The Fetal and Infant Mortality Review Process:

The HIPAA *Privacy Regulations*

NATIONAL NFIMR FETAL–INFANT MORTALITY REVIEW PROGRAM

This document was developed by the American College of Obstetricians and Gynecologists with the assistance of Hogan and Hartson, LLP

Acknowledgements

We especially wish to thank Susannah Frazier, JD, Staff Attorney, ACOG General Counsel's Office for her expert input and invaluable guidance in the development of this document.

We also wish to thank the following for suggesting content, reviewing drafts, and providing valuable insights and suggestions: Janet Chapin, RN, MPH, Director, Division of Women's Health Issues, the American College of Obstetricians and Gynecologists; and Luella Klein, MD, FACOG, Vice President, Division of Women's Health Issues, the American College of Obstetricians and Gynecologists, Annette Phelps, ARNP, MSN, Director, Division of Family Health Services/State Title V Director, Florida Department of Health, Danielle Noell, ARNP, RNC, Nurse Consultant, Pregnancy Associated Mortality Review, Florida Department of Health, Dawn Dailey, RN, MS, CS, FIMR Coordinator, Contra Costa, CA Health Department, Cheryl Nunally-Bodamer, RN, MS, Coordinator of VA Regional Perinatal Coordinating Council 6/FIMR Coordinator, and Brenda Byrd-Norwood, FIMR Coordinator, Pee Dee SC Health District.

Development of this document was supported by the Maternal and Child Health Bureau, Health Resources and Services Administration Grant #6 U93 MC 00136. Opinions expressed in this publication are those of the authors and do not necessarily reflect the views or policies of the Maternal and Child Health Bureau, the Health Resources and Services Administration or the Department of Health and Human Services.

For additional copies of this document, write to: NFIMR, 409 12th Street, SW, Washington, DC 20024.

February, 2003

How To Use This Manual

This document provides a basic overview of the Health Insurance Portability and Accountability Act (HIPAA) as it relates to local Fetal and Infant Mortality Review Programs, specifically their ability to obtain access to pertinent medical records.

However, state laws and regulations will greatly affect how the current HIPAA regulations will be implemented in each state. The current HIPAA regulations give deference to state laws if they are not conflicting. Thus, the final answer to how HIPAA will affect a local FIMR program will be found at the state level. Each FIMR program will need to touch base with their state Title V Director to ensure that they will continue to have access to medical records. Generally, all FIMR programs should be able to do so.

In addition, the HIPAA regulations will be subject to change. Over the next several years, it can be anticipated that several modifications will occur as local hospitals and providers find out what works and what does not.

The best ways to use this document include:

- Use the document as background reading before a meeting or conference call with the state Title V director. Some components of the HIPAA Privacy Rule are easy to understand, while other parts are more complex. Read the NFIMR document and discuss it with other FIMR staff. It is important to have a basic understanding of the HIPAA regulations and a thorough understanding of where the local FIMR program stands in relation to HIPAA.
- Complete the HIPAA/FIMR checklist. (See Appendix F) Be sure to be able to check "yes" to most of the questions.
- Refer to the question and answer section of this document. (See pp 16) Develop answers that relate specifically to the local FIMR program's circumstances. Be prepared to respond when asked about how the HIPAA privacy rule will affect FIMR.

Under the new HIPAA regulations, hospitals or providers should anticipate a FIMR program's request for access to medical records and be prepared to respond positively. However, the local FIMR program can greatly enhance its credibility and access to information by making sure that hospitals and providers 1) know about the benefits of the local FIMR, 2) understand that confi-

---

DISCLAIMER Many State Privacy Laws wil continue to apply following the effective date of HIPAA Privacy Regulations. This document does not include a review of state regulations or laws. ***The information or forms provided in this manual do not constitute legal advice and do not necessarily meet the requirements of your state's laws.***

You are advised to consult a state health official, such as your state Title V (MCH) Director, to determine which regulations protect your fetal and infant mortality review (FIMR) program and the need to revise the content of any FIMR form or agreement currently in place.

dentiality is key to the FIMR process, 3) are included in the FIMR case review team and 5) receive explanatory information such as the Sample Health Officer Letter (see Appendix C) when records are requested.

Finally, be patient. Hospitals and providers vary in their understanding of the HIPAA regulations and their degree of readiness to implement them. In April 2003, when the HIPAA regulations take effect, some hospitals and providers may be totally overwhelmed. Hospitals and providers will generally agree to comply with the FIMR request for information as they begin to understand the HIPAA provisions that allow it.

DISCLAIMER Many State Privacy Laws wil continue to apply following the effective date of HIPAA Privacy Regulations. This document does not include a review of state regulations or laws. ***The information or forms provided in this manual do not constitute legal advice and do not necessarily meet the requirements of your state's laws.***

You are advised to consult a state health official, such as your state Title V (MCH) Director, to determine which regulations protect your fetal and infant mortality review (FIMR) program and the need to revise the content of any FIMR form or agreement currently in place.

Table of Contents

Key Provisions

I. Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) began as legislation designed to ensure that any person would be eligible for comparable health insurance coverage if he or she changed jobs. A subchapter was added to the statute in an effort to develop standards for the growing use of the electronic exchange of health information for certain financial and administrative transactions, while protecting the privacy and security of health information exchanged.

The Department of Health and Human Services (HHS) is responsible for establishing uniform national standards for electronic transactions, unique health identifiers and code sets, as well as standards for the privacy and protection of individually identifiable health information.

FIMR programs assess the care provided to mothers and infants in a community using case information about fetal and infant deaths gathered from various sources, such as hospitals, physician practices, mothers, and social service programs. All of this information is abstracted, de-identified and summarized. The FIMR programs study the de-identified summaries to identify areas for improvement in the delivery of health care and recommend changes in community services systems and resources. FIMR teams then work with community leaders to implement these changes. The FIMR process referred to throughout this document is described in detail in *The Fetal and Infant Mortality Review Manual: A Guide for Communities*. This document is available free of charge by writing to the National Fetal and Infant Mortality Review Program (NFIMR), 409 12th Street SW, Washington, DC 20024.

