to the member college.

4. Effectively applies information security management knowledge to enhance the security of the open network and associated systems and services.

5. Develops, in conjunction with the Privacy Officer and Privacy Contact, appropriate information security policies, standards, guidelines and procedures.

6. Monitors Information Security Program compliance and effectiveness in coordination with the college's Privacy Contact and operational assessment functions.

7. Facilitates and promotes activities to foster information security awareness within the organization and related entities.

8. Reviews system-related information security plans throughout the college's network to ensure alignment between security and privacy practices.

9. Conducts investigations of information security violations and computer crime. Works effectively with management and external law enforcement to resolve these instances.

10. Reviews instances of noncompliance and works effectively and tactfully to correct deficiencies.

11. Provides emergency access to systems containing ePHI in the event of a disaster or emergency.

12. Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.

13. Certifies that IT systems meet predetermined security requirements.

14. Makes recommendations for the improvement of operational and procedural changes.

15. Stays informed of latest web/internet tools and standards.

SANCTIONS POLICY:

It is the policy of FCSRMC and its member colleges that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. FCSRMC will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.

FCSRMC will take appropriate disciplinary action against employees, contractors, or any individuals who violate the information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

PROCEDURE:

1. Once the Privacy Officer has knowledge of an alleged unauthorized use or disclosure of PHI or other sensitive information, he or she shall immediately begin a thorough investigation of the unauthorized use of information. This may be performed through confidential interviews with staff members; inspection of release logs and/or access logs, and any other method(s) the Privacy Officer deems appropriate. It may also be necessary for the Privacy Officer to ask for assistance from another staff member in conducting the investigation. If so, he or she shall ask for assistance from a staff member who is not party to the alleged unauthorized release of PHI.

2. The investigation may find a systemic issue with FCSRMC's policies and procedures on handling PHI, or the investigation may find a personnel issue, or both. The Privacy Officer, upon concluding the investigation, shall implement appropriate changes to policies and/or personnel, as is deemed necessary, and shall do so as expeditiously as possible.

3. The Practice Administrator/ Privacy Officer **may** make changes as follows:

   Policy changes: The Privacy Officer may find the Practice policies and/or procedures require adjustment(s). The Privacy Officer shall make the necessary modifications to the Practice's policies by adding addendum(s) to the current policies, and shall notify all staff members of the change(s) through inter-office memorandum. This shall be done as expeditiously as possible.

   Personnel changes: The Privacy Officer may find that one or more staff members either does not understand or refuses to abide by FCSRMC's policies and procedures on maintaining the privacy and confidentiality of PHI. It may be necessary for employees to be disciplined by the Privacy Officer for violations of the Practice's policies. The Privacy Officer shall determine the severity of the punishment based on the severity of the unauthorized release. However, the following provides a guide as to how the Privacy Officer may discipline the employee(s):

   First Offense: Re-training on the Practice's policies and procedures governing privacy of PHI, and verbal reprimand/counseling with a note of the verbal

reprimand filed in the staff members' personnel file.

Second Offense: Written reprimand from the Privacy Officer, with one copy given to the employee(s) and one copy kept in the employees' file.

Third Offense: Suspension from duties without pay, for a period to be determined by the Administrator/Privacy Officer, but not to exceed two (2) weeks.

Fourth Offense: Termination of the employee.

4. In addition, the Privacy Officer may transfer the employee(s) to another department within FCSRMC in which the employee(s) will no longer have access to PHI.

5. In all cases, the Privacy Officer shall document in writing the unauthorized use(s) or disclosure(s) of PHI, the perpetrator(s), and what action(s) (if any) were taken as a result of the violation(s).

FCSRMC and its Member Colleges Training
HIPAA Questions & Answers

1. What is HIPAA?

Health Insurance Portability and Accountability Act (HIPAA) is federal legislation that was enacted in 1996. Administrative Simplification, under Title II, focuses on three specific issues: Electronic Data Interchange, Privacy and Security.

- **Electronic Data Interchange** establishes standardization of transactions, code sets and identifiers.
- **Privacy Rule** governs the privacy of individually identifiable health information.
- **Security** governs physical and cyber protection of individual health information.

2. When does the HIPAA Privacy Rule become effective for FCSRMC and its member colleges?

The HIPAA Privacy Rule compliance date is April 14, 2003. The policies and procedures are reviewed periodically and revisions are made when necessary based on governmental, business organization, environmental, and/or other changes.

