

FCSRMC

FLORIDA COLLEGE SYSTEM RISK MANAGEMENT CONSORTIUM

HIPAA Privacy Policy

March 1

2023

Revision

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

Table of Contents

PRIVACY POLICY STATEMENT	3
Acknowledgement of Receipt of Privacy Policy.....	9
HIPAA PROCEDURES MANUAL	10
ACCESS REQUEST PROCESSING	12
Actions To Be Taken For All Access Requests	12
AMENDMENT REQUEST PROCESSING	13
Actions To Be Taken For All Amendment Requests.....	13
COMPLAINT PROCESSING	14
Actions To Be Taken For All Complaints	14
Actions To Be Taken When No Compliance Violation Is Found	14
Actions To Be Taken When A Compliance Violation Is Found	15
DISCLOSURE ACCOUNTING REQUESTS	16
INDIVIDUAL PERMISSION	17
Actions To Be Taken When Obtaining Written Authorization.....	17
INFORMATION DISCLOSURES	18
Actions To Be Taken When Disclosing Information to Law Enforcement	18
Actions To Be Taken When Disclosing Information For A Judicial Or	
Administrative Proceeding	18
Actions To Be Taken When Disclosing Information To The Individual.....	19
Actions To Be Taken When Disclosing Information To The Department	
Of Health and Human Services as Part Of A Compliance Review	19
Actions To Be Taken When Disclosing Information About Deceased Individuals	19
Actions To Be Taken When Disclosing Information About Minors To Their	
Parents Or Guardians.....	20
NOTICE AND ACKNOWLEDGEMENT	21
PERSONAL REPRESENTATIVES	21
Actions To Be Taken When Dealing With Personal Representatives	21
TRAINING	22
Actions To Be Taken For Initially Training The Workforce	22
Actions To Be Taken For Training New Workforce Members	22
Actions To Be Taken For Ongoing Training Of The Workforce	22

AUTHORIZATION FOR THE USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION.....	24
Complaint Form	26
Response to Complaint	27
Complaint Tracking Information.....	28
EMPLOYEE RESPONSIBILITIES	29
Employee Requirements.....	29
Prohibited Activities.....	29
BUSINESS ASSOCIATE AGREEMENT	31
PRIVACY OFFICER/PRIVACY CONTACT	39
SECURITY OFFICIAL.....	43
SANCTIONS POLICY	45
BREACH ASSESSMENT/NOTIFICATION	47
Mitigation.....	48
FCSRMC and its Member Colleges Training	49
HIPAA Questions & Answers	49
FCSRMC and its Member Colleges: Workforce Training Acknowledgement Form ..	49
Group Training Attendance Form.....	55
FCSRMC's Business Associate Agreements List.....	56

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, 2023

Expiration Date: *This policy remains in effect until superseded or cancelled.*

Policy Owner: *FCSRMC Privacy Officer: Executive Director & Chief Risk Officer*

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 (PHI)

- We can use your health information and share it with professionals who are treating you.
- We use and disclosure your health information as we pay for your health services.
- We can disclose your health information to your Group Health Plan for plan administration.
- We can use or share health information about you for workers' compensation claims, law enforcement purposes or with a law enforcement official, health oversight agencies for activities authorized by law, and for special government functions such as military and national security.
- We can share health information about you in response to a court or administrative order or in response to a subpoena.

It is the policy of *FCSRMC and its member colleges* that PHI 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. In the unfortunate event of an individuals' death, FCSRMC is permitted to disclose PHI to personal representatives, family members or others who were involved in the care or payment for care prior to the death of the individual, unless inconsistent with any prior expressed preference provided to us.

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 PHI

It is the policy of *FCSRMC and its member colleges* that (except for disclosures made for treatment or healthcare operation purposes) all disclosures of PHI 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 PHI 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 PHI by FCSRMC and Member Colleges

It is the policy of *FCSRMC and its member colleges* that access to PHI 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 PHI, 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 PHI by the Individual

It is the policy of *FCSRMC and its member colleges* that access to PHI 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 PHI

It is the policy of *FCSRMC and its member colleges* that all requests for amendment of incorrect PHI 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 PHI.

