Wake County Medical Society Community Health Foundation, Inc.

CONFIDENTIAL

Wake County Medical Society Community Health Foundation, Inc.

HIPAA Privacy and Breach Notification Policies and Procedures

Index of HIPAA Privacy and Breach Notification Policies and Procedures

Formatted: Header distance from edge: 0.28"

Policy	**Policy Number**
MASTER POLICY	
Master Policy	P1.1
Related Policies	
Definitions	P1.2
Business Associate Agreements	P1.3
Non-Routine Uses and Disclosures	P1.4
Personal Representatives	P1.5
De-Identified Information/Re-Identification	P1.6
Sale of PHI	P1.7
Privacy Incident Reporting and Breach Notification	P1.8
Request for Restrictions	P1.9
Individual's Access to PHI	P1.10
Amendment	P1.11
Accounting of Disclosures	P1.12
Social Media Policy	P1.13
Training and Awareness *(This is the same as the Security Policy)*	P1.14/S4.1
Sanctions *(This is the same as the Security Policy)*	P1.15/S4.2
Privacy/Security Documentation *(This is the same as the Security Policy)*	P1.16/S4.3

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: MASTER POLICY**	
Policy # P1.1	**Rules Addressed: N/A**

1. Purpose:

The purpose of these policies and procedures (the "Policies and Procedures") is to ensure the privacy of each Individual's protected health information ("PHI") in accordance with HIPAA and the HIPAA Privacy Rule.

The HIPAA Privacy Rule governs the Use and Disclosure of PHI and applies to Covered Entities and Business Associates. WCMSCHF functions as a Business Associate of Covered Entities or Business Associates upstream when WCMSCHF creates, receives, maintains or transmits PHI from such Covered Entities or Business Associates upstream, in WCMSCHF's performance of services on behalf of such persons or organizations.

As a Business Associate, WCMSCHF must directly comply with certain provisions of the HIPAA Privacy Rule, the full HIPAA Security Rule and the Breach Notification Rule. To comply with the HIPAA Privacy Rule and Breach Notification Rule, WCMSCHF is implementing these Policies and Procedures to govern the Use and Disclosure of PHI received from, or created, maintained or transmitted by WCMSCHF on behalf of, Covered Entities or Business Associates upstream. Please see the HIPAA Security Policies and Procedures for WCMSCHF's security rules that pertain to PHI.

If you have questions about HIPAA or these Policies and Procedures, please contact the Privacy Officer.

Please also contact the Privacy Officer if you have questions about whether certain health information constitutes PHI that is subject to HIPAA.

2. Policy Organization:

This Master Policy provides an overview of WCMSCHF's policies and procedures governing the Use and Disclosure of PHI. This Master Policy references certain related policies (the "Related Policies") that provide more detailed information and procedures. Please see the Related Policies for more information where applicable.

Except as otherwise defined, all capitalized terms used in these Policies and Procedures shall have the meaning set forth in the Definitions Policy (P1.2).

3. Applicability:

All Employees must follow these Policies and Procedures when creating, Using or Disclosing PHI, regardless of the form of PHI (whether written, electronic or oral). No Employee may have access to PHI until he/she agrees to comply with these Policies and Procedures.

4. Privacy Officer:

All complaints about WCMSCHF's compliance with HIPAA, these Policies and Procedures and permitted Uses and Disclosures of PHI should be immediately directed to the Privacy Officer. The identity of the Privacy Officer is located on WCMSCHF's Intranet.

The Privacy Officer is responsible for: developing, implementing and the oversight of these Policies and Procedures; overseeing WCMSCHF's HIPAA compliance, monitoring the effectiveness of these Policies and Procedures and suggesting changes when necessary; reviewing and revising the Business Associate Agreements; developing and implementing WCMSCHF's training program with respect to these Policies and Procedures; performing annual information privacy risk assessments and conducting ongoing compliance monitoring activities; initiating and overseeing the completion of corrective action plans for violations of these Policies and Procedures; developing and maintaining any necessary HIPAA forms; serving as the contact person for individuals who have complaints and questions about how WCMSCHF Uses and Discloses PHI; and keeping abreast of developments under HIPAA and periodically revising these Policies and Procedures as necessary and with the approval of WCMSCHF's management.

5. General Rules for Access, Use and Disclosure of PHI:

- Only those Employees who are authorized by these Policies and Procedures may access PHI.

- Authorized Employees may access, Use and Disclose PHI only if a Business Associate Agreement is in place with the applicable Covered Entity and only to the extent permitted by the Business Associate Agreement. Please see the Business Associate Agreements Policy (P1.3) for Business Associate Agreement requirements.

- All Uses and Disclosures of PHI must be permitted by (a) the applicable Business Associate Agreement, (b) these Policies and Procedures, (c) HIPAA, and (d) applicable state and other federal laws.

- Employees must maintain and safeguard PHI in accordance with these Policies and Procedures and the WCMSCHF Security Policies and Procedures.

6. Employee Access to PHI:

WCMSCHF has identified in a Standard Operating Procedure the Employees or classes of Employees who need access to PHI to carry out their job functions, the categories of access needed and any conditions appropriate to such access. WCMSCHF will make reasonable efforts to limit the access of PHI in accordance with these designations.

If an Employee needs access to PHI to perform a job function and such access is not authorized by the Standard Operating Procedure, the Employee must obtain approval from their supervisor before accessing PHI. If such access is necessary for the Employee to perform a job function, their supervisor may authorize the access in writing and will document the authorization in accordance with the Privacy/Security Documentation Policy (P1.16/S4.3).

All WCMSCHF personnel will be given individual passwords to access PHI they need. Personnel will be permitted to view the fields they need to perform their job functions based on the access rights attributed to their account. For more information, please see WCMSCHF's HIPAA Security Policies and Procedures. Each password criteria will be set based on the requirements of the system being used (i.e. CMIS, Informatics Center/Provider Portal). Please see additional information in that system's documentation manual.

7. Permitted Uses and Disclosures of PHI:

Authorized by Business Associate Agreement. All Uses and Disclosures of PHI must be authorized under the applicable Business Associate Agreement pursuant to a valid permission set forth in such agreement. See the section entitled "**Valid Business Associate Permissions under HIPAA**" below for a list of such permissions. Please consult the Business Associate Agreement before Using or Disclosing PHI.

Notice of Privacy Practices. The Privacy Rule requires Covered Entities to provide Notice of Privacy Practices to their patients/clients. WCMSCHF is a Business Associate and not a Covered Entity. Therefore, HIPAA does not require WCMSCHF to and WCMSCHF does not provide a Notice of Privacy Practices to Individuals. WCMSCHF will, however, comply with any restrictions in the applicable Covered Entity's Notice of Privacy Practices of which WCMSCHF is made aware.

Minimum Necessary. WCMSCHF will, to the extent practicable, limit the Use, Disclosure, or request of PHI to the Limited Data Set or, if needed, to the minimum amount of PHI necessary to accomplish the intended Use, Disclosure, or request, respectively, in connection with requests for, or Uses and Disclosures of, PHI permitted under these Policies and Procedures. WCMSCHF and Employees will not Use, Disclose or request more than the minimum amount of PHI necessary to accomplish the intended Use, Disclosure, or request for PHI.

- **Routine Uses and Disclosures of PHI**. The following are "routine" Uses and Disclosures of PHI and may be made by Employees without consulting with the Privacy Officer in accordance with the following guidelines:
  - *Community Care of Wake and Johnston Counties:*
    - Purpose: For the coordination of care for Medicaid recipients and other commercial insurance members enrolled with our network programs as a group or individually.
    - Permitted Categories of PHI: Please see the Access, Use, and Disclosure Standard Operating Procedure for the list of permitted categories of PHI.
  - *CapitalCare Collaborative:*
    - Purpose: For the determination of program eligibility and improved health care outcomes for uninsured patients within Wake County.
    - Permitted Categories of PHI: Please see the Access, Use, and Disclosure Standard Operating Procedure for the list of permitted categories of PHI.

- **Non-Routine Uses and Disclosures of PHI**. Any Use or Disclosure of PHI not identified above as "routine" is considered "non-routine". Each non-routine Use or Disclosure of PHI must be approved by the Privacy Officer. The Privacy Officer will determine the minimum amount of PHI necessary for such non-routine Use or Disclosure in accordance with the criteria set forth in the Non-Routine Use and Disclosure Policy (P1.4).

- **Entire Medical Record**. WCMSCHF will not Use, Disclose, or request an entire medical record, except when the entire record is justified as the minimum amount necessary to accomplish a particular purpose.

- **Exceptions**. The "minimum necessary" standard does not apply to the following:
  - Disclosures to or requests by a health care provider for Treatment;
  - Disclosures of PHI made to the Secretary to determine WCMSCHF's or a Covered Entity's compliance with HIPAA;
  - Uses and Disclosures required by law, including for HIPAA compliance; and

- Disclosures pursuant to a HIPAA-compliant Individual authorization.

Valid Business Associate Permissions under HIPAA.

A Business Associate Agreement may permit WCMSCHF to Use or Disclose PHI for one or more of the following purposes.

Note: There may be permissible Uses and Disclosures that are not listed below, but which can be approved by the Privacy Officer upon request (see the section entitled, "**Involvement of Privacy Officer**" below).

Employees must confirm that the applicable Business Associate Agreement authorizes the permissible activity prior to Using or Disclosing PHI for such purpose:

- **To perform Business Associate Agreement or Services Agreement**. The Business Associate Agreement may permit WCMSCHF to Use or Disclose PHI for the purpose of meeting its obligations as set forth in a Business Associate Agreement or as required by an approved and executed services agreement or other contract between WCMSCHF and the applicable Covered Entity or Business Associate upstream.

- **Management and Administration of WCMSCHF**.
  - The Business Associate Agreement may permit WCMSCHF to Use PHI in its possession for its proper management and administration or to carry out any of its present or future legal responsibilities;
  - The Business Associate Agreement may permit WCMSCHF to Disclose PHI in its possession to third parties for WCMSCHF's proper management and administration or to fulfill any of its present or future legal responsibilities, provided that: (a) the Disclosures are "required by law" (as further described below); or (b) WCMSCHF has received from the third party written assurances that the PHI will be held confidentially, that the PHI will only be Used or further Disclosed as required by law or for the purpose for which it was Disclosed to the third party and that the third party will notify WCMSCHF of any instances of which it is aware in which the confidentiality of the information has been breached.