The intersection between HIPAA and FIMR arises as FIMR programs collect information needed for case reviews from hospitals and providers covered by HIPAA. This paper provides an overview of the HIPAA regulations and the Privacy rule and how these will affect FIMR programs.

II. The Privacy Rule

On April 14, 2002, HHS issued a new final privacy rule (the "Privacy Rule"). Compliance with this rule is required by April 14, 2003 for most entities covered under the rule. To view a copy of the Privacy Rule and to read the HHS guidance that explains the Privacy Rule, go to www.hhs.gov/ocr/hipaa. Please note that this website is subject to change.

HHS states that there are several purposes to the Privacy Rule, including

- Safeguarding the rights of patients by providing them access to their protected health information (PHI)
- Enabling consumers to control the use and disclosure of their PHI
- Creating national standards for healthcare privacy in a new electronic age

The Privacy Rule governs the use and disclosure of protected health information by ***covered entities.*** "Covered entities" include:

1. health care providers such as physicians, hospitals or pharmacies that conduct certain standard transactions electronically (e.g., the submission of health claims),
2. health plans, and
3. health care clearinghouses (e.g., billing services).

"Protected health information" is individually identifiable health information that is transmitted or maintained in any form or medium—by electronic means, on paper, or through oral communications. Protected health information specifically includes demographic information and patient lists. "Individually identifiable health information" is defined quite broadly and includes information that

1. is created or received by a health care provider, health plan, employer, or health care clearinghouse
2. identifies, or which can be used to identify, an individual
3. 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

FIMR is not a covered entity, therefore the Privacy Rule does not govern FIMR programs directly. However, the Privacy Rule imposes some new requirements on covered entities before they can disclose protected health information to FIMR programs.

A. Permitted Uses and Disclosures

A covered entity may not use or disclose protected health information, except as specifically required or permitted by the Privacy Rule. A covered entity is permitted to use and disclose protected health information for treatment, payment and health care operations or for other limited purposes specified under the Privacy Rule.

Under certain circumstances, a covered entity may release protected health information for research or public health surveillance. FIMR programs will generally access protected health information through these research or public health provisions.

All other uses and disclosures may be made only pursuant to individual authorization. Thus, FIMR programs, which do not access protected health information through

research or public health provisions, may be required to obtain patient authorization or meet other requirements before a hospital or physician may disclose protected health information to the program.

If FIMR programs are currently obtaining individual authorization for medical record review, they may choose to continue to do so. Accessing medical records through individual authorization, however, has never been the preferred method for FIMR programs. Signing the consent form is a barrier to participation for some mothers and families and may result in a small and skewed sample of cases.

1. Treatment, Payment, and Health Care Operations

A covered entity may use or disclose protected health information for its own treatment, payment and health care operations (*i.e.,* various administrative and management functions of a covered entity). In addition, a covered entity may disclose protected health information for the treatment activities of a health care provider, the payment activities of a health care provider or covered entity, and certain health care operations of another covered entity regarding an individual in common.

These permitted disclosures likely are not applicable to FIMR programs, as FIMR programs are not covered entities or health care providers and do not receive information for these purposes.

2. Disclosures for Other Specified Purposes

Subject to certain requirements, a covered entity is permitted to use and disclose protected health information without authorization for several specified purposes. Most importantly for the FIMR programs, disclosures are permitted in some circumstances for public health and research purposes.

i. Public Health Activities

The Privacy Rule permits a covered entity to disclose protected health information to a "public health authority" for certain public health activities. A "public health authority" is "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting *under a grant of authority from or contract with such public agency,* including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate." (See Appendix A)

Two permitted disclosures are applicable to FIMR programs. A covered entity may disclose protected health information without authorization from the individual to "[a] public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease,

injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions." Additionally, disclosures may be made to "a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect." A public health authority that is a covered entity may use protected health information for these same purposes.

Many of the activities related to FIMR programs fall within the purview of public health disclosures. This permitted disclosure, however, applies only to FIMR programs that have public health agencies as sponsoring agencies or that are acting under a grant of authority from or contract with a public health agency. Disclosures to FIMR programs that are acting under the auspices of a public health agency will be permissible under the new federal privacy rule. Further, the Privacy Rule does not preempt state laws that provide for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

ii Research

A covered entity may disclose protected health information to another person or entity for the purpose of research provided that the researcher obtains individual authorization or a waiver of authorization from an institutional review board (IRB) or a specially constituted privacy board. Research is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

However, the Privacy Rule contains a special exception for research on decedents. For purposes of research on decedents, a covered entity may disclose protected health information to a researcher (or FIMR program) if the researcher represents that the use and disclosure is sought solely for research on the protected health information of decedents and that the information sought is necessary for the research purposes. Additionally, if the covered entity requests, the researcher must provide documentation of the death of the individuals. The Privacy Rule does ***not*** require that an IRB review such requests or representations.

It appears that many disclosures to the FIMR program can be made both pursuant to 1) the general HIPAA research provisions which require IRB waivers are obtained or 2) the specific HIPAA decedent research provisions, which do not require IRB waivers.