Access by Personal Representatives

It is the policy of *FCSRMC and its member colleges* that access to PHI 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 PHI 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 PHI.

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 PHI 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 PHI 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 PHI.

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 PHI.

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. This includes marketing, fundraising or sale of PHI.

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.

Authorizations to use or disclose PHI can be revoked except to the extent that action has already been taken. Revocation of an authorization must be submitted in writing to the Privacy Officer.

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.

You may also file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.E., Washington, D.C. 20201, calling 877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints.

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 PHI. 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 PHI 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 PHI 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 electronic Protected Health Information (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.

We are obligated to notify individuals promptly if a breach occurs that may have compromised the privacy or security of their 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 PHI to the contracted party. This includes subcontractors that *FCSRMC* may utilize to provide activities related to PHI *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 PHI have been trained by the compliance date on the policies and procedures governing PHI 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 Information 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 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

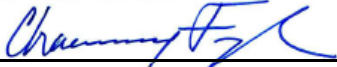
HIPAA PROCEDURES MANUAL

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 & Chief Risk Officer 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.

2023



Chauncey Fagler, Executive Director &
Chief Risk Officer
Florida College System
Risk Management Consortium

02/15/23

Date



Tony Ganstine, Associate Director
Compliance Officer's Signature

02/15/23

Date



Natalie Dyksterhouse
Back-up Compliance Officer's Signature

02/15/23

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 (PHI) 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 PHI, 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 PHI, 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 PHI, 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 (PHI) 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 FCSRMC and requests an amendment to PHI, 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 PHI, 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 PHI, 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 (PHI) 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 PHI, 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 PHI, 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 PHI, 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 PHI, 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 PHI, 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 PHI, 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 PHI, 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 PHI 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: _____

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: <input type="checkbox"/> Yes <input type="checkbox"/> No	Date of Follow-up:

Reviewer's Comments:

Action Taken:

Employee Responsibilities

FCSRMC and its Member Colleges

Staff are responsible for the security of all data which may come to them in whatever format. FCSRMC and member colleges are responsible for guarding against any reasonably anticipated use or disclosure of Protected Health Information (PHI) that is not permitted or required under HIPAA regulations, including ongoing training programs to inform all staff of these requirements.

Employee Requirements

1. Challenge Unrecognized Personnel - It is the responsibility of all personnel to take positive action to provide physical security. If an unrecognized person is seen in a restricted office location, staff should challenge them as to their right to be there. All visitors should sign in at the front desk. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.
2. Unattended Computers - Unattended computers/laptops should be locked by the user when leaving the work area. Computers will have the automatic screen lock function set to automatically activate upon inactivity based on a time agreed upon by the Security Officer or I.T. official. Employees are not allowed to take any action which would override this setting.
3. Home Use of College Assets - Only computer hardware (including iPhones and other PDAs) and software owned by and installed by the College is permitted to be connected to or installed on College equipment. Only software that has been approved for corporate use by the College may be installed on College equipment. Personal computers (including laptops) supplied by the College are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers which may be supplied by the College for home use.
4. Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the College are the property of the College unless covered by a contractual agreement. Nothing contained herein applies to software purchased by College employees at their own expense.

Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

1. Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.

2. Exporting to Home Computer. Emailing or otherwise exporting PHI to home computers for work purposes is prohibited due to unstable/unsecure computer environment.
3. Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
4. Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which staff have not been approved on a "need to know" basis is prohibited. The Practice has access to patient health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which staff have not been granted access by the appropriate approval procedure is strictly prohibited.
5. Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on College computers must be approved by the College.
6. Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the College is strictly prohibited.
7. System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the College is strictly prohibited.
8. Installing College software on home computers is prohibited. Employees can, however, access College software from home via a controlled/secured method (VPN) approved by the College if security access has been granted by the Systems Administrator.