- **Data Aggregation Services**. The Business Associate Agreement may permit WCMSCHF to Use and Disclose PHI to provide data aggregation services relating to the Health Care Operations of a Covered Entity.

- **To the Individual**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI to the Individual who is the subject of the information.

- **Pursuant to Authorization**. The Business Associate Agreement may permit WCMSCHF to Use or Disclose PHI pursuant to an Individual's written authorization. Form Authorizations for Use or Disclosure of Protected Health Information are maintained by the Privacy Officer. Please see the Privacy Officer for the current version. See the "Individual Authorization Required to Use and Disclose PHI" section of this policy for more information about authorizations.

- **Treatment**. The Business Associate Agreement may permit WCMSCHF to Use or Disclose PHI for Treatment purposes of the Covered Entity.

Formatted: Font: Not Bold

Formatted: Indent: Left: 1", Space After: 0 pt, No bullets or numbering

- **Payment**. The Business Associate Agreement may permit WCMSCHF to Use or Disclose PHI for Payment purposes of the Covered Entity.

- **Health Care Operations**. The Business Associate Agreement may permit WCMSCHF to Use or Disclose PHI for Health Care Operations of the Covered Entity.

- **Family, Friends and Disaster Relief Organizations**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI related to an Individual's current condition to the Individual's family member, other relative, a close personal friend or any other person identified by the Individual who is involved in the Individual's care or Payment for care, or a disaster relief organization (for purposes of notifying an Individual's family member or personal representative), provided that the Individual: (a) is given an opportunity to agree or object to the Use or Disclosure of PHI and the Individual does not object; or (b) is not present, is incapacitated or cannot be given the opportunity to agree or object because of an emergency circumstance, but the Disclosure is consistent with a prior expressed preference of the Individual, if any, that is known to the covered health care provider, and is in the Individual's best interests in the exercise of professional judgment. If the Individual is deceased, the Business Associate Agreement may permit WCMSCHF to Disclose to a family member, other relative, a close personal friend or any other person identified by the Individual who is involved in the Individual's care or Payment for care prior to an Individual's death, PHI of the Individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the Individual that is known to the Covered Entity.

- **Public Health Activities**. The Business Associate Agreement may permit WCMSCHF to Use or Disclose PHI to: (a) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (b) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls and post-marketing surveillance; (c) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; (d) employers, regarding employees when requested by employers, for information concerning a work-related illness or injury or workplace-related medical surveillance, as such information is needed by the employer to comply with the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA) or similar state law; and (e) schools, if the PHI is limited to proof of immunization, are required by state law to have proof of immunization prior to admitting an Individual and the Covered Entity obtains and documents the agreement to the Disclosure by the parent, guardian or other person acting in loco parentis of the Individual or the Individual if the Individual is an adult or an emancipated minor.

- **Victims of Abuse, Neglect or Domestic Violence**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI to appropriate government authorities regarding victims of abuse, neglect or domestic violence.

- **Health Oversight Activities**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.

- **Judicial and Administrative Proceedings**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such

information may also be Disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the Individual or a protective order are provided.

- **Law Enforcement Purposes**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI to law enforcement officials for law enforcement purposes under the following circumstances: (a) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (b) to identify or locate a suspect, fugitive, material witness or missing person; (c) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (d) to alert law enforcement of a person's death if WCMSCHF suspects that criminal activity caused the death; and (e) when WCMSCHF believes that PHI is evidence of a crime that occurred on its premises.

- **Decedents**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI to funeral directors as needed and to coroners or medical examiners to identify a deceased person, to determine the cause of death and to perform other functions authorized by law.

- **Cadaveric Organ, Eye or Tissue Donation**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI to facilitate the donation and transplantation of cadaveric organs, eyes and tissue.

- **Research**. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge. The Business Associate Agreement may permit WCMSCHF to Disclose PHI for research purposes, without an Individual's authorization, provided that WCMSCHF obtains either: (a) documentation that an alteration or waiver of the Individual's authorization for the Use or Disclosure of PHI about the Individual for research purposes has been approved by an Institutional Review Board or Privacy Board; (b) representations from the researcher that the Use or Disclosure of the PHI is solely to prepare a research protocol or for a similar purpose preparatory to research, that the researcher will not remove any PHI from WCMSCHF and that PHI for which access is sought is necessary for the research; or (c) representations from the researcher that the Use or Disclosure sought is solely for research on the PHI of decedents, that the PHI sought is necessary for the research, and, at the request of WCMSCHF, documentation of the death of the Individuals about whom information is sought.

- **Serious Threat to Health or Safety**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI that it believes is necessary to prevent or lessen a serious and imminent threat to a person or the public when such Disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). WCMSCHF may also Disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

- **Essential Government Functions**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President of the United States, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution and determining eligibility for or conducting enrollment in certain government benefit programs.

- **Workers' Compensation**. The Business Associate Agreement may permit WCMSCHF to Disclose PHI as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

Required Uses and Disclosures of PHI.

Employees will *immediately* notify the Privacy Officer of requests that are purportedly required by law. All requests for Use/Disclosure of PHI as "required by law" must be approved by the Privacy Officer.

The term "required by law" includes, but is not limited to: court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury or a governmental or trial inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; and statutes or regulations that require the production of information, including statutes or regulations that require such information if Payment is sought under a government program providing public benefits and mandates contained in law that compel WCMSCHF to make a Use or Disclosure of PHI and that are enforceable in a court of law. This includes when WCMSCHF is compelled to release information from the North Carolina Community Care Networks, Inc. Informatics Center/Provider Portal or Case Management Information System.

If a Use or Disclosure of PHI is required by law, WCMSCHF may Use or Disclose PHI to the extent that the Use or Disclosure: (a) complies with such law, and (b) is limited to its legal requirements. In the event that two or more laws or regulations governing the same Use or Disclosure conflict, WCMSCHF will comply with the more restrictive laws or regulations.

Sale of PHI. Generally, WCMSCHF may not exchange PHI in exchange for direct or indirect remuneration. Certain limitations exist as described in the Sale of PHI Policy (P1.7).

Marketing. Generally, WCMSCHF may not Use or Disclose PHI for marketing purposes. Marketing purposes includes any communications about a product or service that encourages the recipient of the communication to purchase the product or service. However, to the extent permitted by the applicable Business Associate Agreement, WCMSCHF may communicate with an Individual for case management or care coordination purposes or to recommend alternative therapies, provided in each case that WCMSCHF does not receive payment for making such communication. Please consult with the Privacy Officer for other permitted exceptions.

De-Identification of PHI. WCMSCHF may only Use PHI to create de-identified information if such Use is expressly permitted under its Business Associate Agreements. Similarly, any activities involving the re-identification of de-identified information must be permitted under WCMSCHF's Business Associate Agreements. Any activities involving de-identification or re-identification of PHI will be coordinated through the Privacy Officer. Please see the De-Identified Information/Re-Identification Policy (P1.6) for more information.

Involvement of Privacy Officer. If you are unsure whether a Use or Disclosure of PHI is permitted or required by these Policies or Procedures or whether the Privacy Officer is required to handle a particular type of Use or Disclosure, please consult with the Privacy Officer. The following PHI requests are examples of Disclosures that must be handled by WCMSCHF's Privacy Officer:

- Requests from agencies, entities, or providers that have not entered into a Technology Enabled Care Coordination Agreement
- Individual requests (whether made directly by the Individual or by a Covered Entity) to access PHI, to restrict the Use or Disclosure of PHI or for accountings of Disclosures of PHI
- Requests made on behalf of the Secretary
- Activities involving the de-identification or re-identification of PHI
- Requests for the exchange of PHI for payment pursuant to the Sale of PHI Policy (P1.7)

- Requests for PHI required by law or other legal requests for PHI

8. Individual Authorization Required to Use and Disclose PHI:

WCMSCHF may not Use or Disclose PHI without a valid authorization from the Individual unless (a) the Use or Disclosure is permitted by the Business Associate Agreement and (b) at least one of the following exceptions apply:

- The Disclosure is required by law;
- The Disclosure is to the Personal Representative of the Individual;
- The Disclosure is for Treatment, Payment or Health Care Operations; or
- The Disclosure is otherwise permitted without an Individual's authorization by the HIPAA Privacy Rule.

All written authorizations must be obtained using the approved Authorization for Release/Request of the Individual. Information forms are to be maintained by the Privacy Officer. Please see the Privacy Officer for the current forms. However, any signed form presented by an Individual or his or her Personal Representative that contains the same information is acceptable.

Every authorization must be voluntary and the Individual may refuse to sign it. The authorization may be revoked in writing at any time to the extent it has not been acted upon.
The authorization must be documented and retained for a period of at least six years after it was created or expired, whichever is later, in accordance with the Privacy/Security Documentation Policy (P1.16/S4.3).

9. Individual Rights:

Individuals have the right to request to restrict or amend their PHI, the right to access or obtain a copy of their PHI and the right to an accounting of Disclosures of their PHI. All requests for such restrictions will be handled by the Privacy Officer. Employees will *immediately* notify the Privacy Officer upon receipt of any such request.

The Privacy Officer will handle all such requests in accordance with the Request for Restrictions Policy (P1.9), Individual's Access to PHI Policy (P1.10), Amendment Policy (P1.11) and Accounting of Disclosures Policy (P1.12).

10. Log Disclosures:

All Disclosures of PHI must be logged in the Data Disclosure Log unless one of the exceptions described below applies. If the Disclosure must be logged, the Employee must coordinate with the Privacy Officer prior to making the Disclosure so that the Privacy Officer can properly log the Disclosure. The Data Disclosure Log is located on the shared drive in the Privacy Folder. Please see the Accounting of Disclosures Policy (P1.12) for more information.