3. Authorization

A covered entity may disclose protected health information for any purpose with the written authorization of the individual. The Privacy Rule sets forth the requirements that must be contained in an authorization, which for FIMR programs, include: (1) a description of the information to be used or disclosed that identifies

the information; (2) the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure; (3) the name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure; (4) a description of each purpose of the requested use or disclosure; (5) an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure; (6) a statement of the individual's right to revoke the authorization in writing, a description of how to revoke, and the exceptions to this right; (7) a statement describing the covered entity's ability or inability to condition treatment, payment, or enrollment or eligibility for benefits on obtaining the authorization; (8) a statement that information disclosed pursuant to this authorization may be subject to further disclosure by the recipient and may no longer be protected by the Privacy Rule; and (9) the signature of the individual and date (and, if signed by a personal representative, his or her authority to act on behalf of the individual). If a FIMR program is obtaining protected health information from covered entities pursuant to individual authorization, the authorization must meet the requirements of the Privacy Rule. (See Appendix B)

B. Other Applicable HIPAA Standards

1. Minimum Necessary

Under the overall Privacy Rule, uses, disclosures and requests of protected health information must be limited to the "minimum amount necessary" to accomplish the purpose of the use, disclosure or request. The Privacy Rule exempts from the minimum necessary requirement all uses and disclosures made pursuant to individual authorization. The use, disclosure or request of an individual's entire medical record is consistent with the minimum necessary limitation only if specific justification is provided regarding why the entire medical record is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

The Privacy Rule also exempts from the minimum necessary requirement all uses and disclosures that are required by other laws, such as any state law that provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

In addition, HHS has issued guidance permitting a covered entity to rely on the judgment of the certain parties requesting the disclosure as to the minimum amount of information that is needed. This exception is referred to as ***"reasonable reliance".*** Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency who states that the information requested is the minimum necessary for a purpose permitted under the Privacy Rule, such as for public health purposes
- Another covered entity.
- A professional who is a workforce member or business associate of the covered entity holding the information.
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

The rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

To summarize:

- Hospitals and physicians are permitted, but not required, to use reasonable reliance to release medical record information—including the entire record—to a FIMR program when that program operates under the auspices of a public health agency or an IRB waiver.
- Hospitals and physicians should comply with state laws that currently allow FIMR programs to access medical records for public health surveillance.

2. Business Associate

A business associate is a person or entity that performs a function or activity or provides a specified service (*i.e.,* accounting, accreditation, actuarial, administrative, consulting, data aggregation, financial, legal, or management services) for, or on behalf of, the covered entity, which involves the use or disclosure of protected health information. For example, a third party that is hired by a hospital to *assist the hospital* in performing data analyses (*i.e.,* a health care operation) using protected health information is a business associate. However, a third party that obtains protected health information from a covered entity for its own data analysis purposes is not a business associate of the covered entity. In general, a covered entity may disclose protected health information to its business associate only pursuant to a written agreement that meets specific requirements set forth in the Privacy Rule. The covered entity is responsible for violations of the contract by its business associate, of which it becomes aware, if the covered entity fails to take certain corrective action.

FIMR programs likely are **not** business associates of covered entities as the activity performed by a FIMR program is for its own purposes (e.g., to improve the service systems and resources of the community's women, infants and families) and not for that of a covered entity.

3. De-Identified Information

Data that have been de-identified in accordance with the Privacy Rule's stringent de-identification standard are not considered protected health information and are not subject to the rule. Information is deemed de-identified if the covered entity has no actual knowledge that the information could be used alone or in combination with other information to identify the individual and eighteen "identifiers" related to the individual (and the individual's relatives, household members, and employer(s)) are removed from the data (*e.g.*, all elements of date except for year, including dates of service, that directly relate to an individual, medical record numbers, social security numbers). This "safe harbor" method, however, may be too restrictive to be useful for the purposes of the FIMR program.

Alternatively, information is considered de-identified if a statistician concludes "the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information." Thus far, most statisticians have been unwilling to provide these certifications due to the vague standard and liability concerns.

4. Limited Data Sets

Covered entities are permitted to disclose facially de-identified protected health information for the purpose of research, public health activities, or health care operations, provided that it does so pursuant to a data use agreement with the recipient. The data use agreement must limit the recipient's use and disclosure of the information and prohibit the recipient from identifying or contacting the individual. The Privacy Rule sets forth sixteen direct identifiers that may not be included in a limited data set, but permits the inclusion of zip codes, dates of service, dates of birth and death, and geographic subdivisions (except street address), among others. Like the de-identification standard, this method may not be useful for FIMR purposes because it requires the removal of most identifying information.

5. Routine versus non-routine disclosures

The Privacy Rule does not define when disclosures are routine versus non-routine. A covered entity is responsible for determining whether the disclosures it makes are routine or non-routine based on factors such as how frequently a particular type of information is disclosed and to whom. If a covered entity discloses certain categories of protected health information to FIMR programs on a routine or recurring basis, the covered entity should have policies and procedures to accomplish the purpose of the disclosure to the FIMR program. Routine disclosures may include regular reporting of infant death or other information to a FIMR program.

C. Individual Rights

The Privacy Rule provides individuals with the several rights, including, among others, the right to receive an accounting of certain disclosures of their protected health information. Although FIMR programs themselves will not need to account for disclosures because they are not covered entities, the programs will none-the-less be affected. Disclosures made to FIMR programs for public health activities or research purposes pursuant to an IRB waiver will trigger this requirement for covered entities.

In these instances, covered entities will need to record the following information: the date of the disclosure, the name of the entity or person receiving the information (and address if known), a brief description of the information disclosed, and a statement of the purpose of the disclosure. For FIMR programs, a letter from the sponsoring agency on agency letterhead may suffice. (See Appendix C)

If FIMR programs are currently obtaining individual authorization for medical record review, they may continue to do so. Disclosures made pursuant to a written authorization of the patient will not trigger this accounting requirement.

III. Application of State Laws

The Privacy Rule does not affect any state law that provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention. (See Appendix D) To the extent that a covered entity is disclosing information to a FIMR program under such a law, the Privacy Rule will not prohibit the disclosure.

Further, state laws that are contrary to the Privacy Rule and provide individuals with more stringent privacy protections remain in effect. "Contrary" means that it is impossible to comply with both laws or complying with the state law stands as an obstacle to the accomplishment and execution of the Privacy Rule. "More stringent" means that it provides the individual with greater rights or amounts of information, or increases the privacy protections afforded the individual. Thus, the Privacy Rule creates a federal floor, or minimum standards, of privacy protection, such that current or future state laws that provide more privacy protection remain in effect.