**FLORIDA COLLEGE SYSTEM RISK MANAGEMENT
CONSORTIUM (FCSRMC)**

BUSINESS ASSOCIATE AGREEMENT

THIS **BUSINESS ASSOCIATE AGREEMENT** (this “Agreement”) is entered into on _____, 202_ (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.”

The purpose of this Agreement is to comply with the requirements of (i) the Florida Information Protection Act of 2014 (“FIPA”); (ii) the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the associated regulations, as may be amended; (iii) the HIPAA Privacy Rule codified at, 45 C.F.R. Parts 160 and 164, Subparts A and E, as may be amended; (iv) the HIPAA Security Rule codified at 45 C.F.R. Part 160 and 164, Subpart C, as may be amended; (v) the Breach Notification Rule, codified at 45 C.F.R. Part 164, Subpart D, as may be amended; (vi) the Enforcement Rule codified at 45 C.F.R. Part 160, Subparts C and D, as may be amended; (vii) the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”); and (viii) the HIPAA Omnibus Final Rule published in the Federal Register at 78 Fed. Reg. 5,566 (Jan. 25, 2013), and effective on March 26, 2013. The HITECH Act provides further protection for the privacy and security of PHI used and disclosed through health information technology. The Privacy, Security, Breach Notification and Enforcement Rules are collectively referred to herein as the “HIPAA Rules.” Unless otherwise defined in this Agreement, capitalized terms have the meanings given in the HIPAA Rules, HITECH Act and FIPA.

In consideration of the Parties’ new or continuing obligations under the Services Agreement and other good and valuable consideration, the receipt and sufficiency is hereby acknowledged, the Parties agree to comply with the requirements of the HIPAA Rules and HITECH Act as follows:

1. **Services.** Covered Entity and Business Associate have entered into an agreement (the “Services Agreement”) under which Business Associate may create, receive, use, maintain or transmit PHI from or on behalf of Covered Entity in the course of providing certain services (the “Services”) for Covered Entity. The Services Agreement is incorporated herein by this reference. In the event of a conflict between the terms of the Services Agreement and this Agreement, this Agreement shall control.

2. **Relationship of the Parties.** None of the provisions of this Agreement are intended to create, nor shall they be deemed to create, any relationship between the Parties other than that of independent parties contracting with each other solely for the purposes of effecting the provisions of this Agreement and any other agreements between the Parties

evidencing their business relationship. Business Associate is an independent contractor, and not an agent of Covered Entity.

3. **Permitted Uses and Disclosures.** Business Associate may use and/or disclose PHI and Personal Information only as permitted or required by this Agreement, or as otherwise required by law. Business Associate may disclose PHI and Personal Information to, and permit the use of PHI and Personal Information 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 shall make uses and disclosures, and requests for PHI and Personal Information from Covered Entity, only in a manner consistent with Covered Entity's minimum necessary policies and procedures, and no more than the minimum PHI and Personal Information necessary to perform the Services. Business Associate shall not use or disclose PHI in a manner (i) inconsistent with Covered Entity's obligations under the HIPAA Rules, or HITECH Act, or FIPA, or (ii) that would violate the HIPAA Rules, HITECH Act or FIPA if disclosed or used in such a manner by Covered Entity. Business Associate may use PHI and Personal Information for the proper management and administration of Business Associate's business and to carry out its legal responsibilities in accordance with 45 C.F.R. § 164.504(e)(4). Business Associate may not de-identify PHI received from, or created on behalf of Covered Entity without the express written authorization of Covered Entity.