Exceptions - the following Disclosures do not need to be logged:

- for Treatment, Payment or Health Care Operations (this exception does NOT apply to Disclosures made through an Electronic Health Record);
- to an Individual concerning the Individual's PHI;
- incidental to a Use or Disclosure otherwise permitted or required by these Policies and Procedures;
- pursuant to a valid patient authorization;

- to persons assisting in an Individual's care (provided that the Individual had the opportunity to object to such Disclosures);
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials as provided for under the HIPAA Privacy Rule.

11. Personal Representatives:

WCMSCHF will treat the Personal Representative of an Individual just as it would treat the Individual with respect to Disclosures of PHI, access to PHI and exercise of the Individual's HIPAA rights, except as otherwise provided by this policy. Who may act as a "Personal Representative" is dictated by HIPAA. If you receive a request from someone requesting to act as a Personal Representative of an Individual, please see the Personal Representatives Policy (P1.5) to determine if the person is authorized to act as a Personal Representative.

12. Verification Requirements:

Before making any Disclosure of PHI, Employees must verify (a) the identity of the person requesting the PHI and (b) the authority of any such person to have access to PHI if the identity or authority of such person is not known to WCMSCHF. Further, if obtaining documentation, statements or representations (whether oral or written) is a condition of the Disclosure, WCMSCHF must obtain such documentation, statements or representations. WCMSCHF will rely on documentation, statements or representations that, on their face, meet the applicable requirements, provided that such reliance is reasonable under the circumstances.

- **Requests by Telephone**. If an Employee (a) knows a caller's voice and can confidently identify the caller in that manner or (b) can verify the identity of a caller using caller ID, the Employee can Disclose PHI to that individual if permitted by these Policies and Procedures.

- **Public Officials**. If the requester is a public authority, WCMSCHF must verify the ***identity*** and the ***authority*** of the public official to make the request.
  - Identity. WCMSCHF may reasonably rely on the following to verify the ***identity*** of the public official:
    - Presentation, in person, of an agency identification badge, official credential or other proof of government status;
    - Appropriate government letterhead if a request is made in writing; or
    - For Disclosures to a person purporting to act on behalf of a public official, a written statement on appropriate government letterhead that says that the person is acting under the government's authority.
  - Authority. WCMSCHF may reasonably rely on the following to verify the authority of the public official:
    - A written statement of the legal authority under which the information is requested or, if a written statement is impracticable, an oral statement of such authority; or
    - A warrant, subpoena, order or other legal process issued by a grand jury, all of which may be presumed to constitute legal authority.

13. Privacy Safeguards:

- **Protect PHI**. Employees must protect the confidentiality of PHI in accordance with these Policies and Procedures and the Standard Operating Procedures.

Employees should not leave PHI (including patient records) where unauthorized persons could access itthem or discuss PHI in public areas or where unauthorized persons could overhear the conversation. Employees are not permitted to leave outgoing voicemail messages, send unencrypted email or text message anything that involves or relates to PHI about any Individual.

For the administrative, technical and physical safeguards implemented by WCMSCHF to protect Electronic PHI, please refer to the HIPAA Security Policies and Procedures.

Certain service programs use contracted patient documentation/information systems that may have additional privacy and security requirements and features. Employees accessing these systems will receive education and training concerning these unique systems. This includes the Care Management Information Systems, Informatics Center/Provider Portal, Epic, Centricity, MediTech and MediLink.

- **Privacy Incidents and Breaches of PHI**. Company Employees will *immediately* report to the Privacy Officer any actual or suspected Breaches of PHI, Security Breaches, Privacy Incidents or any questionable Uses or Disclosures of PHI. Please immediately notify the Privacy Officer *by telephone* and *email to the extent email remains secure*. The Privacy Officer will investigate the report in accordance with the Privacy Incident Reporting and Breach Notification Policy (P1.8).

- **Mitigation**. WCMSCHF will take all reasonable steps necessary to mitigate any harmful effect of a Use or Disclosure of PHI in violation of the HIPAA Privacy Rule, a Business Associate Agreement, or these Policies and Procedures, of which WCMSCHF becomes aware. This requirement applies whether the harm is created by WCMSCHF or by one of its agents or subcontractors.

- **Confidentiality Agreements**. Employees will treat all information stored, handled and accessed by WCMSCHF as confidential. All new Employees must sign an Employee a Employee Confidentiality Agreement prior to accessing WCMSCHF's systems or partner systems. Employees will be required to re-sign a Confidentiality Agreement each year after HIPAA privacy and security awareness training. A current version of the Employee Employee Confidentiality Agreement is maintained by the Privacy and Security Officers.

  Contractors, vendors and external parties approved to access WCMSCHF must sign a Visitor Confidentiality Agreement prior to accessing WCMSCHF systems. A current version of the Visitor Confidentiality Agreement is located on the Intranet under the Privacy and Security section.

  If the contractor, vendor or other external party will have access to PHI, the party must sign a Business Associate Agreement prior to receiving access to the PHI or WCMSCHF's systems.

  Signed Confidentiality Agreements will be maintained and filed by the Security and Privacy Officers.

- **Dispose of PHI**. All PHI in paper, electronic or other format will be destroyed using an acceptable method of destruction after the appropriate document retention period has been met. Please see the Disposal of PHI Policy in the HIPAA Security Policies and Procedures for further guidelines.

- **Follow HIPAA Security Policies and Procedures**. The HIPAA Security Policies and Procedures set forth specific policies and procedures to safeguard PHI, including in paper and electronic formats. All Employees must comply with the HIPAA Security Policies and Procedures.

- **Comply with Social Media Policy**. Employees will comply with the Social Media Policy. Please see the Social Media Policy (P1.13) for more information.

14. Visitors:

Visitors to WCMSCHF must review and sign a Visitor Confidentiality Agreement. The approved form of Visitor Confidentiality Agreement is maintained by the Privacy Officer. Please see the Intranet's main page or the Privacy Officer for the current version. Employees should follow the Visitor Access Policy (S2.6). PHI will not be Disclosed to visitors except to the extent otherwise permitted by these Policies and Procedures.

15. Documentation:

WCMSCHF shall maintain all documentation required by these Policies and Procedures in accordance with the Privacy/Security Documentation Policy (P1.16/S4.3).

16. Training:

All Employees will receive regular training in accordance with the Training and Awareness Policy (P1.14/S4.1).

17. Privacy Complaints:

All complaints regarding compliance with these Policies and Procedures or HIPAA should be made directly to the Privacy Officer (regardless of whether involving the compliance of WCMSCHF or a Covered Entity, Business Associate, Sub-Business Associate, Employee or other individual or entity). If an Employee other than the Privacy Officer receives such a complaint, *immediately* forward the complaint to the Privacy Officer.

The Privacy Officer will investigate and take appropriate steps to resolve any complaints. The Privacy Officer will consult with the Security Officer and other appropriate parties as needed. The Privacy Officer will document all complaints received and their resolution, including the findings of any investigation. The Privacy Officer will maintain such documentation for at least six years from the date of creation in accordance with the Privacy/Security Documentation Policy (P1.16/S4.3).

If the Privacy Officer receives a complaint that a Sub-Business Associate has violated its privacy rules or procedures or the Business Associate Agreement, the Privacy Officer will follow the procedures and take corrective action as described in the Sub-Business Associate Agreement and the Business Associate Agreements Policy (P1.3).

WCMSCHF and Employer's personnel are prohibited from retaliating against any person who files a complaint with respect to WCMSCHF's compliance with HIPAA.

18. Requests from the Secretary:

If WCMSCHF receives a request made on behalf of the Secretary that WCMSCHF make its internal practices, books and records relating to the Use and Disclosure of PHI available to the Secretary, WCMSCHF will comply with the request in accordance with the "Permitted Uses and Disclosures"

section of this Master Policy and shall promptly notify the applicable Covered Entity of the request, unless otherwise directed by the Secretary. Employees must *immediately* notify the Privacy Officer of all requests made on behalf of the Secretary.

19. Non-Retaliation:

WCMSCHF and WCMSCHF personnel are prohibited from retaliating against any person who files a complaint with the Secretary or testifies, assists or participates in certain investigations, compliance reviews, proceedings and hearings related to WCMSCHF's compliance with HIPAA.

WCMSCHF and WCMSCHF personnel are also prohibited from retaliating against any Covered Entity, person or other entity for exercising its rights under a Business Associate Agreement or for participating in any process established by the HIPAA Privacy Rule or the Breach Notification Rule, such as reporting of a breach of a Business Associate Agreement by WCMSCHF to the Secretary.

20. Update to Policies and Procedures:

WCMSCHF will review these Policies and Procedures at least annually and will modify its Policies and Procedures (and corresponding forms) as necessary to comply with changes in law, including, without limitation, changes to the HIPAA Privacy Rule and HIPAA Security Rule. These changes must be promptly documented and implemented.

21. Sanctions:

Individuals found violating these Policies and Procedures will be subject to appropriate sanctions in accordance with the Sanctions Policy (P1.15/S4.2).

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 10, 2015 by Smith Anderson and Tara Robinson
Approved: July 28, 2015 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: DEFINITIONS**	
Policy # P1.2	**Rules Addressed: N/A**

Purpose: This Definitions Policy defines language that is used throughout the Privacy and Breach Notification Policies and Procedures.

Policy:

For purposes of these Policies and Procedures, the following definitions apply:

1. Breach:

Breach means the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which "compromises the security or privacy of the PHI." Breach does not include:

- Any unintentional acquisition, access or Use of PHI by an Employee or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under the HIPAA Privacy Rule;

- Any inadvertent Disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under the HIPAA Privacy Rule; or

- A Disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

Except as provided in this definition, an acquisition, access, Use or Disclosure of PHI in a manner not permitted under Subpart E of 45 C.F.R. Part 164 is *presumed* to be a Breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

- The unauthorized person who Used the PHI or to whom the Disclosure was made;

- Whether the PHI was actually acquired or viewed; and

- The extent to which the risk to the PHI has been mitigated.

Formatted: Indent: Left: 0.5"

Formatted: Indent: Left: 1", Space After: 0 pt, No bullets or numbering

2. Breach Notification Rule:

Breach Notification Rule means the "Breach Notification for Unsecured Protected Health Information" regulations issued by the United States Department of Health and Human Services Office for Civil Rights at 74 Fed. Reg. 42740 (Aug. 24, 2009), and 78 Fed. Reg. 5566 (Jan. 25, 2013), as codified at 45 C.F.R. Part 164, Subpart D.