In practice, few state laws will be "contrary" to the Privacy Rule. Instead, state laws often will supplement the requirements of the Privacy Rule. For example, a state law may require that an authorization form contain an additional statement not required by, but not inconsistent with, the Privacy Rule. As the Privacy Rule permits the authorization form to contain additional elements if they are not inconsistent with the required elements, to be valid under the Privacy Rule and the applicable state law, the authorization would need to meet the requirements of the Privacy Rule and contain the additional statement required by the state

law. FIMR programs will need to take account of the various ways in which state privacy laws will continue to affect the ability of the program to obtain patient information.

IV. FIMR Preparations for HIPAA Compliance

First, each FIMR program director is strongly encouraged to contact his or her Title V (MCH) Director before April 2003 to clarify FIMR's status in relation to HIPAA and the Privacy Rule. At that time, the Director can also review the FIMR program's protection from discovery and immunity of team members. The state Title V (MCH) Director can also determine whether or not any local FIMR forms, such as the home interview consent or the team pledge of confidentiality, should be updated or revised to incorporate the HIPAA regulations.

Second, FIMR programs should inform the agency or health department director that sponsors FIMR about FIMR program functions under the HIPAA privacy requirements. Questions about FIMR and HIPAA may go directly to the health department director and not to FIMR program staff. There should be no surprises or situations where the agency director is caught off guard or embarrassed by questions s/he cannot answer about HIPAA and FIMR. Also FIMR staff will want to be apprised of any new policies or procedures. The FIMR case review team will want to be reassured that the Privacy Rule will not affect their deliberations.

Third, the new HIPAA regulations provide a positive opportunity to update all the policies and procedures FIMR programs use to maintain confidentiality and to strengthen them, as needed. Confidentiality is key to FIMR.

Preserving the privacy of all the involved parties is therefore of paramount importance to any FIMR program. Local providers and institutions will not participate in the FIMR process or provide records for review without assurance that all information will be kept strictly confidential.

As the case data is being collected, FIMR program staff must remember the importance of protecting both paper and electronic copies of all information. Staff should never write family, provider, or institutional identifiers on the abstraction forms, but only the number assigned to the case. In the field, staff should be careful not to leave completed forms out in a car where they could be seen. Forms must be locked in the trunk until they can be transferred to the locked files within the office.

As the case is being prepared by FIMR staff for team review, all of the following information is also confidential:

- Names, addresses, telephone numbers and other contact information for families, providers or institutions;
- Completed interview questionnaires;
- Completed medical record abstraction forms;
- Tracking forms or cards;
- All other forms and papers with individual case information on them;
- Case summaries, even de-identified ones.

In the office, completed forms should always be stored in a locked file. If the case is being summarized or entered into a computer database and the transcriber must leave, even briefly, the record must be locked up and the computer screen should be closed. Computer systems for entering or summarizing maternal interview information should be secured with a password. It is essential that no one learn the information obtained from the case.

When preparing the de-identified case summary—even though HIPAA allows it—the birth and death dates on individual case summaries may need to be deleted. In small communities, and even in some large ones, these dates could lead back to the identity of the deceased. Take care to ensure complete confidentiality, and case summary de-identification.

At the end of the case review meeting, the de-identified case summaries should be collected from all team members and shredded. After the team reviews the case, all tracking forms that might link the family, the provider and institutions to the case summary should be deleted and/or shredded; and the paper data abstraction forms and home interview form should also be shredded (if the law allows). There should be no paper trail for anyone, including the abstractor, to trace the case number back to a particular family, provider or institution. Finally, in keeping minutes of the case review meeting, many FIMR programs already find it prudent to develop minutes that summarize general discussions such as trends and sentinel events rather than individual case notes, even though these are de-identified.

V. Frequently Asked HIPAA Questions for FIMR Programs

There are two general types of questions and answers contained in this section: those that FIMR programs may be asked by covered entities and those that the FIMR program might ask each other or the Title V director. The audience for the questions may overlap, to some degree. Each FIMR program is encouraged to develop questions and answers that relate specifically to their circumstances.

Question:

Where can I get a copy of the HIPAA Privacy Rule?

Answer:

To view a copy of the Privacy Rule and to read the HHS guidance that explains the Rule, go to www.hhs.gov/ocr/hipaa Please note that this website is subject to change.

Question:

How does the HIPAA Privacy Rule affect the FIMR process?

Answer:

The Privacy Rule does not appear to apply directly to FIMR programs. However, it will impact the process FIMR programs use to obtain medical records (protected health information). The effect of the Privacy Rule on a FIMR program depends on the specific facts and circumstances surrounding the program.

For many programs, disclosures by covered entities to the FIMR program will be for the purpose of public health activities or research. Under the Privacy Rule, physicians and hospitals (covered entities) may disclose protected health information for either purpose, provided that certain requirements are met.

Question:

Will FIMR programs have to stop collecting data and reviewing cases due to HIPAA prohibitions?

Answer:

No. The HIPAA Privacy Rule does not prohibit the FIMR programs from collecting data and reviewing cases. In fact, there are several ways in which the Privacy Rule allows hospitals and physicians (covered entities) to share information with the FIMR programs.

Specifically, covered entities may disclose protected health information to a FIMR program, depending on the nature of the program, if the disclosure:

(1) meets the requirements for public health disclosure

(2) meets the requirements for a research disclosure

(3) is made pursuant to a valid individual authorization

Question:

When will FIMR programs have to comply with the new HIPAA regulations?

Answer:

FIMR programs will begin to comply with the requirements of the Privacy Rule when they take effect on April 14, 2003.

Question:

Will FIMR programs be requesting protected health information?

Answer:

Yes. FIMR programs routinely collect information from prenatal, labor and delivery, child health medical records, coroner/medical examiner reports, social services records, home visiting/case management records, emergency medical technician transport records, birth and death records, etc. All of the information is protected health information.

Question:

Are FIMR activities, which are sponsored by our local health department, negatively affected by the Privacy Rule?