3. Who must comply with the HIPAA Privacy Rule?

All covered entities must comply with the HIPAA Privacy Rule. Health Plans, providers and health care clearinghouses are considered covered entities under this rule.

4. How does the HIPAA Privacy Rule specifically affect FCSRMC and its member colleges?

FCSRMC, acting as the covered entity and its member colleges, acting as the plan sponsor, have undertaken fiduciary duties to the plan. A covered health plan includes a group health plan, which is defined as an employee welfare benefit plan under ERISA. This may include hospital and medical benefit plans, plans, vision plans, health flexible spending accounts and employee assistance plans.

5. What is Protected Health Information?

Names	All geographic subdivision smaller than States
Account numbers	Certificate/License numbers
Medical record numbers	WEB universal resource locator (URL)
Social security numbers	Internet protocol address number (IP)
All elements of Dates excluding year	Biometric identifier
Health plan beneficiary numbers	Device identifiers and serial numbers
Electronic mail addresses	Fax numbers
Telephone numbers	

Any other unique identifying number, characteristic, or code

6. Are other insurance plans covered under the HIPAA Privacy Rule?

No. The HIPAA Privacy Rule does not apply to Life, Workers' Compensation, Disability or Property and Casualty plans.

7. What is FCSRMC and its member colleges' policy for using or disclosing PHI?

It is the policy of FCSRMC and its member colleges that protected health information may not be used or disclosed except under very specific conditions.

8. Under what conditions can PHI be used or disclosed?

When at least one of the following conditions is true PHI may be used or disclosed:

- The individual who is the subject of the information has authorized the use or disclosure.
- The individual who is the subject of the information has received the Notice of Privacy Practices developed and distributed by Florida Blue thus allowing the use or

disclosure and the use or disclosure is for treatment, payment or health care operations.

- The individual who is the subject of the information agrees with the disclosure via the authorization form or a signed copy of this Privacy Policy and the disclosure is to persons involved in the processing or assistance of health care claims.
- The disclosure is to the individual who is the subject of the information or to HHS for compliance-related purposes.
- The use or disclosure is for one of the HIPAA "public purposes" (i.e. required by law, etc.).

9. Are there any circumstances that allow PHI to be used or disclosed without prior authorization?

PHI may be used or disclosed only for treatment, payment or healthcare operation purposes without a prior authorization. Other permitted disclosures without an authorization include: public health activities, victims of abuse/neglect/domestic violence, law enforcement purposes, compliance with Workers' Compensation, and to avoid serious threat to health or safety.

10. Can PHI be used to make employment elated decisions (i.e. hiring, termination, promotion)?

It is the policy of FCSRMC and its member colleges that PHI will **not** be used to make employment related decisions (e.g. hiring, terminations, promotions).

11. How are individuals advised of Notice of Privacy Practices?

Florida Blue as the Group Health Plan Third Party Administrators will publish and distribute a Notice of Privacy Practices to all the Group Health Plan participants for Blue Cross Blue Shield of FL, Health Options Inc., and Delta Dental for Dental.

12. Are there any limitations on what protected information can be released?

All disclosures of protected health information must be limited to the minimum amount of information needed to accomplish the purpose of the disclosure.

13. Can an individual request that no disclosures of PHI be made?

It is the policy of *FCSRMC and its member colleges* that individuals have a right to request that no disclosure be made of PHI. *FCSRMC or its member colleges* is not obligated to grant the request.

14. Who has access to PHI?

It is the policy of *FCSRMC and its member colleges* that access to protected health information may be granted to authorized employee(s) or contractor(s) based on the assigned job functions of the employee or contractor. It is also the policy of this organization that such access privileges should not exceed those necessary to accomplish the assigned job function. Unique sign-ons and passwords will be required in order to access to systems containing protected health information.

15. Can an individual have access to her/his own PHI?

It is the policy of *FCSRMC and its member colleges* that access to protected health information must be granted to the person who is the subject of such information when such access is requested. Access requests should be directed to and will be processed by Blue Cross Blue Shield of FL, for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Group Health Plan Third Party Administrators.

16. Can an individual amend or correct her/his own PHI?

Yes, in most instances an individual can amend or correct her/his PHI. However, it is the policy of *FCSRMC and its member colleges* that all requests for amendment of incorrect protected health information will be directed to and processed by Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information.