4. **Safeguards for the Protection of PHI and Personal Information.** Business Associate shall conduct an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by Business Associate. Business Associate warrants that Business Associate has implemented and shall maintain commercially reasonable and appropriate security safeguards that meet the National Institute of Standards and Technology ("NIST") and Federal Information Processing Standards for both PHI and Personal Information at rest and in motion, to protect the confidentiality and integrity of such PHI and Personal Information created, received, used, maintained or transmitted from, or on behalf of Covered Entity. PHI and Personal Information at rest is defined as data which resides in a data base, file system or other structured storage. This might include data on a laptop, tablet, phone, removable media, flash drives, USB sticks, hard-drives, personal computer, central servers (database for EMR and practice management system). PHI and Personal Information in motion is data that is moving through a network, including wireless transmission, such as e-mail or another form of electronic interchange, such as claim submission. Unencrypted PHI data must be destroyed or completely and securely removed from computers, devices and electronic media (including backups) before disposal, repair, or re-assignment of such equipment. Upon request by Covered Entity, Business Associate shall provide a written description of such risk assessment and security safeguards. Business Associate shall comply with the HIPAA Security Rule codified at 45 C.F.R. Part 160 and 164, Subpart C, as may be amended, and with the applicable provisions of the HIPAA Privacy Rule codified at, 45 C.F.R. Parts 160 and 164, Subparts A and E, as may be amended, to the extent Business Associate is to carry out any of Covered Entity's obligations under the Privacy Rule.

5. **Reporting and Mitigating the Effect of Unauthorized Uses and Disclosures.** If Business Associate has knowledge of any use or disclosure of PHI and/or Personal Information not provided for by this Agreement, then Business Associate shall promptly notify Covered Entity in accordance with Section 13. Business Associate shall

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 and/or Personal Information of which it becomes aware. Furthermore, in the event Business Associate becomes aware of a Security Incident involving PHI and/or Personal Information, by itself or any of its agents or subcontractors, Business Associate shall notify Covered Entity in writing within five (5) calendar days, 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."

6. **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 and "Breach" of "Personal Information" as those terms are defined by Fla. Stat. §501.171 (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 shall, following the discovery of a Data Breach, promptly notify Covered Entity and in no event later than five (5) 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 Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate shall 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 Business Associate. No later than five (5) 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. and Fla. Stat. §501.171. Specifically, such information shall include Business Associate's risk assessment, which conforms to the requirements of 45 C.F.R. § 164.402, as to the probability that the impermissible use or disclosure did or did not compromise PHI or Personal Information and if the following information is known to (or can be reasonably obtained by) Business Associate, Business Associate shall 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, date of discovery, and number of Individuals affected by the Data Breach; (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, diagnosis 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 and/or

learn additional information concerning the Data Breach. Following a Data Breach, Business Associate shall 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 the items above.

7. **Use and Disclosure of PHI by Subcontractors, Agents, and Representatives.** Business Associate shall require any subcontractor, agent, or other representative that is authorized to create, receive, maintain, or transmit PHI on behalf of Business Associate to execute a business associate agreement to agree in writing to the same terms set forth herein. Business Associate shall terminate its business associate agreement with any subcontractor, agent or other representative if such subcontractor, agent or representative fails to abide by any material term of such agreement. Such business associate agreement shall identify Covered Entity as a third-party beneficiary with rights of enforcement in the event of any HIPAA violations.

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

8.1. **Right of Access.** Business Associate agrees to provide access to PHI maintained by Business Associate in a Designated Record Set, at the request of Covered Entity, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. §164.524. Such access shall be provided by Business Associate in the time and manner designated by Covered Entity, including, where applicable, access by electronic means pursuant to Section 13405(e) of the HITECH Act.

8.2. **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 Covered Entity or an Individual, and in the time and manner designated by Covered Entity.

8.3. **Right to Accounting of 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, as amended by Section 13405(c) of the HITECH Act and any related regulations or guidance issued by HHS in accordance with such provision.

9. **Ownership of PHI.** Covered Entity holds all right, title and interest in and to any and all PHI received by Business Associate from, or created or received by Business Associate on behalf of, Covered Entity, and Business Associate does not hold, and shall not acquire by virtue of this Agreement or by virtue of providing any services or goods to Covered Entity in the course of fulfilling its obligations pursuant to this Agreement, any right, title or interest in or to such PHI. Except as specified in this Agreement, Business Associate shall have no right to compile or distribute any statistical analysis or report

utilizing such PHI derived from such PHI, any aggregate information derived from such PHI, or any other health and medical information obtained from Covered Entity.