3. Business Associate:

Business Associate means a person or organization that performs or assists in the performance of certain functions, activities or services on behalf of a Covered Entity or a Business Associate upstream that involves creating, receiving, maintaining or transmitting PHI. WCMSCHF often functions as a Business Associate.

Business Associates include (but are not limited to): A Health Information Organization, E-prescribing Gateway or other person that provides data transmission services with respect to PHI to a Covered Entity and that requires access on a routine basis to such PHI, a person or entity that offers a personal health record to one or more Individuals on behalf of a Covered Entity; a subcontractor that creates, receives, maintains or transmits PHI on behalf of the Business Associate.

Examples of such functions, activities or services include: data analysis, processing or administration; website hosting; utilization review; quality assurance; patient safety activities (listed at 42 C.F.R. § 3.20); billing; collections; benefit management; practice management; repricing; legal services; actuarial services; accounting and auditing services; consulting; data aggregation; management and administrative services; accreditation; financial services; or any other service in which the person or organization obtains PHI from or on behalf of a Covered Entity or another Business Associate. Employees are not considered Business Associates of WCMSCHF.

The exchange of PHI between providers of health care, for purposes of providing Treatment to an Individual, does not create a Business Associate relationship.

4. Business Associate Agreement:

Business Associate Agreement means a contract between a Business Associate and a Covered Entity or a Business Associate upstream pursuant to 45 C.F.R. § 164.504(e).

5. Covered Entity:

Covered Entity has the same meaning as the term "Covered Entity" set forth at 45 C.F.R. § 160.103, and includes: a health plan, a health care clearinghouse or a health care provider that conducts electronic transactions for which HIPAA standard transactions have been adopted.

6. Designated Record Set:

Designated Record Set means a group of records maintained by or for a Covered Entity that is: (a) the medical records and billing records about Individuals maintained by or for a covered health care provider; (b) the enrollment, Payment, claims adjudication and case or medical management record systems maintained by or for a health plan; or (c) Used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes PHI and is maintained, collected, Used or disseminated by or for a Covered Entity.

7. Disclose or Disclosure:

Disclosure means the release, transfer, provision of access to or divulging in any manner of information outside the entity holding the information.

8. Electronic Health Record:

Electronic Health Record means an electronic record of health-related information pertaining to an Individual that is created, gathered, managed and consulted by authorized health care personnel.

9. Electronic Media:

Electronic Media means:

- Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory card; and
- Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile and of voice via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

10. Electronic PHI:

Electronic PHI means PHI transmitted or maintained in Electronic Media. This includes email, text or any form of transmission where PHI is in an electronic medium.

11. Employees:

Employees means, solely with respect to these Policies and Procedures, any member of WCMSCHF's Workforce, including employees, volunteers, trainees, interns and temporary staff and other persons whose conduct, in the performance of work for WCMSCHF, is under the direct control of WCMSCHF, whether or not they are paid by WCMSCHF.

12. Employee Confidentiality Agreement:

Employee Confidentiality Agreement means an agreement between the applicable Employee and WCMSCHF, where the Employee agrees to, among other things, comply with the WCMSCHF privacy and security policies and procedures (including these Privacy Policies and Procedures and the Security Policies and Procedures) and to protect the confidentiality of WCMSCHF confidential information, including PHI, and proprietary information as further described in the Employee Confidentiality Agreement.[1]

~~12.~~13. Health Care Operations:

Formatted: Font: Not Bold

Formatted: Indent: Left: 0.5", No bullets or

[1] Note to WCMSCHF: We have revised the description of the Employee Confidentiality Agreement to cover confidentiality obligations, but not other issues such as non-solicitation obligations since this is outside of the scope of the HIPAA policies. There may be some instances where an employee negotiates the terms of the agreement, and we don't want those changes to be inconsistent with these Policies.

Health Care Operations means any of the following activities of a Covered Entity, to the extent that the activities are related to the Covered Entity's covered functions:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities, patient safety activities (as defined in 42 C.F.R. § 3.20), population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about Treatment alternatives; and related functions that do not include Treatment;
- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities;
- Except as prohibited under 45 C.F.R. § 164.502(a)(5)(i), underwriting, enrollment, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- Business management and general administrative activities of the entity, including, but not limited to:
    - Management activities relating to implementation of and compliance with the requirements of HIPAA;
    - Customer service, including the provision of data analyses for policy holders, plan sponsors or other customers, provided that PHI is not Disclosed to such policy holder, plan sponsor or customer;
    - Resolution of internal grievances;
    - The sale, transfer, merger or consolidation of all or part of a Covered Entity with another Covered Entity or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and
    - Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set and fundraising for the benefit of a Covered Entity.

~~13.~~14. HIPAA:

HIPAA means the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act and the HIPAA Privacy Rule and HIPAA Security Rule.

~~14.~~15. HIPAA Privacy Rule:

HIPAA Privacy Rule means the "Standards for Privacy of Individually Identifiable Health Information" set forth at 45 C.F.R. Parts 160 and 164, Subparts A and E.

~~15.~~16. **HIPAA Security Rule:**

HIPAA Security Rule means the "Security Standards" set forth at 45 C.F.R. Parts 160 and 164, Subparts A and C.

~~16.~~17. **HITECH Act:**

HITECH Act means Title XIII of the American Recovery and Reinvestment Act of 2009, known as the "Health Information Technology for Economic and Clinical Health Act."

~~17.~~18. **Individual:**

Individual means the person who is the subject of PHI and includes persons who are living or those who are deceased for 50 years or less.

~~18.~~19. **Individually Identifiable Health Information:**

Individually Identifiable Health Information is that subset of health information, including demographic information collected from an Individual, that:

- Is created by or received by a health care provider, health plan, employer or health care clearinghouse;
- Relates to the past, present or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present or future Payment for the provision of health care to an Individual; and
- That identifies the Individual or with respect to which there is a reasonable basis to believe that information could be used to identify the Individual.

~~19.~~20. **Limited Data Set:**

Limited Data Set means PHI that excludes the following direct identifiers of the Individual or of relatives, employers or household members of the Individual:

- Names;
- Postal address information, other than town or city, state and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and

Formatted: Indent: Left: 0.5", Space After: 0 pt

Formatted: Indent: Left: 0", Hanging: 0.5", Keep with next

Formatted: Keep with next

Formatted: Indent: Left: 0.5", Keep with next

- Full face photographic images and any comparable images.

~~20.~~21. Payment:

Payment means the activities undertaken by: (a) Except as prohibited under 45 C.F.R. § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (b) a health care provider or health plan to obtain or provide reimbursement for the provision of health care. The activities described in this definition relate to the Individual to whom health care is provided and include, but are not limited to:

- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts) and adjudication or subrogation of health benefit claims;
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance) and related health care data processing;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care or justification of charges;
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
- Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
    - Name and address;
    - Date of birth;
    - Social Security number;
    - Payment history;
    - Account number; and
    - Name and address of the health care provider and/or health plan.

~~21.~~22. Policies and Procedures:

Policies and Procedures means these HIPAA Privacy and Breach Notification Policies and Procedures.

~~22.~~23. Privacy Incident:

Privacy Incident means the acquisition, access, Use or Disclosure of PHI that is not permitted under WCMSCHF's Business Associate Agreement.

~~23.~~24. Privacy Officer:

Privacy Officer means the individual with WCMSCHF that holds such title, identified on WCMSCHF's intranet.

~~24.~~25. PHI or Protected Health Information:

PHI or Protected Health Information means Individually Identifiable Health Information transmitted or maintained in any format (written, electronic or oral) relating to an Individual (meaning those who are living or who have been deceased for 50 years or less), that WCMSCHF

has created, received, maintained or transmitted when functioning as a Business Associate of a Covered Entity or another Business Associate upstream.

~~25.~~26. **Secretary:**

Secretary means the Secretary of the United States Department of Health and Human Services ("HHS") or any other officer or employee of HHS to whom the Secretary's authority has been delegated.

~~26.~~27. **Security Breach:**

A Security Breach means an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal Use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to an Individual. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key will constitute a Security Breach. Good faith acquisition of personal information by an employee or agent of WCMSCHF for a legitimate purpose is not a Security Breach, provided that the personal information is not Used for a purpose other than a lawful purpose of WCMSCHF and is not subject to further unauthorized Disclosure.

~~27.~~28. **Security Officer:**

The individual with WCMSCHF that holds such title.

~~28.~~29. **Standard Operating Procedures:**

Standard Operating Procedures means those operating procedures that apply to a specific arrangement or project as determined by the Privacy Officer.

~~29.~~30. **Sub-Business Associate:**

Sub-Business Associate means any agent or subcontractor of a Business Associate that creates, receives, maintains or transmits PHI on behalf of the Business Associate, other than in the capacity of a member of the Workforce of such Business Associate. "Sub-Business Associate" is used for convenience in these Policies and Procedures. For clarity, references to "Sub-Business Associates" hereunder shall have the same meaning as "Business Associate" under HIPAA.

~~30.~~31. **Sub-Business Associate Agreement:**

Sub-Business Associate Agreement means a contract between a Business Associate and Sub-Business Associate as required under a Business Associate Agreement or 45 C.F.R. § 502(e).

~~31.~~32. **Technology-Enabled Care Coordination Agreement:**

Data used by Community Care of North Carolina ("CCNC") is governed by the Technology-Enabled Care Coordination Agreement ("TECCA"). The TECCA is an agreement that approved agencies, entities and providers can execute with CCNC in order to obtain access to CCNC's Informatics Center/Provider Portal.

~~32.~~33. **Treatment:**

Treatment means the provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a

health care provider with a third party, consultation between health care providers relating to a patient or the referral of a patient for health care from one health care provider to another.

~~33.~~34. **Use:**

Use means the sharing, employment, application, utilization, examination or analysis of information within an entity that maintains the information.

~~34.~~35. **Unsecured PHI:**

Unsecured PHI means PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance published at 74 Fed. Reg. 19006 (April 27, 2009), and in annual guidance published thereafter.

~~35.~~36. **WCMSCHF:**

WCMSCHF means Wake County Medical Society Community Health Foundation, Inc.