17. Who qualifies as a "personal representative" for the purposes of use and disclosure of PHI?

It is the policy of *FCSRMC and its member colleges* that access to protected health information

must be granted to personal representatives of individuals as though they were the individuals themselves. Personal representatives may include legal designations such as Power of Attorney or parent to a minor child. It is the policy of *FCSRMC and its member colleges* that all requests for access to protected health information will be directed to and processed by Blue Cross Blue Shield of FL, for Blue Cross Blue Shield of FL, Health Options, Inc., and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information.

18. Is a deceased individual's information protected under the HIPAA Privacy Rule?
It is the policy of *FCSRMC and its member colleges* that privacy protections extend to information concerning deceased individuals.

19. Can an individual request an alternate communication channel relative to their PHI?
It is the policy of *FCSRMC and its member colleges* that all requests for alternative communication channels will be directed to and processed by Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information and that alternative communications channels be used, as requested by the individuals, to the extent possible.

20. Can an individual request an accounting of all disclosures of PHI?
It is the policy of FCSRMC and its member colleges that an accounting of all disclosures subject to such accounting of protected health information be given to individuals whenever such an accounting is requested. These requests should be directed to Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information.

21. Under what circumstances should PHI be disclosed for Judicial or other legal proceedings?
It is the policy of *FCSRMC and its member colleges* that information be disclosed for the purposes of a judicial or administrative proceeding only when: accompanied by a court or administrative order or grand jury subpoena; when accompanied by a subpoena or discovery request that includes either the authorization of the individual to whom the information applies, documented assurances that good faith effort has been made to adequately notify the individual of the request for their information and there are no outstanding objections by the individual, or a qualified protective order issued by the court. These requests should be directed to Florida Blue for Blue Cross Blue Shield of FL, Health Options Inc. and Delta Dental for Dental as the Third Party Administrators and maintainer of the Protected Health Information.

22. What are de-identified data and limited data sets?
It is the policy of *FCSRMC and its member colleges* to disclose de-identified data only if it has been properly de-identified by removing all the relevant identifying data. We will make use of limited data sets, but only after the relevant identifying data have been removed and then only to organizations with which we have adequate data use agreements and only for research, public health, or health care operations purposes.

23. When is an authorization required for release of PHI?
It is the policy of FCSRMC and its member colleges that a valid authorization will be obtained for all disclosures that are not related to treatment, payment, health care operations, the individual or their personal representative. A signed copy of this Privacy Policy will serve as authorization for FCSRMC and/or the member colleges to provide assistance in resolving healthcare claims issues. If a signed copy of this Privacy Policy is not on file, the individual requesting assistance will be asked to sign the Privacy Policy. An individual will also need to submit a signed Authorization Form in the event that they want to grant authorization to a third party (e.g. a spouse or parent). A copy of the signed authorization will be forwarded to FCSRMC by the member college.

24. How can an individual file a complaint regarding her/his PHI?
It is the policy of FCSRMC and its member colleges that all complaints relating to the protection of health information be investigated and resolved in a timely fashion. Furthermore, it is the policy of FCSRMC that all complaints will be addressed to the college Privacy Contact for research and resolution. The Privacy Contact may involve FCSRMC and/or Florida Blue as needed to

resolve a complaint. All complaints will be forwarded to FCSRMC's Privacy Officer for tracking purposes.

25. Does FCSRMC and its member colleges' HIPAA Privacy Policy specify prohibited activity?

It is the policy of FCSRMC and its member colleges that no employee or contractor may engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA regulations. It is also the policy of this organization that no employee or contractor may condition payment, enrollment or eligibility for benefits on the provision of an authorization to disclose protected health information.

26. Who is responsible for implementing and managing FCSRMC and its member colleges' HIPAA Privacy Policy and Procedures?

It is the policy of *FCSRMC and its member colleges* that the responsibility for designing and developing procedures to implement this policy lies with the Privacy Officer and/or the Privacy Contact where appropriate.

27. What does verification of identity mean?

It is the policy of *FCSRMC and its member colleges* that the identity of all persons who request access to protected health information is reasonably verified before such access is granted.