10. **Prohibition on Sale of PHI.** Business Associate shall not sell PHI or receive any remuneration, direct or indirect, in exchange for PHI, except as expressly permitted by this Agreement and the Services Agreement.

11. **Inspection of Books and Records.** Business Associate shall make its internal practices, books, records, and policies and procedures relating to the use and disclosure of PHI and/or Personal Information 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”), Florida Attorney General (“AG”), or their agents or to Covered Entity for purposes of monitoring compliance with the HIPAA Rules and the HITECH Act. Such information shall be made available in a time and manner designated by Covered Entity, HHS, OCR, or AG. With reasonable notice, Covered Entity may audit Business Associate to monitor compliance with this Agreement. Business Associate will promptly correct any violation of this Agreement found by Covered Entity and will certify in writing that the correction has been made. Covered Entity’s failure to detect any unsatisfactory practice does not constitute acceptance of the practice or a waiver of Covered Entity’s enforcement rights under this Agreement.

12. **Term and Termination.**

12.1. **Term.** This Agreement shall commence on the Effective Date and end with the termination of the Services Agreement unless terminated sooner pursuant to this Agreement.

12.2. **Termination for Breach by Covered Entity.** As provided for under 45 C.F.R. § 164.504(e)(2)(iii), Covered Entity may immediately terminate this Agreement, all relevant Services Agreement(s) and any related agreements if Covered Entity determines that Business Associate has breached a material term of this Agreement. Alternatively, and in the sole discretion of Covered Entity, Covered Entity may choose to provide Business Associate with written notice of the existence of the breach and provide Business Associate with thirty (30) calendar days to cure said breach upon mutually agreeable terms.

12.3. **Termination by for Breach by Business Associate.** If Business Associate determines that Covered Entity has breached a material term of this Agreement, then Business Associate shall provide Covered Entity with written notice of the existence of the breach and shall provide Covered Entity with thirty (30) calendar days to cure said breach upon mutually agreeable terms or end the violation within this thirty (30) day period. Failure by Covered Entity to cure said breach or violation in the manner set forth above shall be grounds for immediate termination of the Services Agreement by Business Associate.

12.4. **Effect of Termination.** Within thirty (30) calendar days of termination of this Agreement, Business Associate shall recover any PHI and/or Personal Information relating to this Agreement in possession of Business Associate and its subcontractors, agents, or representatives. Business Associate shall return to Covered Entity or destroy all such PHI and Personal Information plus all other PHI

and Personal Information relating to this Agreement in its possession, and shall retain no copies. Business Associate agrees that all paper, film, or other hard copy media shall be shredded or destroyed such that it may not be reconstructed, and electronic PHI and Personal Information shall be purged or destroyed concurrent with NIST Guidelines for Media Sanitization at <http://www.csrc.nist.gov/>. If Business Associate believes that it is not feasible to return or destroy the PHI and Personal Information 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 and Personal Information 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 and Personal Information, Business Associate shall ensure that any and all protections, requirements and restrictions contained in this Agreement shall be extended to any PHI and Personal Information retained after the termination of this Agreement, and that any further uses and/or disclosures shall be limited to the purposes that make the return or destruction of the PHI and Personal Information infeasible. Business Associate further agrees to comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment of such PHI and Personal Information.