Answer:

No. The Privacy Rule permits the disclosure of protected health information from physicians and hospitals (covered entities) to a public health agency or an agency acting under a grant of authority from or contract with such public agency without individual authorization. Further, it permits the public health agency to use the information for public health activities.

Question:

Because of the new Privacy Rule, will the local health department sponsored FIMR program have to get both IRB approval and individual authorization from the mother before records can be released?

Answer:

No. The Privacy Rule allows for the disclosure of information to a public health agency or an agency acting under a grant of authority from or contract with such public agency without any additional individual authorization or IRB approval.

Question:

Are FIMR programs sponsored by universities, hospitals or community advocacy groups (Healthy Mothers/Healthy Babies, federal Healthy Start, etc.) negatively affected by the Privacy Rule?

Answer:

No. The Privacy Rule permits the disclosure of protected health information from the physicians and hospitals (covered entities) to researchers without authorization if the researchers obtain a waiver of authorization based on specific criteria in the Privacy Rule, from an institutional review board (IRB) or a specially constituted privacy board. Our agency has obtained such a waiver.

OR

Our FIMR program has obtained a valid individual authorization from the mother of the deceased infant to abstract these records.

Question:

What requirements must be contained in the FIMR medical record authorization (consent) form?

Answer:

The Privacy Rule sets forth nine criteria, which are applicable to FIMR programs, for a valid individual authorization (consent) to access medical records, including the following:

1) a description of the information to be used or disclosed;
2) the persons or class of persons authorized to make the use or disclosure;
3) the persons or class of persons to whom the covered entity may make the disclosure;
4) a description of each purpose of the use or disclosure;
5) an expiration date, or an expiration event that relates to the individual or the purpose of the use or disclosure;
6) a statement of the individual's right to revoke the authorization in writing, a description of how to revoke, and the exceptions to such right;
7) a statement describing the covered entity's ability or inability to condition treatment, payment, enrollment or eligibility for benefits on obtaining the authorization;
8) a statement that information disclosed pursuant to the authorization may be subject to further disclosure by the recipient and may no longer be protected by the Privacy Rule; and
9) the signature of the individual and date (and, if signed by a personal representative, his or her authority to act on behalf of the individual).

Question:

Is the FIMR program a covered entity?

Answer:

No. Under the Privacy Rule, covered entities include health plans, health care clearinghouses and any health care provider (physician, hospital, etc) who conducts certain standard transactions electronically, such as billing.

Question:

Is the FIMR program a business associate? Doesn't the FIMR program have to have a written agreement with a hospital?

Answer:

No. The FIMR program is not a business associate of a hospital or other covered entity as the activity performed by a FIMR program is for its own purposes (e.g. to improve the health of the community and not for that of a covered entity.) Therefore, the FIMR program is not required to have a business associate agreement.

According to HIPAA, a business associate is a person or entity that performs a function or activity or provides a specified service (i.e., accounting, accreditation, actuarial, administrative, consulting, data aggregation, financial, legal, or management services) **for, or on behalf of, the hospital or physician (covered entity),** which involves the use or disclosure of protected health information.

Question:

What are the compliance requirements of the privacy rule for hospitals and physicians?

Answer:

Hospitals and physicians (covered entities) must implement the requirements set forth in the Privacy Rule, which include provisions governing: (1) uses and disclosures of protected health information; (2) individual rights of the subjects of the information; and (3) administrative requirements. These include, among others, the appointment of a privacy officer, the implementation of privacy policies and procedures, and the training of members of the workforce.

The Privacy Rule:

- Governs how hospitals and physicians (and other covered entities) use and disclose protected health information. For certain uses and disclosures, a hospital or physician will be required to obtain authorization from the individual. For others, no authorization is required but other requirements must be met.
- Requires that hospitals and physicians meet certain administrative standards pertaining to the use and disclosure of protected health information. For example, a

covered entity generally must ensure that it is using, disclosing or requesting only the minimum amount of information necessary to accomplish the purpose of the use, disclosure or request.

- Provides individuals with certain privacy rights. For instance, an individual has a right to inspect and copy certain information about him or herself.

Question

Because of the Privacy Rule, doesn't the FIMR program know that hospitals cannot provide complete medical record information to FIMR for case reviews? Hospitals are only allowed to provide the minimum amount of information.

Answer

In certain circumstances, the Privacy Rule does permit a physician or hospital to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. This "reasonable reliance" is permitted when the request is made by:

- A public health official or agency for a disclosure permitted under the rule.
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

Also, hospitals are permitted to provide complete information under the current state law.

Question:

The hospital has asked the FIMR abstractor to leave his or her name, address and a picture identification (e.g. driver's license) in any chart from which he or she abstracted. Does the FIMR abstractor have to leave this information in each medical record that is reviewed?

Answer:

It depends. The Privacy Rule requires a covered entity to provide a patient who requests it in writing with an accounting of certain disclosures of her protected health information made by the covered entity for the six years prior to the request (but after the compliance date). Such disclosures would include disclosures to FIMR for research and public health activities.

The Privacy Rule does not require an accounting if the FIMR program has obtained individual authorization.

According to HIPAA, an accounting only includes the four following requirements:

(1) the date of the disclosure;

(2) the name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(3) a brief description of the protected health information disclosed; and

(4) a brief statement of the purpose of the disclosure.

The FIMR program should prepare a letter from the local Commissioner of Health or other agency sponsor on agency letterhead to include for the hospital's or physician's disclosure records. (See Appendix C)

Question:

Could the medical abstractor be subpoenaed to disclose case review information or findings because his or her name is in the medical record? Could other members of the FIMR case review team be contacted or subpoenaed because the trail led from the abstractor to the FIMR review team members?

Answer:

Since 1984, FIMR programs all over the country have successfully reviewed tens of thousands of de-identified cases. To the best of our knowledge, no FIMR staff or team members have ever subpoenaed.

However, the possibility of FIMR staff or team members being subpoenaed, though remote, has always been a concern. For this reason, almost all FIMR programs have chosen not to review cases actively involved in litigation or criminal prosecution.