~~36. Worker Confidentiality, Non-Disclosure, Non-Solicitation Agreement:~~

~~The Worker Confidentiality, Non-Disclosure, Non-Solicitation Agreement states that Workforce members agree to comply with the WCMSCHF privacy and security policies and to protect the confidentiality of sensitive information, including PHI, and proprietary information as defined in this Agreement. This Agreement states that Workforce members agree to not solicit (as defined in this Agreement) any current or former WCMSCHF employees. A current version of this Agreement is maintained by the Privacy and Security Officers.~~

~~39.~~37. **Workforce:**

Workforce means employees, volunteers, trainees and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 10, 2015 by Smith Anderson and Tara Robinson
Approved: July 28, 2015 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: BUSINESS ASSOCIATE AGREEMENTS**	
Policy # P1.3	**Rules Addressed: 45 C.F.R. § 164.504(e)**

1. Purpose:

This Business Associate Agreements Policy explains the different types of Business Associate Agreement forms required under HIPAA that WCMSCHF is authorized to use, as well as the role of Employees and Privacy Officer with these agreements.

2. Synopsis:

HIPAA requires that Business Associates and Sub-Business Associates enter into written contracts with the Covered Entity or Business Associate, as applicable, to assure that appropriate measures are taken to Use, maintain, and Disclose PHI received from Covered Entities or Business Associates. This policy explains how these agreements are carried out within WCMSCHF.

3. Policy:

WCMSCHF is a Business Associate of Covered Entities. As a Business Associate, WCMSCHF enters into written contracts (known as "Business Associate Agreements") with Covered Entities providing Covered Entities satisfactory assurances that WCMSCHF will appropriately safeguard PHI received from Covered Entities. WCMSCHF also enters into written contracts (known as "Sub-Business Associate Agreements") with its Sub-Business Associates (i.e., subcontractors) to ensure that all Sub-Business Associates agree to the same restrictions, conditions and requirements that apply to WCMSCHF with respect to such information.

Business Associate Agreements are required to comply with Section 164.504(e) of the HIPAA Privacy Rule. The Privacy Officer is responsible for securing an executed Business Associate Agreement or Sub-Business Associate Agreement, as applicable, with all of WCMSCHF's Covered Entities and Sub-Business Associates. Employees should verify that the appropriate Business Associate Agreements are in place with the Privacy Officer prior to receiving, creating, maintaining or transmitting PHI.

4. Business Associate Agreements:

WCMSCHF has two types of Business Associate Agreements:

- *Business Associate Addendum* (between WCMSCHF and a Covered Entity). This agreement should be used with any Covered Entities for whom WCMSCHF functions as a Business Associate. The approved form of Business Associate Addendum is maintained by the Privacy Officer. Please see the Privacy Officer for the current version.

- *Sub-Business Associate Agreement* (between WCMSCHF and its Sub-Business Associate). This agreement should be used with any agents or subcontractors that create, receive, maintain or transmit PHI while performing services on behalf of

WCMSCHF. As required by 45 C.F.R. § 164.502(e) and the Business Associate Agreements with Covered Entities, WCMSCHF is required to ensure that any agents or subcontractors to whom WCMSCHF provides PHI received from, or created or received by WCMSCHF on behalf of, Covered Entities (known as "Sub-Business Associates") agree to the same restrictions and conditions that apply to WCMSCHF with respect to such PHI. Such agreements should take the form of a Sub-Business Associate Agreement. The approved form of Sub-Business Associate Agreement is maintained by the Privacy Officer. Please see the Privacy Officer for the current version.

Any non-standard Business Associate Agreements or modifications to current Business Associate Agreements must be approved by the Privacy Officer and Executive Director prior to execution.

5. Sub-Business Associate's Breach of Sub-Business Associate Agreement:

If WCMSCHF knows of a pattern of activity or practice of a Sub-Business Associate that constitutes a material breach of the Sub-Business Associate Agreement with WCMSCHF, WCMSCHF should take reasonable steps to cure the breach or end the violation by the Sub-Business Associate. If unsuccessful, WCMSCHF should terminate the Business Associate Agreement and the underlying arrangement with the Sub-Business Associate, if feasible. The Privacy Officer will have the authority to terminate a Business Associate Agreement and the underlying arrangement, subject to the approval of WCMSCHF's management. If termination of the Business Associate Agreement and the underlying agreement is unfeasible, Business Associate should notify the Secretary of the problem.

If an Employee knows or suspects of a pattern of activity or practice of a Sub-Business Associate that constitutes a material breach of the Business Associate Agreement (including any HIPAA violation), the Employee will promptly notify the Privacy Officer. The Privacy Officer will investigate such reports and take action as required by these Policies and Procedures.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 10, 2015 by Smith Anderson and Tara Robinson
Approved: July 28, 2015 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: NON-ROUTINE USES AND DISCLOSURES**	
Policy # P1.4	**Rules Addressed: 45 C.F.R. § 164.514(d)** **NCQA Standard: CM 9: A.2**

1. Purpose:

This Non-Routine Uses and Disclosures Policy addresses the non-routine sharing of PHI as it applies to the "minimum necessary" standard.

2. Policy:

HIPAA requires that only the "minimum necessary" amount PHI is Used, Disclosed, or requested. Routine Uses and Disclosures of PHI are addressed in the "Permitted Uses and Disclosures" section of the Master Policy (P1.1), and may be handled by Employees without the involvement of the Privacy Officer. Any Use or Disclosure of PHI not identified as "routine" in the Master Policy (P1.1) is considered "non-routine", and must be reviewed on an individual basis by the Privacy Officer to determine the minimum amount of PHI reasonably necessary for the purpose of the request.

3. Criteria for Determining Minimum Necessary:

In response to a non-routine Use or Disclosure of PHI, the criteria for determining the minimum amount of PHI necessary to accomplish the purpose of a request or Disclosure include:

- How much information is being requested;
- If all the information to be provided is relevant to the stated purpose of the Use or Disclosure;
- Whether the information is particularly sensitive;
- Whether the requesting party could accomplish its purpose with de-identified information; and
- Such other criteria as the Privacy Officer deems appropriate under the surrounding facts and circumstances.

4. Entire Medical Records:

WCMSCHF will not Use, Disclose or request an entire medical record except when the entire record is specifically justified as the minimum amount necessary to accomplish a particular purpose.

5. Exceptions to Minimum Necessary Standard:

The "minimum necessary" standard does not apply in the following circumstances:

- Disclosures to or requests by a health care provider for Treatment;

- Disclosures of PHI made to the Secretary to determine WCMSCHF's or a Covered Entity's compliance with HIPAA;
- Uses and Disclosures required by law, including for HIPAA compliance; and
- Disclosures pursuant to a HIPAA-compliant Individual authorization.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 16, 2015 by Smith Anderson and Tara Robinson
Approved: July 28, 2015 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: PERSONAL REPRESENTATIVES**	
Policy # P1.5	**Rules Addressed: 45 C.F.R. § 164.502(g)**

1. Policy:

WCMSCHF will treat the Personal Representative of an Individual just as it would treat the Individual with respect to Disclosures of PHI access to PHI, and exercise of the Individual's HIPAA rights, except as otherwise provided by this policy.

The HIPAA Privacy Rule specifies who may act as a Personal Representative for the following three categories of Individuals:

If the Individual is . . .	**then the Personal Representative is . . .**
a deceased Individual (or the deceased Individual's estate)	the executor, administrator or other person who has the authority under state law to act on behalf of the deceased Individual or the Individual's estate.
an adult or emancipated minor	the person who has the authority under state law to act on behalf of the adult or emancipated minor in making decisions related to health care.
an unemancipated minor	the parent, guardian or a person acting in the place of a parent who has the authority under applicable state law to act on behalf of an unemancipated minor in making decisions related to health care.

Special requirements apply regarding who can be a Personal Representative of an unemancipated minor. A person may not be a Personal Representative of an unemancipated minor, and the minor has the authority to act as the Individual with respect to PHI pertaining to a health care service, if:

- the minor consents to such health care service; no other consent to such service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as a personal representative;
- the minor may lawfully obtain such health care service without the consent of a parent, guardian or other person acting in the place of a parent; and the minor, a court or another person authorized by law consents to such health care service; or
- a parent, guardian or other person acting in the place of a parent assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

Notwithstanding any other policy described above, including applicable state law, WCMSCHF may elect not to treat a person as a Personal Representative if WCMSCHF has a reasonable belief that:

- the Individual has been or may be subjected to domestic violence, abuse or neglect by such person or treating such person as the Personal Representative could endanger the Individual; and
- WCMSCHF, in the exercise of professional judgment, decides that it is not in the best interests of the Individual to treat the person as the Individual's Personal Representative.

Revision History:
Effective: August 16, 2011
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: DE-IDENTIFIED INFORMATION/RE-IDENTIFICATION**	
Policy # P1.6	**Rules Addressed: 45 C.F.R. § 164.514(b)**

1. Purpose:

This De-Identified Information/Re-Identification Policy describes the conditions that meet the definition of "de-identified information."

2. Synopsis:

When information does not identify an Individual and there is no reasonable basis to believe that it can be Used to identify an Individual, it is considered "de-identified" and is not considered to be PHI. There are certain criteria that define whether or not PHI has been de-identified as described in this Policy. The HIPAA Privacy Rule does not restrict the Use or Disclosure of information that is de-identified in accordance with 45 C.F.R. § 164.514(b).

3. Policy:

Use of PHI to Create De-Identified Information. WCMSCHF may only Use PHI to create de-identified information if such Use is expressly permitted under its Business Associate Agreements. Similarly, any activities involving the re-identification of de-identified information must be permitted under WCMSCHF's Business Associate Agreements. Any activities involving de-identification or re-identification of PHI will be coordinated through the Privacy Officer.