13. **Notices.** Any and all notices and other communications required or permitted to be given under this Agreement shall be: (a) delivered by personal delivery, provided the person to whom delivered signs a receipt; (b) delivered by commercial courier such as Federal Express, provided the person to whom delivered signs a receipt or the commercial courier can verify delivery; (c) sent by overnight U.S. express mail, provided the postal service can verify delivery; (d) sent by registered or certified mail, postage prepaid, provided delivery is actually made; or (e) sent by facsimile, provided the person that sent the notice can verify delivery. All notices shall be sent to the following addresses or to such other addresses as shall be furnished by notice to the other party in accordance with the provisions of this Section 13:

If to Covered Entity:

Florida College System Risk
Management Consortium (FCSRMC)
4500 NW 27th Avenue, Suite B2
Gainesville, FL 32606
Attn: Natalie Dyksterhouse

If to Business Associate:

Attn: _____

14. **Indemnification.** Business Associate shall indemnify, defend and hold harmless Covered Entity and its respective shareholders, directors, officers, members, managers, employees, and agents from and against all claims, actions, damages, judgments, losses, liabilities, fines, penalties, costs, or expenses (including without limitation reasonable attorney's fees, expert witness fees, consultant fees and costs of investigation, litigation or dispute resolution), arising directly or indirectly, in whole or in part, out of (a) any breach by Business Associate of this Agreement, (b) any act or omission by Business

Associate, its employees, contractors, subcontractors, agents, affiliates or representatives in the performance of its obligations hereunder; or (c) any HIPAA, FIPA or privacy violation committed by Business Associate, its employees, contractors, subcontractors, agents, affiliates, or representatives. This indemnification obligation of Business Associate shall survive termination of this Agreement.

15. **Miscellaneous.**

15.1. **Survival.** The respective rights and obligations of the Parties under Section 11 (Inspection of Books and Records), Section 12.4 (Effect of Termination), Section 14 (Indemnification) and Section 15 (Miscellaneous) shall survive termination of this Agreement indefinitely, and those other provisions of this Agreement that apply to rights or obligations of a Party, which continue or arise upon or after the termination of this Agreement shall survive the termination this Agreement to the extent necessary to enforce such rights and obligations and to otherwise effectuate such provisions.

15.2. **State Law.** In addition to FIPA, Business Associate shall comply with all applicable Florida privacy laws.

15.3. **Regulatory References.** A citation in this Agreement to the Code of Federal Regulations or to the Florida Statutes shall mean the cited section as that section may be amended from time to time.

15.4. **Amendment.** This Agreement may be amended or modified only in a writing signed by the Parties. The Parties agree that they shall negotiate amendments to this Agreement to conform to any changes in the HIPAA Rules and/or FIPA as are necessary for Covered Entity to comply with the current requirements of the HIPAA Rules and/or FIPA. In addition, in the event that either Party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Rules and/or FIPA or any other applicable legislation, then such Party shall notify the other Party of its belief in writing. For a period of up to thirty (30) days, the Parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such thirty-day period, the Agreement fails to comply with the HIPAA Rules and/or FIPA or any other applicable legislation, then either Party has the right to terminate this Agreement and the Services Agreement upon written notice to the other Party.

15.5. **Interpretation.** Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules, HITECH Act and FIPA.

15.6. **Injunctive Relief.** Business Associate expressly acknowledges and agrees that the breach, or threatened breach, by it of any provision of this Agreement may cause Covered Entity to be irreparably harmed and that Covered Entity may not have an adequate remedy at law. Therefore, Business Associate agrees that upon such breach, or threatened breach, Covered Entity shall be entitled to seek injunctive relief to prevent Business Associate from commencing or continuing any action constituting such breach without having to post a bond or other security and without having to prove the inadequacy of any other available remedies. Nothing in this

Section shall be deemed to limit or abridge any other remedy available to Covered Entity at law or in equity.

15.7. Governing Law; Venue. This Agreement shall be governed by and construed in all respects by the laws of the State of Florida. Venue for any action commenced under this Agreement shall be Duval County, Florida.

15.8. No Third Party Beneficiaries. Except as provided in Section 7, 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.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement effective as of the Effective Date.

Covered Entity:

Business Associate:

**Florida College System Risk
Management Consortium (FCSRMC)**

By: _____

By: _____

Name: _____

Name: _____

Its: _____

Its: _____

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 PHI 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).