In addition, the state Title V director has confirmed that the state law that will continue to protect local FIMR from discovery and gives team members immunity is ———————-.

Question:

How does the Privacy Rule affect state privacy laws?

Answer:

The Privacy Rule allows state laws (including procedures established under such laws) to remain in effect if they provide for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention. **Therefore, the Privacy Rule does not affect any state law that provides for such reporting or conduct.** To the extent that a covered entity is disclosing information to a FIMR program under such a law, the Privacy Rule will not prohibit the disclosure.

Question:

How does the Privacy Rule affect state laws that grant peer review or other type of protection to FIMR reviewers?

Answer:

The Privacy Rule will not affect the protections afforded to peer review information under state law. Peer review information generally is not used to make decisions about the individual; rather,

it is used to improve patient care at the community level. Therefore, peer review information usually is not considered part of a designated record set.

Question:

What impact does the Privacy Rule have on Freedom of Information Act ("FOIA") requests for minutes of FIMR case review meetings?

Answer:

Under FOIA and similar state laws, federal and state agencies are required to disclose certain information in their possession to the public. Reporters sometimes have mistakenly assumed that FIMR information was covered by this requirement and was accessible. However, FOIA sets forth exemptions to this requirement.

For example, FOIA exemption 6 permits a federal agency to withhold personnel and medical files and similar files which would constitute a clearly unwarranted invasion of personal privacy.

The state freedom of information exemptions apply to FIMR.

Question:

Under the new HIPAA regulations, could a family request a copy of the de-identified summary of the FIMR case summary and/or the recommendations that the Case Review Team made about the death?

Answer:

No. FIMR programs are not covered entities. Therefore the HIPAA Privacy Rule does not apply to FIMR.

A family who request such information might be told: "I am sorry but we are not able to provide that information to you. All information from individual cases has been de-identified and is nameless. Therefore, we cannot link any family's name back to their summary or recommendations of a case. We did this to ensure that any information about you, your baby and your family would remain strictly confidential."

Question:

What is the FIMR program doing to prepare for HIPAA?

Answer:

To get ready for the HIPAA regulations and the Privacy Rule that will take effect on April 14 2003, the FIMR program is:

- Reviewing the new National FIMR guidance on HIPAA
- Meeting with the state Title V director to clarify the state regulations that protect

FIMR reviews from discovery and give the team members immunity and determine which sections of the HIPAA regulations are pertinent to the FIMR program's access to protected health information.

- Keeping a record of all the state statutes and HIPAA regulations that support the local FIMR program.
- Taking this positive opportunity to review all the FIMR policies and procedures to maintain confidentiality of protected health information and to strengthen them, as needed. Confidentiality has always been key to the FIMR process.

VI. Conclusion

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations will take effect on April 14, 2003. The intersection between HIPAA and FIMR arises as FIMR programs collect information needed for case reviews from hospitals and providers, which are entities covered by HIPAA.

FIMR programs are not covered entities. Therefore, the Privacy Rule does not appear to apply directly to FIMR programs. However, it may impact the ability of FIMR programs to obtain protected health information from covered entities. The effect of the Privacy Rule on a FIMR program depends on the specific facts and circumstances surrounding the program. In general, FIMR programs will continue to be able to access information from maternal and infant health records after these regulations are implemented.

For the majority of FIMR programs, disclosures by hospital and physicians to the FIMR program will be for the purpose of public health activities. Others will be for the purpose of research. Under the Privacy Rule, covered entities may disclose protected health information for either purpose without individual authorization.

In addition, the Privacy Rule allows state laws (including procedures established under such laws) to remain in effect if they provide for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention. Current state laws or regulations, which support the FIMR program for the conduct of public health surveillance and intervention, will be unaffected.

Finally, under the new HIPAA regulations, hospitals or providers should anticipate a FIMR program's request for access to medical records and be prepared to respond positively. However, the local FIMR program can greatly enhance its credibility and access to information by making sure that hospitals and providers 1) know about the benefits of the local FIMR, 2) understand that confidentiality is key to the FIMR process, 3) are included in the FIMR case review team and 5) receive explanatory information such as the Sample Health Officer Letter (see Appendix C) when records are requested.

Appendix A

HIPAA Section 164.512(b) *–Public Health Disclosures

Uses and Disclosures for which an authorization or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to applicable requirements of this section.

(a) *Standard: uses and disclosures required by law.*

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure complies with and is limited to the relevant requirements of such law.

(1) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: uses and disclosures for public health activities.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

Note: this citation is current at the time of the printing of this document. It is subject to change. Please consult the HHS web site www.hhs.gov/ocr.hipaa for the most up to date version of HIPAA.

Appendix B

Sample FIMR Medical Authorization Form

(NB: FIMR programs, which do not access protected health information through research or public health provisions, may be required to obtain patient authorization. This is a sample of an individual authorization form, which incorporates the HIPAA individual authorization requirements listed on p. 7–8)

Purpose of the Study

The Fetal and Infant Mortality Review Program ("FIMR Program") sponsored by the Great Beginning Program in Kerry County is conducting a study of miscarriages and infant deaths in our area. The purpose of the study is to learn more about each death and to find ways to help families such as yours in the future.

To achieve these goals, each case review will have two parts: (1) a summary of a personal interview with you (or other family member), if you agree; and (2) a review of records related to your infant's care and your pregnancy, delivery and other records that may pertain to the purpose of the study.

Benefit of Participation

Participation in this program may not benefit you or your family directly but may prevent other families from having a loss like yours.

Authorization to Disclose and Use Health Information—Confidentiality of Records

If you would like to participate in this study, you will need to sign this Authorization form. Your signature on this form will allow your health care providers to disclose to representatives of the FIMR Program health information related to your loss, including prenatal, labor, and infant health medical records.