De-Identified Information. Information is de-identified only if the following conditions are met and WCMSCHF does not have knowledge that the information could be Used alone or in combination with other information to identify the Individual: (a) a person with appropriate knowledge of and experience with statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk of the anticipated recipient being able to identify an Individual is small and documents the methods and results of such analysis; or (b) the following identifiers are removed:

- Names;
- Geographic subdivisions smaller than a state;
- All elements of dates (except year) for dates directly related to an Individual and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;

- Certificate/license numbers;
- Vehicle identifiers and serial numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic or code.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: SALE OF PHI**	
Policy # P1.7	**Rules Addressed: HITECH Act § 13405**

1. Purpose:

This Sale of PHI Policy addresses the prohibitions and exceptions to prohibitions on sale of PHI.

2. Synopsis:

Employees will not exchange PHI for payment unless it falls under one of the exceptions listed in this Policy and requires the approval of the Privacy Officer.

3. Policy:

Prohibition on Sale of PHI. WCMSCHF shall not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless the Covered Entity obtained from the Individual a valid authorization in accordance with 45 C.F.R. § 164.508 that states that the Disclosure will result in remuneration to the Covered Entity or Business Associate.

Likewise, arrangements involving the *payment* by WCMSCHF of direct or indirect remuneration in exchange for PHI must be reviewed in advance by the Privacy Officer for appropriate authorizations and vetting.

Exceptions to Prohibition on Sale of PHI. If the purpose of the exchange is for any of the following reasons, the prohibition above does not apply as long as the activity is expressly permitted in writing by the respective Covered Entity and is approved by the Privacy Officer:

- For public health activities;
- For research if the remuneration received is a reasonable cost-based fee that reflects the costs of preparation and transmittal of the data for such purpose;
- For the Treatment of the Individual or Payment purposes, subject to any regulation the Secretary may promulgate to prevent PHI from inappropriate access, Use or Disclosure;
- For the sale, transfer, merger or consolidation of all or part of a Covered Entity with another Covered Entity or an entity that, following such activity, will become a Covered Entity and due diligence related to such activity;
- For remuneration provided by a Covered Entity to a Business Associate, or by a Business Associate to a subcontractor of the Business Associate, for activities involving the exchange of PHI that the Business Associate or the subcontractor of a Business Associate undertakes on behalf of and at the specific request of the Covered Entity or the Business Associate pursuant to a Business Associate Agreement or Sub-Business Associate Agreement, as applicable;
- To provide an Individual with a copy of the Individual's PHI pursuant to 45 C.F.R. §§ 164.524 and 164.528;
- For Disclosures required by law, as permitted under 45 C.F.R. § 164.512(a); and

- Any other purpose permitted by Subpart E of 45 C.F.R. § 164 where the only remuneration received by the Covered Entity or Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

All requests for the exchange of PHI in exchange for remuneration or payment will be handled by the Privacy Officer. Employees will immediately notify the Privacy Officer of any such requests.

Additional Guidance and State Laws. WCMSCHF will comply with any additional guidance issued by the Secretary with respect to the sale of PHI or more stringent obligations imposed under Business Associate Agreements or applicable state laws.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: PRIVACY INCIDENT REPORTING AND BREACH NOTIFICATION**	
Policy # P1.8	**Rules Addressed: 45 C.F.R. § 164.410** **NCQA Standard: CM 9: C.2, C.3**

1. Purpose:

This Privacy Incident Reporting and Breach Notification Policy provides direction on the breach notification requirements under the Breach Notification Rule and applicable state laws, including without limitation the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. § 75-60 et. seq. (such applicable state laws, collectively, the "State Breach Notification Laws").

2. Synopsis:

Employees will notify Privacy Officer of any Breaches of PHI, Security Breaches, or Privacy Incidents, as well as questionable Uses or Disclosures of any information that identifies or could be Used to identify an Individual, so that WCMSCHF can respond appropriately, including providing applicable notifications to applicable Covered Entities, agencies and Individuals pursuant to the Breach Notification Rule and State Breach Notification Laws.

3. Policy:

Incident Reporting (Employees). Employees will immediately notify the Privacy Officer *by telephone* and e*mail to the extent email remains secure* if the Employee knows of or suspects any unauthorized access, Use or Disclosure of PHI or any information that identifies or could be Used to identify an Individual, including without limitation: Social Security or employer taxpayer identification numbers; driver's license, state identification card or passport numbers; checking account numbers; savings account numbers; credit card numbers; debit card numbers; personal identification (PIN) codes; electronic identification numbers, electronic mail names or addresses, internet account numbers or internet identification names; digital signatures; any other numbers or information that can be Used to access an Individual's financial resources; biometric data; fingerprints; passwords; or a parent's legal surname prior to marriage. If you think the email system is compromised by the suspected incident, do not use email to report the incident to the Privacy Officer. Please use the telephone instead.

Investigating Incidents and Breaches. The Privacy Officer, in consultation with the Security Officer, WCMSCHF management and legal counsel, as necessary, shall investigate and evaluate reported and detected Breaches of PHI, Security Breaches or Privacy Incidents, as well as questionable Uses or Disclosures of any information that identifies or could be Used to identify an Individual. The Privacy Officer, in consultation with the Security Officer, WCMSCHF management and legal counsel, as necessary, will evaluate the event and analyze the appropriate response under the Breach Notification Rule and State Breach Notification Laws. These efforts will include conducting a risk assessment to determine whether the unauthorized access, Use or Disclosure constituted an event subject to the Breach Notification Rule and/or State Breach Notification Laws.

The Privacy Officer will document the risk assessment in writing and will maintain such documentation in accordance with these Policies and Procedures. The risk assessment should be documented in writing using the Privacy and Security Incident Report form (a copy of the form is maintained by the Privacy Officer) or using a similar form or format. Following the risk assessment, the Privacy Officer, in consultation with WCMSCHF management and legal counsel, as necessary, will notify appropriate entities as described below.

4. Breach of Unsecured PHI:

Timeline for Notification. Following the risk assessment by the Privacy Officer, if it is determined that a Breach of Unsecured PHI has occurred, WCMSCHF will provide notification to applicable Covered Entities in accordance with the Business Associate Agreement with such Covered Entities. In all cases, notification will occur without unreasonable delay and in no event later than 60 calendar days following discovery of a Breach or in such earlier timeframe required under the Business Associate Agreement pertaining to such information.

Discovery of Breach. Unless the law indicates otherwise, a Breach will be treated as discovered by WCMSCHF as of the first day on which such Breach is known to WCMSCHF or, by exercising reasonable diligence, would have been known to WCMSCHF. WCMSCHF will be deemed to have knowledge of a Breach if the Breach is known or by exercising reasonable diligence would have been known to any person, other than the person committing the Breach, who is an employee, officer or other agent of WCMSCHF.

Contents of Notice. The notification to Covered Entities will include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by WCMSCHF to have been, accessed, acquired, Used or Disclosed during the Breach. WCMSCHF will provide Covered Entities with any other available information that the Covered Entity is required to include in the notification to the Individual under the Breach Notification Rule at the time of the notification or promptly thereafter as information becomes available, including:

- a brief description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;
- a description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);
- any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
- a brief description of what WCMSCHF is doing to investigate the Breach, to mitigate harm to Individuals and to protect against any further Breach; and
- contact procedures for Individuals to ask questions or learn additional information, which will include a toll-free telephone number, an email address, Website or postal address.

Delays for Criminal Investigations. If a law enforcement official states to WCMSCHF that a notification required hereunder would impede a criminal investigation or cause damage to national security, WCMSCHF will:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification for the time period specified by the official; or
- If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification temporarily but no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

Burden of Demonstrating Breach Notification. In the event of a Use or Disclosure in violation of the HIPAA Privacy Rule, WCMSCHF will have the burden of demonstrating that all notifications were made as required by the Breach Notification Rule or that the Use or Disclosure did not constitute a Breach.

5. Use or Disclosure of PHI not Permitted under Business Associate Agreement:

Following the risk assessment by the Privacy Officer, if it is determined that a Breach or other Use or Disclosure of PHI not permitted under WCMSCHF's Business Associate Agreements has occurred, WCMSCHF will provide notification to applicable Covered Entities in accordance with the Business Associate Agreement with such Covered Entities or individuals, as applicable in accordance with other applicable laws.

6. Security Breach:

Following the risk assessment by the Privacy Officer, if it is determined that a Security Breach has occurred, WCMSCHF will provide notification to appropriate entities as required under the North Carolina Identity Theft Protection Act or other applicable State laws. The Privacy Officer will consult with legal counsel, as necessary, to determine the entities required to receive notification and the contents of the notification. The notification will be sent without unreasonable delay and as otherwise in accordance with WCMSCHF's Business Associate Agreements.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 16, 2015 by Smith Anderson and Tara Robinson
Approved: July 28, 2015 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard

Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: REQUEST FOR RESTRICTIONS**	
Policy # P1.9	**Rules Addressed: 45 C.F.R. § 164.522** **NCQA Standard: CM 9: A.5**

1. Purpose:

The purpose of this Right to Request Restrictions Policy is to address how WCMSCHF will handle an Individual's request for restrictions.

2. Policy:

The HIPAA Privacy Rule allows an Individual to request restrictions on the Uses and Disclosures of his or her PHI.

All requests for restrictions will be handled by the Privacy Officer. Employees will *immediately* notify the Privacy Officer upon receipt of any such requests.

If WCMSCHF receives a request directly from an Individual to restrict Uses and Disclosures of PHI, WCMSCHF will promptly notify the applicable Covered Entity of the request. WCMSCHF agrees to comply with any requests for restrictions to which a Covered Entity has agreed and of which WCMSCHF has been notified by Covered Entity, except where such Use, Disclosure or request is required or permitted under applicable law.

WCMSCHF will comply with an Individual's request to restrict Disclosures of PHI, of which WCMSCHF has been notified by Covered Entity, if: (a) the Disclosure is to a health plan for purposes of carrying out Payment or Health Care Operations (and is not for purposes of carrying out emergency Treatment); and (b) the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket, in full.

The restriction must be documented and retained for a period of at least six years after it was created or expired, whichever is later, in accordance with the Privacy/Security Documentation Policy (P1.16/S4.3).

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: INDIVIDUAL'S ACCESS TO PHI**	
Policy # P1.10	**Rules Addressed: 45 C.F.R. § 164.524**

1. Purpose:

The purpose of this Individual's Access to PHI Policy is to explain how WCMSCHF handles Individuals' requests to access their PHI.

