DELAWARE CENTER FOR MATERNAL FETAL MEDICINE

of CHRISTIANA CARE

(DCMFMCC)

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW PROTECTED HEALTH INFORMATION (PHI) ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

THE PRIVACY OF YOUR PROTECTED HEALTH INFORMATION (PHI) IS OF THE UTMOST IN IMPORTANTANCE TO US.

OUR LEGAL DUTY

We are required by applicable federal and state law to maintain the privacy of your protected health information (PHI). We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning your PHI. We must follow the privacy practices that are described in this notice while it is in effect.

This notice takes effect January 1, 2013 and will remain in effect until further notice by DCMFMCC.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided such changes are permitted by applicable law. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all health information that we maintain, including health information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and make the new notice available upon request.

You may request a copy of our Privacy Practices Notice at any time. For more information about our privacy practices, or for additional copies of this Privacy Practices Notice, please contact us using the information listed at the end of this notice or you can download our Privacy Practices Notice from our website at http://dcmfm.com/patient-resources/forms.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION (PHI)

We use and disclose health information about you for research, treatment, payment, and healthcare operations. For example:

Research: We may give your medical information to people within Christiana Care who are preparing a research project or trying to get patients involved in research.

Treatment: We may use medical information about you to provide you with medical treatment or services, and we may disclose medical information about you for treatment purposes to doctors, nurses, technicians, or other health care providers who are involved in your care. This includes a re-disclosure of records obtained from other providers by DCMFMCC. A record of your treatment with the Delaware Center for Maternal and Fetal Medicine of Christiana Care will be sent to the physician who referred you to us for medical care and CCHS, unless otherwise specified by you in writing. DCMFMCC is not responsible for records once disclosed, as the information may no longer be protected by Federal Privacy Rules, and may be re-disclosed by the recipient.

Payment: We may use and disclose medical information about you so that the treatment and services you receive from us may be billed and payment may be collected from you and/or an insurance company or third party.

Healthcare Operations: We may use medical information about you to support our healthcare operations, such as comparing patient data to improve treatment methods. We may disclose health information to others of your treating health care providers for limited operations, such as quality assessment and protection from fraud.

Compliance with Law: We may disclose health information when required by law and will comply with state disclosure laws that are more restrictive than the federal privacy law. Subject to certain requirements, we may release medical information about you without prior authorization for public health purposes, abuse or neglect reporting, health oversight audits or inspections. Under no circumstance with DCMFMCC disclose your PHI to law enforcement officials without a subpoena from an authorized court of law demanding such release. You will be notified in writing if we receive a subpoena from an authorized court of law requesting your Protected Healthcare Information (PHI).

Other Uses of Medical Information: In any situation not covered by this notice or the laws that apply to us, we will ask for your written authorization before using or disclosing medical information about you. If you choose to authorize use or disclosure, you can later revoke that authorization by notifying us in writing at any time.

Your Authorization: In addition to our use of your health information for treatment, payment or healthcare operations, you may give us written authorization to use your health information or to disclose it to anyone for any purpose. Your preferred method of external communications with DCMFMCC must be identified on the DCMFMCC PATIENT CONSENT FORM TO EXTERNALLY COMMUNICATE PHI and signed by you, our patient.

If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this Notice.

To Your Family and Friends: We must disclose your health information to you, as described in the Patient Rights section of this notice. We may disclose your health information to a family member, friend or other person to the extent necessary to help with your healthcare or with payment for your healthcare, but only if you agree that we may do so.

Persons Involved In Care: We may use or disclose health information to notify, or assist in the notification of (including identifying or locating) a family member, your personal representative or another person responsible for your care, of your location, your general condition, or death. If you are present, then prior to use or disclosure of your health information, we will provide you with an opportunity to object to such uses or disclosures. In the event of your incapacity or emergency circumstances, we will disclose health information based on a determination using our professional judgment disclosing only health information that is directly relevant to the person's involvement in your healthcare. We will also use our professional judgment and our experience with common practice to make reasonable inferences of your best interest in allowing a person to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of health information.

Marketing Health-Related Services: We will not use your health information for marketing communications without your written authorization.

Appointment Reminders: We may use or disclose your health information to provide you with appointment reminders (such as voicemail messages, postcards, or letters). These appointment reminder notifications will not include Protected Healthcare Information (PHI) or privacy data.

PATIENT RIGHTS

Access: You have the right to look at or get copies of your personal health information (PHI) and medical records by requesting such in writing.