Once a health care provider discloses health information to a third party, such as the FIMR program, the information may no longer be protected by federal privacy laws and could be disclosed further by the FIMR program (if allowed by state law). However, the FIMR Program promises to keep strictly confidential all information that identifies you or your infant. This information will not be given to anyone outside of the FIMR Program and will be destroyed after your case has been reviewed by the Case Review Team. Neither your name, your infant's name, nor the name of anyone else in your family will appear in any reports about the Program. Finally, all of the FIMR Program staff and team members have taken a written oath to protect your privacy.

FIMR Program staff and team members will use the health information collected during the personal interview (if applicable) and from your health care providers to conduct this study. All information that could be used to identify you, your family, or your health care providers will be removed before the Case Review Team studies your case. This information will be kept in a locked file cabinet. Access to this cabinet is restricted to FIMR program staff.

You do not have to participate in this study. You should be assured that a decision not to partici-

pate will not affect your ability to obtain services from the Great Beginnings Program in Kerry County now or in the future.

You may change your mind and revoke (cancel) this Authorization at any time and for any reason, except to the extent that your health care providers and FIMR Program staff and team members have already relied on it. To cancel this Authorization, you must write a letter to Mary Smith, Director, Great Beginnings Program, 100 Main Street, Center City, CA 91234.

Compensation

Your involvement in this program is voluntary and you will not be paid for participating.

Questions

If you have any questions concerning your rights as a participant, please call (name of individual) who is the Director of the FIMR Program at (phone number).

Expiration

This Authorization will expire (end) 60 days after your case is reviewed.

By signing below, you indicate that you have read this form and understand the purpose of and conditions for participation in the FIMR Program. You will be given a copy of this Authorization after you have signed it.

_____ _____

Signature of participant or participant's legal representative Date

_____ _____

Printed name of participant or participant's representative Representative's relationship to participant

_____ _____

Witness to Signature Date

Adapted from: Western North Carolina FIMR Program, Asheville

Appendix C

A Sample Health Officer Letter

To: Whom It May Concern

From: Jane Smith, MD, MPH
Commissioner of Health Services
100 Main Street
Center City
Kerry County, CA 91234

Date: April 14, 2003

Subject: Authority to Conduct Fetal and Infant Mortality Review (FIMR)

The Department of Health Services has been charged by the State of California with conducting the Fetal-Infant Mortality Review (FIMR) Project for Kerry County. The purpose is to study fetal, neonatal and post-neonatal deaths in order to identify systems factors associated with them. A primary objective is to pinpoint possible gaps in services, which may be amenable to community or governmental action.

Information is gathered from birth and death certificates, medical records, autopsy reports and family interviews. Standard medical record abstraction forms, developed by the National Fetal and Infant Mortality Review Program—a partnership between the American College of Obstetricians and Gynecologists and the federal Maternal and Child Health Bureau, are used to collect a small subset of information from these records. In turn, FIMR staff summarizes this information. Names of providers, institutions and families are carefully removed from the summary in order to de-identify the information. Confidentiality is key to FIMR.

The anonymous, de-identified summaries are presented to the interdisciplinary Case Review Team for interpretation, conclusions and recommendations. The FIMR Community Action Team provides a mechanism by which the Department takes recommendations to community wide action to improve services and resources for women, infants and families.

Under provisions of California Health and Safety Code §100325 (General Powers of the Department of Health Services), the local health officer may obtain access to medical records for the purpose of public health investigation of fetal and infant deaths. I have assigned this authority to implement the Fetal-Infant Mortality Review (FIMR) Project to my staff in the County Department of Health Services Family Health Programs/Maternal and Child Health. This memorandum provides authorization for the FIMR Project staff to review relevant health and medical records from your institution for this purpose. I certify that the records, which we request, pertain to an infant who has died.

This authority shall be valid until April 13, 2004 and will be re-authorized on a yearly basis.

I urge you, as a key partner in this process, to facilitate access to information for review of this case. I appreciate your cooperation in this public health endeavor to further promote and protect the health and well being of women, infants and families in Kerry County. For more information about the Fetal-Infant Mortality Review Project, you may contact me at the above address.

Adapted from the Florida Pregnancy Associated Mortality Review, Kern County, CA and Los Angeles County, CA FIMR Program Authorization Memorandums

Appendix D

Sample Public Health Laws Affecting FIMR

NEW YORK STATE PUBLIC HEALTH LAW

§ 206.1(j) Commissioner; general powers and duties

1. The commissioner shall:
(j) cause to be made such scientific studies and research, which have for their purpose the reduction of morbidity and mortality and the improvement of the quality of medical care through the conduction of medical audits within the state. In conducting such studies and research, the commissioner is authorized to receive reports on forms prepared by him and the furnishing of such information to the commissioner, or his authorized representatives, shall not subject any person, hospital, sanitarium, rest home, nursing home, or other person or agency furnishing such information to any action for damages or other relief. Such information when received by the commissioner, or his authorized representatives, shall be kept confidential and shall be used solely for the purposes of medical or scientific research or the improvement of the quality of medical care through the conduction of medical audits. Such information shall not be admissible as evidence in any action of any kind in any court or before any other tribunal, board, agency or person.

MASSACHUSETTS

Chapter 111.PUBLIC HEALTH LAW

Chapter 111: Section 24A. Reduction of morbidity and mortality; establishment of program; information and reports.

Section 24A. The commissioner may authorize or cause to be made scientific studies and research, which have for their purpose the reduction of morbidity and mortality within the commonwealth. All information, records of interviews, written reports, statements, notes, memoranda, or other data procured in connection with such scientific studies and research conducted by the department, or by other persons, agencies or organizations so authorized by the commissioner shall be confidential and shall be used solely for the purposes of medial or scientific research. The furnishings of such information to the department or to the authorized representative of such an authorized study or research project, shall not subject any person, hospital, sanitarium, rest home, nursing home or other person or agency furnishing such information, to any action for damages or other relief.

Appendix E

A Glossary of HIPAA Terms

Authorization Form: A form that a healthcare provider must obtain from the individual patient or patient guardian in order to use or disclose the individual's protected health information (PHI) for purposes other than for treatment, payment, and healthcare operations (TPO) or for specific purposes listed in the Privacy Rule, such as public health surveillance or research.