2. Policy:

Individual Right to Access. The HIPAA Privacy Rule provides an Individual with the right to access, inspect and obtain a copy of his or her PHI for as long as the information is maintained. However, this right of access excludes Psychotherapy Notes, as defined in the HIPAA Privacy Rule; any and all information compiled in anticipation of, or for Use in, a civil, criminal or administration action or proceeding; information protected by the Clinical Laboratory Improvements Amendments of 1988, codified at 42 U.S.C. § 263a. (CLIA); certain information pertaining to inmates; and information obtained from a third party other than a health care provider under a promise of confidentiality which, if Disclosed, would likely reveal the source of the information.

Access Request Approval by Privacy Officer. All Individual requests to access their PHI will be handled by the Privacy Officer and will follow the conditions of the current Business Associate Agreement with the applicable Covered Entity and these Policies and Procedures. Employees should *immediately* notify the Privacy Officer upon the receipt of any such requests. Individuals or their legal guardian must complete the Patient Request to Access Records form, a copy of which is maintained by the Privacy Officer. Please see the Privacy Officer for the current version.

Requests to Access PHI in a Designated Record Set. If WCMSCHF receives a request directly from an Individual to access PHI, WCMSCHF will promptly notify the applicable Covered Entity of the request. If PHI is maintained in a Designated Record Set by WCMSCHF, and, if an Individual requests access to such PHI from a Covered Entity or WCMSCHF or if the Covered Entity requests access, WCMSCHF will provide the PHI to the applicable Covered Entity upon request. As a Business Associate of the Division of Medical Assistance (DMA), WCMSCHF is not permitted to provide a hard copy of claims-based information to Medicaid recipients; these requests must be directed to DMA. WCMSCHF may, if requested to do so by Covered Entity, provide access to PHI directly to the requesting Individual.

Requests to Access PHI in Electronic Health Records. The HITECH Act provides that, if a Covered Entity Uses or maintains an electronic health record with respect to PHI, an Individual has a right to access his or her PHI in an electronic format and to direct the Covered Entity to transmit a copy of such PHI directly to a designated person or entity. WCMSCHF will use reasonable efforts to comply with an Individual's right to receive his or her PHI in an electronic format, as directed by a Covered Entity.

Form and Fees. WCMSCHF will make PHI available in the format and medium directed by the Covered Entity, which may include electronic formats or media. WCMSCHF may not charge a

fee for this service and may only charge for actual costs incurred that are reasonable in amount and approved in advance by the Covered Entity.

Documentation. The Designated Record Sets that are subject to access by Individuals and the titles of persons or offices responsible for receiving and processing requests for access by Individuals must be documented and retained for a period of at least six years after it was created or expired, whichever is later, in accordance with the Privacy/Security Documentation Policy (P1.16 /S4.3).

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 16, 2015 by Smith Anderson and Tara Robinson
Approved: July 28, 2015 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: AMENDMENT**	
Policy # P1.11	**Rules Addressed: 45 C.F.R. § 164.526** **NCQA Standard: CM 9: A.6**

Under the HIPAA Privacy Rule, an Individual generally has the right to have a Covered Entity amend his or her PHI for as long as the information is maintained.

All requests to amend PHI will be handled by the Privacy Officer and will follow the conditions of the current Business Associate Agreement with the applicable Covered Entity. Employees should *immediately* notify the Privacy Officer upon the receipt of any such requests.

If WCMSCHF receives a request directly from an Individual to amend his or her PHI, WCMSCHF will promptly notify the applicable Covered Entity of the request. If an Individual or Covered Entity requests an amendment to PHI maintained by WCMSCHF in a Designated Record Set, WCMSCHF will, upon request of the applicable Covered Entity, (1) provide the PHI to the Covered Entity for amendment, and (2) incorporate any amendments.

The titles of the persons or offices responsible for receiving and processing requests for amendments by Individuals and the amended PHI must be documented and retained for a period of at least six (6) years after it was created or expired, whichever is later, in accordance with the Privacy/Security Documentation Policy (P1.16/S4.3).

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: ACCOUNTING OF DISCLOSURES**	
Policy # P1.12	**Rules Addressed: 45 C.F.R. § 164.528(a)(2) and Section 13405(c) of the HITECH Act** **NCQA Standard: CM 9: A.7**

1. Purpose:

The purpose of this Accounting of Disclosures Policy is to explain how an accounting of Disclosures of PHI can be shared with the requesting Individual.

2. Policy:

Individual Right to Accounting of Disclosures. An Individual generally has the right to receive an accounting of Disclosures of PHI made by WCMSCHF and its agents and subcontractors during the six years prior to the Individual's request. If PHI is maintained in a Designated Record Set by WCMSCHF and if an Individual or Covered Entity requests an accounting of Disclosures of such PHI, WCMSCHF will provide the necessary information to the applicable Covered Entity (or directly to the Individual upon Covered Entity's request) to allow Covered Entity to provide an accounting of Disclosures to the Individual. If WCMSCHF receives a request directly from an Individual to receive an accounting of Disclosures of PHI made by WCMSCHF, WCMSCHF will promptly notify the applicable Covered Entity of the request.

Disclosures of PHI subject to an accounting will be documented in the Data Disclosure Log, located on the shared drive in the Privacy Folder and is available to Employees who need access for a business purpose.

Exceptions to Right to Accounting of Disclosures. Individuals do not have the right to receive an accounting of Disclosures: (a) when the Individual's right is temporarily suspended upon request by law enforcement or a health oversight agency as provided in 45 C.F.R § 164.528(a)(2); or (b) with respect to Disclosures:

- for Treatment, Payment or Health Care Operations (this exception does NOT apply to Disclosures made through an Electronic Health Record; see below for more information);
- to an Individual concerning the Individual's PHI;
- incident to a Use or Disclosure otherwise permitted or required by these Policies and Procedures;
- pursuant to a valid patient authorization;
- to persons assisting in an Individual's care (provided that the Individual had the opportunity to object to such Disclosures);
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials as provided under the HIPAA Privacy Rule; or
- that occurred prior to April 14, 2003.

No Exception for Certain Disclosures through Electronic Health Records. As a result of the HITECH Act, the exception to the accounting of Disclosures requirement for Treatment, Payment, and Health Care Operations does not apply to Disclosures made through an electronic health record. However, an Individual only has the right to receive an accounting of such Disclosures during the three-year period prior to the date of the Individual's request.

Consultation with Privacy Officer. Unless a Disclosure of PHI falls within one of the exceptions to the accounting requirement listed above, Employees are required to consult with the Privacy Officer prior to making a Disclosure of PHI so that the required information can be logged. The Privacy Officer and/or his or her designee will be responsible for maintaining the log. All requests for an accounting of disclosures of PHI will be handled by the Privacy Officer and will follow the conditions of the current Business Associate Agreement with the applicable Covered Entity. Employees should *immediately* notify the Privacy Officer upon the receipt of any such requests.

Content of Accounting of Disclosures. Upon receiving a request from a Covered Entity for an accounting of Disclosures of an Individual's PHI, WCMSCHF (through the Privacy Officer) will provide an accounting within the time frame specified in the Business Associate Agreement. Each accounting must generally contain the following information:

- the date of each Disclosure;
- the name of the entity or person who received the PHI and, if known, their last known address;
- a brief description of the PHI Disclosed; and
- a brief statement of the purpose of the Disclosure that reasonably informs the Individual of the basis for the Disclosure or, in lieu of such statement, a copy of a written request for a Disclosure, if any.

Documentation. The following information must be documented and retained for a period of at least six years after it was created or expired, whichever is later, in accordance with the Privacy/Security Documentation Policy (P1.16/S4.3): the information required to be included in an accounting of Disclosures of an Individual's PHI, the written accounting that is provided to the Individual and the titles of the persons or offices responsible for receiving and processing requests for an accounting by an Individual.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Tara Robinson
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 16, 2015 by Smith Anderson and Tara Robinson
Approved: July 28, 2015 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Policy: SOCIAL MEDIA**	
Policy # P1.13	**Rules Addressed: N/A**

1. Purpose:

The Social Media Policy defines the use of social media in such a way that protects WCMSCHF's confidential and sensitive information.

2. Synopsis:

WCMSCHF understands that social media can be a fun way to share your life, opinions and pictures with family and friends. However, the use of social media presents certain risks and carries with it certain responsibilities. This policy is developed to assist Employees in making responsible decisions about their use of social media, only inasmuch as it impacts the function of our organization and staff. Nothing in this Company's social media policy is designed to interfere with, restrain or prevent Employee communications regarding wages, hours or other terms and conditions of employment. Employees have the right to engage in or refrain from such activities.

3. Policy:

- Social media includes all means of communicating or posting information or content of any sort on the Internet, including your own or someone else's weblog, blog, journal or diary, personal website, social networking or affinity website, web bulletin board or chat room, whether or not associated or affiliated with WCMSCHF as well as any other form of electronic communication.
- Employees are ultimately responsible for what they post online and any risks or rewards involved.
- Any conduct that adversely affects an Employee's job performance, the performance of fellow Employees or otherwise affects members, customers, suppliers, people who work on behalf of WCMSCHF or WCMSCHF's legitimate business interests may result in disciplinary action up to and including termination.
- Inappropriate postings that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject the Employee to disciplinary action up to and including termination.
- Always be fair and courteous to fellow Employees, members, customers, suppliers, and people who work on behalf of WCMSCHF. Keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers or by utilizing Human Resources or the Employee Assistance Program than by posting complaints to a social media outlet. If you decide to post complaints or criticisms, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, and threatening or intimidating, that disparage or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, relation or another other status protected by law or company policy.