28. How is PHI safeguarded?

It is the policy of *FCSRMC and its member colleges* that appropriate physical safeguards will be in place to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy Rule. These safeguards will include physical protection of premises and PHI, technical protection of PHI maintained electronically and administrative protection. These safeguards will extend to the oral communication of PHI.

29. What is a Business Associate Agreement?

It is the policy of FCSRMC and *its member colleges* that business associates must be contractually bound to protect health information to the same degree as set forth in this policy. It is also the policy of this organization that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate.

30. What happens if FCSRMC and its member colleges' HIPAA Privacy Policy and Procedures are violated?

It is the policy of *FCSRMC and its member colleges* that sanctions will be in effect for any member of the workforce who intentionally or unintentionally violates any of these policies or any procedures related to the fulfillment of these policies. Sanctions will adhere to and be carried out according to *FCSRMC and each respective member college's* disciplinary procedures for violation of any of its policies and procedures.

31. How long must records designated by HIPAA be kept?

It is the policy of FCSRMC and its member colleges that the HIPAA Privacy Rule records retention requirement of six years will be strictly adhered to. All records designated by HIPAA in this retention requirement will be maintained in a manner that allows for access within a reasonable period of time. This records retention time requirement may be extended at this organization's discretion to meet with other governmental regulations or those requirements imposed by our professional liability carrier. Florida Blue as the Third Party Administrators will retain the health insurance records of Plan Participants.

32. Which agencies act as HIPAA oversight authorities?

Under Title II, The Office for Civil Rights of the Department of Health and Human Services is the primary oversight body.

33. Should these oversight agency representatives be given access to PHI?
It is the policy of *FCSRMC and its member colleges* that oversight agencies such as the Office for Civil Rights of the Department of Health and Human Services be given full support and cooperation in their efforts to ensure the protection of health information within this organization. It is also the policy of this organization that all personnel must cooperate fully with all privacy compliance reviews and investigations.

34. Can protected health information be stored in the personnel file?
The Americans with Disabilities Act (ADA) and HIPAA require that all medical documents be filed separately from personnel records. Medical information (i.e. pre-employment physicals, drug/alcohol testing results, workers' comp paperwork, medical leave LOA forms, disability paperwork, insurance applications that reveal pre-existing conditions, etc.) should be kept confidential and away from personnel records.

35. Is HIPAA training and education mandatory or voluntary?
The Department of Health and Human Services mandates privacy and security training , as well as regular reminders, for all employees of Covered Entities that have access to protected health information.

36. What is a Breach?
A breach is the **unauthorized** use or disclosure of **unsecured** protected health information. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the protected health information has been compromised. Suspected breaches should be reported to the Privacy Contact at the member college.

37. Is it OK to download software or open attachments from to emails from unknown sources?
Staff should never open attachments to emails from unknown sources, or download software that has not been approved by the IT Security Official at the member college. Staff should immediately contact the IT Security Official if they suspect that their computer has been infected by a virus.

FCSRMC and its member colleges: Workforce Training

A HIPAA Privacy Policy has been adopted by the Florida College System Risk Management Consortium's (FCSRMC) Health Program and its member colleges. FCSRMC functioning as the Group Health Plan and the member colleges functioning as the employer/plan sponsor complies fully with all federal and state privacy protection laws and regulations. Protection of patient privacy is of paramount importance to this organization. Violations of any of these provisions may result in severe disciplinary action including termination of employment and possible referral for criminal prosecution.

Further, *FCSRMC and its member colleges* have placed sanctions in effect for any member of the workforce who intentionally or unintentionally violates any of these policies or any procedures related to the fulfillment of these policies. Sanctions will adhere to and be carried out according to *FCSRMC and each respective member college's* disciplinary procedures for violation of any of its policies and procedures.

My signature below indicates that I have received *FCSRMC and its member colleges'* HIPAA Privacy Rule Awareness and Compliance Training and that I fully understand the penalty for violating the Privacy Policy.

_____ _____

Employee Name Date

_____

Employee Signature

Group Training Attendance Form

Program Title: _____

Program Date: _____

Location: _____

Print Name	Job Title	Signature

FCSRMC's Business Associate Agreements

FCSRMC has singed Business Associate Agreements with the following business partners:

- Aetna Resources for Living (EAP provider)
- Delta Dental
- FBMC
- Florida Blue, Blue Cross Blue Shield of Florida
- Mercer Consulting
- VSP
- Unum