You may request that we provide a hardcopy of your medical records information or in an electronic softcopy in PDF document format. We will use the format you request unless we cannot practicably do so. (If you do not want a hardcopy print-out of your medical records information, you can request a softcopy in writing by submitting your request to DCMFMCC's Practice Manager). You must make a request in writing to obtain access to your health information. You may obtain a form to request access by using the contact information listed at the end of this notice.

DCMFMCC will charge you a reasonable cost-based fee for making hardcopies or softcopies of your medical records information according to the guidelines defined by the State of Delaware as follows:

- $2.00 for first 10 pages
- $1.00 per page for pages 11 – 20
- $0.90 per page for pages 21-60
- $0.50 per page for pages 61 and above
-

If you request an alternative format, we will charge a cost-based fee for providing your health information in that format as per the above guidelines.

Contact us using the information listed at the end of this notice for a full explanation of our fee structure.

Restriction: You have the right to request that we place additional restrictions on our use or disclosure of your health information. We are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in an emergency).

Alternative Communication: You have the right to request that we communicate with you about your health information by alternative means or to alternative locations. (You must make your request in writing.) Your request must specify the alternative means or location, and provide satisfactory explanation how payments will be handled under the alternative means or location you request.

Amendment: You have the right to request that we amend your health information. (Your request must be in writing, and it must explain why the information should be amended.) We may deny your request under certain circumstances.

Electronic Notice: If you receive this notice from our web site or by electronic mail (e-mail), you are entitled to receive this notice in written form, but must request in writing a hardcopy be mailed to you.

WHO MUST COMPLY WITH THIS NOTICE

Any healthcare professional or employee of the Delaware Center for Maternal and Fetal Medicine of Christiana Care authorized to view or enter PHI or ePHI information into your electronic health record chart.

QUESTIONS AND COMPLAINTS

If you want more information about our privacy practices or have questions or concerns, please contact us. If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about access to your health information or in response to a request you made to amend or restrict the use or disclosure of your health information or to have us communicate with you by alternative means or at alternative locations, you may complain to us using the contact information listed at the end of this notice.

You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to the privacy of your health information. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Delaware Center for Maternal Fetal Medicine
Practice Manager / HIPAA Security & Privacy Officer
One Centurion Drive, Suite 312
Newark, DE 19713
302-319-5680

DATA BREACH OR UNAUTHORIZED DISCLOSURE OF PHI – MITIGATION & PUBLIC ANNOUNCEMENT PLAN

HITECH Act Requirements

Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Definition of Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Breach Notification Requirements

Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

Media Notice

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

Breach Notification Process

In the event of a data breach or unauthorized disclosure of PHI for greater than 500 patients, the following shall define who and which entity is responsible and accountable for disclosure of such data breach or unauthorized disclosure of PHI and informing the public.

In the event of a known data breach and/or unauthorized disclosure of PHI or ePHI (> 500 patients) from DCMFMCC's, outsourced, electronic health records (EHR) provider, the following shall apply:

1. DCMFMCC's outsourced, electronic health records (EHR) provider, shall notify DCMFMCC's in writing of any physical data breach or unauthorized access to patient PHI or ePHI when such event occurs and is known to occur.

2. DCMFMCC's outsourced, electronic health records (EHR) provider, shall abide by the requirements of the Federal Trade Commission (FTC) pursuant to section 13407 of the HITECH Act.

3. As per the HITECH Act Final Rule, EHR providers must notify consumers following a breach involving unsecured information. In addition, if a service provider to one of these entities has a breach, it must notify DCMFMCC, which in turn must notify consumers. The Final Rule also specifies the timing, method, and content of notification, and in the case of certain breaches involving 500 or more people, requires notice to the media. Entities covered by the rule must notify the FTC, and they may use a standard form, which can be found along with additional information about the rule at www.ftc.gov/healthbreach.

4. DCMFMCC will notify its parent company, Christiana Care Health Systems (CCHS) in writing with a complete forensics report describing the extent and magnitude of the breach.

5. CCHS, upon review and audit of the incident, must notify consumers on behalf of DCMFMCC as per the Media Notice and timeline requirements defined above.

In the event of a known data breach and/or unauthorized disclosure of PHI or ePHI (> 500 patients) from DCMFMCC's occurring from within its two facilities, following shall apply:

1. DCMFMCC will notify its parent company, Christiana Care Health Systems (CCHS) in writing with a complete forensics report describing the extent and magnitude of the breach.

2. CCHS, upon review and audit of the incident, must notify consumers on behalf of DCMFMCC as per the Media Notice and timeline requirements defined above.