- Avoid offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, relation or any other status protected by law or company policy.
- Be honest and accurate regarding statements about WCMSCHF, Employees, partners and associates; if a mistake is made, correct it promptly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about WCMSCHF, fellow employees, members, customers, suppliers, or people working on behalf of WCMSCHF.
- Maintain the confidentiality of WCMSCHF's sensitive, private or confidential information including systems, processes, products, know-how, technology or activities. Do not post internal reports, policies, procedures or other internal business-related confidential communications.
- Do not create a link from your blog, website or other social networking site to a WCMSCHF website without identifying yourself as a WCMSCHF employee.
- Express only your personal opinions and never represent yourself as a spokesperson for WCMSCHF.
- If your post is about WCMSCHF, make sure you specify that you are an Employee, that your views do not represent those of WCMSCHF, fellow Employees, members, partners, customers, suppliers or those working on behalf of WCMSCHF.
- If you are posting about your position or work related to WCMSCHF, make clear that you are not speaking on behalf of WCMSCHF. It is best to use a disclaimer such as "The postings on this site are my own and do not necessarily reflect the view of WCMSCHF".
- Minimize use of social media while at work in compliance with all WCMSCHF policies.
- Do not use your WCMSCHF email address to register on social networks, blogs or other online tools utilized for personal use.
- WCMSCHF prohibits taking negative action against any Employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any Employee who retaliates against another Employee for report of a possible deviation from this policy will be subject to disciplinary action, up to and including termination.
- Employees should not speak to the media on WCMSCHF's behalf without contacting the Executive Director. All media inquiries should be directed to the Executive Director.

Revision History:
Created: July 13, 2015 by Smith Anderson, Hazen Weber, and Tara Robinson
Approved: July 28, 2015 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES **HIPAA SECURITY POLICIES AND PROCEDURES** **(JOINT POLICY)**	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Security Officer: Hazen Weber** **Policy: TRAINING AND AWARENESS**	
Policy # P1.14/S4.1	**Rules Addressed: 45 C.F.R. § 164.530(b); 164.308(a)(5)** **NCQA Standard: D.1, E.1, E.2, E3, F.3**

1. Purpose:

This Training and Awareness Policy sets requirements in frequency and content for privacy and security awareness training for Employees.

2. Synopsis:

Privacy and Security laws governing our organization change and these changes impact WCMSCHF, Employees and the patients and entities to which we have obligations. The Privacy and Security Officers must notify staff of these changes and provide supporting information via policies and procedure documents. This policy explains the ways by which Employees will be made aware of our current privacy and security policies, how we provide regular training and how Employees will be updated with changes.

3. Policy:

- Each new Employee will receive privacy and security training as specified by the orientation schedule, usually within the first week, but no later than 30 days after the start of employment.
- Each new Employee will be required to read all WCMSCHF privacy and security policies and sign an acknowledgement form stating that they have done so.
- Each new Employee will be required to enter into an Employee ~~Worker~~ Confidentiality~~, Non-Disclosure, Non-Solicitation~~ Agreement with WCMSCHF, agreeing to comply with the WCMSCHF privacy and security policies and to protect the confidentiality of sensitive information, including PHI. A current version of ~~this~~ the Employee Confidentiality Agreement is maintained by the Privacy and Security Officers.
- All signature forms will be stored for a period of at least six years.
- The Privacy and Security Officers will hold at least one awareness presentation each calendar year that is mandatory for all Employees to attend. The awareness training will contain highlights of policies and Standard Operating Procedures, changes to policies and Standard Operating Procedures and examples of lessons learned.
- All Employees will be required to review and sign an acknowledgement form stating that they have re-read all privacy and security policies once each year, in coordination with the annual awareness training.
- ~~All Employees will be required to sign the Worker Confidentiality, Non-Disclosure, Non-Solicitation Agreement with WCMSCHF annually.~~[2]

Formatted: Font color: Auto

[2] Note to WCMSCHF: We have suggested some tweaks to the policy of having Employees re-sign the Employee Confidentiality Agreement each year. Employees should sign the Employee Confidentiality Agreement when they

- When WCMSCHF makes a material change to these Policies and Procedures, it will provide additional training for those Employees affected by the change within 30 days of such change.
- Employees who violate privacy and/or security policies may be asked to attend an awareness training for new hires or a one-on-one awareness training at the discretion of their manager or the Privacy and/or Security Officers and per the Sanctions Policy (P1.15/S4.2).

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson, Hazen Weber, and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Hazen Weber
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors

commence employment (the signature page should be moved to the actual agreement rather than on the annual signature page form). Employees should not re-sign or re-acknowledge the Employee Confidentiality Agreement each year (there is recent case law that may make the contract unenforceable because there is not additional consideration paid in connection with re-signing the agreement). For HIPAA purposes, it is sufficient to have the employees acknowledge that they have received annual HIPAA training and understand that they are obligated to comply with HIPAA and your policies and procedures. Please note that we have not substantively reviewed the Worker Confidentiality, Non-Disclosure, Non-Solicitation Agreement that you sent via email, but would be happy to involve one of employment lawyers if you would like it reviewed. We should also discuss whether any "clean-up" is needed for employees who have resigned the Employee Confidentiality Agreement after their employment started.

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES **HIPAA SECURITY POLICIES AND PROCEDURES** **(JOINT POLICY)**	
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Security Officer: Hazen Weber** **Policy: SANCTIONS**	
Policy # P1.15/S4.2	**Rules Addressed: 45 C.F.R. § 164.530(e); 164.308(a)(1)(ii)(C)**

1. Purpose:

This Sanctions Policy specifies what considerations and actions can be taken in the event that sanctions are levied against an employee for violating a privacy and/or security related policy. This policy is a mandatory requirement of HIPAA.

2. Synopsis:

Sanctions are a necessary part of business and a requirement by law. This policy explains some of the variables and considerations that will be taken into account when applying a specific sanction, so that the process is as transparent as is reasonably possible. It also serves as a guide to senior management so that violations with like circumstances will be met with like sanctions and are thus fair.

3. Policy:

Sanctions will be levied against Employees who violate any security and/or privacy policy by use of defined categories for incident types as specified below.

Category 1:
Unintentional breach of privacy or security that may be caused by carelessness, lack of knowledge or judgment (e.g., emailing PHI to an employee's personal email account).

Category 2:
Deliberate unauthorized access to PHI, without loss or Disclosure (e.g., Employee accessing confidential information of a co-worker without a legitimate business reason or sharing a password with a co-worker).

Category 3:
Deliberate unauthorized access of PHI or deliberate tampering of data but done without malice or personal gain (e.g., staff accessing information and Disclosing to an unauthorized individual or tampering with an electronic document to expedite a process).

Category 4:
Deliberate unauthorized Disclosure of PHI for malice or personal gain (e.g., selling information to the tabloids or Using personal information to open lines of credit).

Before sanctions will be levied, consideration will be given to the following mitigating factors:

- Offending Employee voluntarily admits the breach and cooperates with the investigation;
- Offending Employee shows remorse;

- Action was taken under pressure from an individual in a position of authority;
- Employee was inadequately trained;
- Offending Employee has multiple offenses;
- Whether or not harm came to the breach victim(s);
- Type of breach (e.g., specially protected information such as HIV-related, psychiatric, substance abuse and genetic data):
    - High volume of people or data affected
    - High exposure for the institution and marked damage to the Company's reputation
    - Large organizational expense incurred, such as breach notifications
    - Hampering an investigation
    - Negative influence of actions on others

Sanctions specified within this document are for privacy and security violations and fall outside of those specified within the Employee Handbook.

Sanctions have been specified below as general guidelines and are dependent on the circumstances of the violation.

Types of Sanctions:

1. A written sanction specifying the incident and the appropriate process that should have been followed will be sent to the Employee and his or her direct supervisor by either the Privacy and/or Security Officer and will be signed and filed along with an entry in the Incident Log, which shall be maintained by the Privacy Officer and Security Officer for at least six years.
2. A written sanction as described in #1 and a mandatory one-on-one training with the Privacy and/or Security Officer.
3. A written sanction and a mandatory one-on-one training as described in #2 along with a written warning will be filed in the employee's personnel file for a period of two years.
4. A written sanction and mandatory one-on-one training as described in #2 along with a final written warning will be filed in the employee's personnel file for a period of one year.
5. Other sanctions include demotion, loss in pay, leave without pay and termination of employment.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson, Hazen Weber, and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Hazen Weber
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson, Hazen Weber, and Tara Kinard

Approved: July 19, 2016 by WCMSCHF Board of Directors

HIPAA PRIVACY AND BREACH NOTIFICATION POLICIES AND PROCEDURES **HIPAA SECURITY POLICIES AND PROCEDURES** **(JOINT POLICY)**
Company: Wake County Medical Society Community Health Foundation, Inc. **Privacy Officer: Tara Kinard** **Security Officer: Hazen Weber** **Policy: PRIVACY/SECURITY DOCUMENTATION**

Policy # P1.16/S4.3 **Status: Approved**	**Effective Date: June 22, 2010** **Rules Addressed: 45 C.F.R. §§ 164.530(j); 164.316** **NCQA Standard: A.3**

WCMSCHF shall maintain these Policies and Procedures in written or electronic form. It shall also maintain, in writing or in electronic form, any communication required to be in writing by these Policies and Procedures. Also, if any action, activity or designation is required by these Policies and Procedures to be documented, WCMSCHF shall maintain a written or electronic record of such action, activity or designation.

WCMSCHF will retain all documentation noted above for at least six years from the date of its creation or the date when it last was in effect, whichever is later. Information no longer required to be retained by these Policies and Procedures (including this Privacy/Security Documentation Policy) will be destroyed by secure means. Any and all documentation that becomes part of a medical record will be retained according to the laws applicable to retention of medical records.

Company Employees may not destroy or dispose of records involved in a government investigation, public records request, audit or litigation or records that are required to be maintained by these Policies and Procedures or federal, state or local laws or regulations.

All PHI must be destroyed or disposed of in accordance with the Disposal of PHI Policy (S4.5).

WCMSCHF has also implemented Financial Policies and Procedures for the retention and destruction of certain financial documents of WCMSCHF that supplement, but do not replace, the document retention requirements described in this Policy.

Revision History:
Effective: June 22, 2010
Approved: September 7, 2012 by Susan Davis

Revised: August 21, 2013 by Smith Anderson, Hazen Weber, and Tara Robinson
Approved: September 6, 2013 by Susan Davis

Revised: June 20, 2014 by Smith Anderson and Hazen Weber
Approved: July 28, 2014 by WCMSCHF Board of Directors

Revised: July 6, 2016 by Smith Anderson, Hazen Weber, and Tara Kinard
Approved: July 19, 2016 by WCMSCHF Board of Directors