BREACH ASSESSMENT/NOTIFICATION

A breach of PHI shall be treated as “discovered” as of the first day on which such breach is known to the College, or by exercising reasonable diligence would have been known to the College. Following the discovery of a potential breach, the College shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach.

The Privacy Officer shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others at FCSRMC as appropriate (e.g. administration, human resources, public relations, legal counsel, etc.). The Privacy Officer shall be the key facilitator for all breach notifications processes to the appropriate entities (e.g. HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six (6) years.

A risk assessment will be performed and documented to determine whether the impermissible use or disclosure of PHI presents a significant risk to the employee as a result of the use or disclosure. The following factors should be considered to assess the potential risk:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person(s) who used or had access to the PHI or to whom the disclosure was made.
3. Whether the PHI was actually acquired or viewed.
4. The extent to which the risk to the PHI has been mitigated.

There are several exceptions to the Breach Notification Rule and in these instances no breach occurred:

1. PHI was unintentionally accessed or used by a workforce member or person acting under the authority of the College and the PHI was not further impermissibly used/disclosed.
2. PHI was inadvertently disclosed by an authorized person at the College to another authorized person at the College and the PHI was not further impermissibly used/disclosed.
3. The College has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

4. PHI was encrypted, destroyed or properly de-identified.

If there is high probability that a breach occurred, the Privacy Office must provide proper notification as outlined in the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.

MITIGATION: The College will mitigate, to the extent practicable, any harmful effects that are known that result from a use or disclosure of PHI in violation of its own privacy policies and procedures or its Business Associates. Mitigation is required, where practicable, for known harmful effects caused by the College's own workforce misusing or disclosing ePHI, or by such misuse or wrongful disclosure by a Business Associate of FCSRMC or the College. While appropriate steps to mitigate harm caused by an improper use or disclosure in an electronic environment will vary based on a totality of the circumstances, some mitigation steps may include:

1. Identifying the cause of the violation and amending privacy policies and technical procedures, as necessary, to assure it does not happen again.
2. Contacting the Systems Administrator, as well as other potentially affected entities, to try to retrieve or otherwise limit the further distribution of improperly disclosed information.
3. Notifying the individual of the violation if the individual needs to take self-protective measures to ameliorate or avoid the harm, as in the case of potential identify theft.

The Privacy Officer will maintain a *Breach Notification Log* for all confirmed HIPAA breaches. The Log will be maintained for a period of six (6) years.

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, 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 related 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 as 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

FCSRMC BUSINESS ASSOCIATE LISTINGS

Business Associate	Type of Service Provided	Contact Name	Contact Address	Contact Phone, Fax, Email
LifeWorks	EAP	Bob Separ		bob.separ@lifeworks.com 917-891-0335
Delta Dental	Dental Insurance	Tammy Adams		TAdams2@delta.org 210-355-6573 917-891-0335A
The Standard Life	Life Insurance	Christine D'Angelo		Christine.dangelo@standard.com 813-728-1879
VSP	Vision Insurance	Keisa Talley		Keisa.talley@vsp.com 678-628-1412
BDO	HIPAA Training & Assessment	Carol Crews	501 Riverside Ave., Suite 800, Jacksonville, FL 32202	904-224-9787 (phone) 904-399-4012 (fax) ccrews@bdo.com
Health Equity	Health Reimbursement Account	Tierrany Sepulveda-Daniels		Tierrany Sepulveda-Daniels tsdaniels@healthequity.com 214-492-8060
FBMC	Enrollment Maintenance Billing	Ray Griffin	FBMC Benefits Management, 3101 Sessions Rd, Tallahassee, FL 32303	850-425-6200 x 2105 rgriffin@fbmc.com
Florida Blue	Health Insurance	Greg Ferguson	Florida Blue, 4800 Deerwood Campus Parkway, DC 3-5, Jacksonville, FL 32246	904-905-8034 (phone) 904-257-8290 (fax) greg.ferguson@floridablue.com
Mercer	Consulting	Amy Tree		954-261-5668 (cell)

Revised: February 15, 2023