Business Associate: A person or entity that is not a member of a hospital or physician workforce who uses or discloses PHI to carry out certain functions or activities on behalf of the hospital, physician or other covered entity.

Covered Entity: Under HIPAA, this includes health plans, healthcare clearinghouses and any healthcare providers (physicians, hospitals, nursing homes, etc.) who transmit any health information in electronic form in connection with a HIPAA transaction.

Designated Record Set: A group of records maintained by or for a covered entity that is:

- the medical records and billing records about individuals maintained by or for a covered healthcare provider;
- the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- used, in whole or in part, by or for the covered entity to make decisions about individuals.

Direct Treatment Relationship: A treatment relationship between an individual and a healthcare provider in which the provider delivers healthcare directly to an individual rather than through another healthcare provider.

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

Health Information: Any information created or received by a hospital or provider that relates to the past, present, or future physical or mental health condition of a patient, or the past, present or future payment for the provision of healthcare to a patient, or the provision of healthcare to a patient.

Health Plan: An individual or group plan that provides, or pays the cost of, medical care.

Healthcare: Healthcare includes, but is not limited to, the following:

Preventive, diagnostic, therapeutic, rehabilitative maintenance, or palliative care, and counseling service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Healthcare Clearinghouse: Under HIPAA, this is an entity that processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or that receives a standard transaction from another entity and processes or facilitates the processing of that information into nonstandard format or nonstandard data content for a receiving entity.

Healthcare Provider: A person or organization that provides, bills and is paid for healthcare services.

Minimum Necessary: In regard to HIPAA, the principle that, to the extent practical, individual identifiable health information (IIHI) should only be disclosed to the extent needed to support the intended purpose of the disclosure of the information for treatment.

Office of Civil Rights (OCR): The HHS sub-department responsible for the enforcement of the HIPAA privacy rules.

Payment: The activities by the hospital or provider to obtain reimbursement for healthcare services. This includes, among others, billing, claims management, collection activities, verification of insurance coverage and pre-certification of services.

Protected Health Information (PHI): With few exceptions, includes individually identifiable health information held or disclosed by a hospital or provider regardless of how it is communicated (e.g., electronically, verbally, or written.)

Treatment: The provision, coordination or management of healthcare and related services by one or more healthcare providers; consultation between health care providers relating to a patient or the referral of a patient for healthcare from one provider to another.

Use: With respect to protected health information (PHI), the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Appendix F

Sample FIMR Checklist

This checklist is a simple method to help focus a FIMR program's preparation for the introduction of the HIPAA regulations and the Privacy Rule. Local FIMR programs and state Title V agencies are encouraged to develop and add additional checklist items that are relevant to their circumstances.

All FIMR programs should review the first general section of the checklist. Then based on whether the FIMR program will seek medical record disclosure through public health, research or individual authorization, select and review the appropriate one of the three remaining sections.

General

Yes	*No*	
❑	❑	Are you expecting any issues to be raised about FIMR and the HIPAA Privacy Rule?
❑	❑	Have you contacted your State Title V director to clarify these issues and to document the current status of your FIMR program?
❑	❑	Do you know the state and local laws that pertain to your FIMR program?
❑	❑	Do you have copies of these laws?
❑	❑	Did you obtain buy-in from local hospitals and physician groups? Are representatives from those groups on your case review and/or community action teams?
❑	❑	Have you developed a form letter for the covered entity explaining why HIPAA permits disclosure to your FIMR program? (See Appendix C)
❑	❑	Can you answer the questions about FIMR and the Privacy Rule (see pages 16–22)?
❑	❑	Does your sponsoring agency, as well as your FIMR staff, understand why the Privacy Rule permits disclosure of medical records information to FIMR?
❑	❑	Do your case review team members understand why the Privacy Rule permits disclosure of medical record information to your FIMR?

Yes	*No*	
		Have you updated your
❑	❑	- interview consent form
❑	❑	- other forms, as needed
❑	❑	- confidentiality protocols and procedures

PUBLIC HEALTH

Yes	*No*	
❑	❑	Does a state law public health or regulation support your FIMR?
		Does it provide for
❑	❑	- immunity for team members
❑	❑	- protection from discovery
❑	❑	Is the purpose of this law "for the conduct of public health surveillance or investigation or intervention?
❑	❑	Do you have a copy of this state law?
❑	❑	Can you quote the statute? (e.g. "The law that protects our FIMR is public health law 206 (1) (j))
❑	❑	What exemption from your state's Freedom of Information Act (FOIA) apply to your program?
❑	❑	Do you have a copy of the FOIA exemptions?

RESEARCH

Yes	*No*	
❑	❑	Did your State Department of Health apply for and receive approval from the Department's Institutional Review Board to conduct FIMR without individual authorization?
❑	❑	Do you have copies of these approvals?
❑	❑	Did you apply for and receive approval from your local hospitals and public health department IRBs to conduct FIMR?
❑	❑	What exemption from your state's Freedom of Information Act (FOIA) apply to your program?
❑	❑	Do you have a copy of the FOIA exemptions?

Individual Authorization

Yes	*No*	
❑	❑	Do you request permission of the mother to review her medical records?
❑	❑	Have you revised your authorization (consent) form to comply with the HIPAA Privacy Rule?
❑	❑	Do you have data about the number of mothers who agree to or decline the authorization form to release medical records?

To learn more about the fetal and infant mortality review process, please write, fax or call:

NATIONAL NFIMR FETAL–INFANT MORTALITY REVIEW PROGRAM

THE NATIONAL FETAL AND INFANT MORTALITY REVIEW PROGRAM

THE AMERICAN COLLEGE OF OBSTETRICIANS AND GYNECOLOGISTS

Mailing Address: PO Box 96920, Washington, DC 20090-6920

Fax: 202-484-3917 • Phone: 202-863-2587 • E-mail address: nfimr@acog.org • Web Site: www.acog.org/goto/nfimr