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Expiration Date: *This policy remains in effect until superseded or cancelled.*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