SUMMARY OF NEW FEDERAL MEDICAL PRIVACY PROTECTIONS FOR VICTIMS OF DOMESTIC VIOLENCE

June 4, 2003

Written by Rodney Hudson JD, an Associate of Drinker, Biddle and Reath
for the Family Violence Prevention Fund
www.endabuse.org

..

The Department of Health and Human Services (HHS) released the final modifications to the federal medical privacy regulation on August 9, 2002. This regulation provides important new protections for victims of domestic violence and incorporates some—but not all—of the protections set forth in *Health Privacy Principles for Victims of Domestic Violence* (Family Violence Prevention Fund (October 2000) (endabuse.org)) that protect the privacy of victims. The following provides background and a brief description of the domestic violence related provisions of the regulation as adopted by HHS.

I. BACKGROUND

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required that the Secretary of HHS issue health privacy regulations if Congress did not enact comprehensive health privacy protections by August 21, 1999. Congress failed to act by the deadline. The Secretary released proposed regulations in November 1999. The Secretary received over 52,000 comments, including many from domestic violence advocates, shelters, state coalitions, and national domestic violence and women's organizations about how those protections should be crafted.

As required by HIPAA, HHS published the final regulation in the *Federal Register* on December 28, 2000. This regulation became effective on April 14, 2001 but covered entities were not required to comply until later. On March 20, 2002, HHS proposed modifications to the privacy regulation. The final modifications, which scaled back some of the basic protections included in the December 28, 2000 version, was published in the *Federal Register* on August 14, 2002. The modifications to the regulation took effect on October 15, 2002. Covered entities, except small health plans, must comply with the regulation by April 14, 2003. Small health plans have an additional year to comply.

II. COMPREHENSIVE PROTECTIONS REQUIRE CONGRESSIONAL ACTION

Under HIPAA, the Secretary only had authority to require that health care providers, health plans and health care clearinghouses comply with the regulation. Therefore, despite the new regulations, many entities that regularly receive health information, including employers (see special rules regarding employers below), casualty and property insurance companies and workers compensation carriers, are not required by this federal law to protect patient privacy.

HIPAA also limited the Secretary's authority to enforce the regulation. The Secretary only has authority to impose civil and criminal penalties against covered entities for violating privacy standards. Individuals do not have a right to bring a federal lawsuit to enforce the regulations or recover damages. This is unlike many other federal privacy laws [i] that permit individuals to bring federal suits.

States may enact stronger privacy protections that cover employers, casualty and property insurance companies and workers compensation carriers or they could enact state laws that give individuals the opportunity to bring lawsuits. Congress may also enact legislation that changes the protections or allows individuals to bring federal lawsuits.

III. NEW FEDERAL MEDICAL PRIVACY RULES

A. Impact on More Protective State Laws

The new federal rules do not preempt state laws that are more protective of patient privacy. Therefore, the regulations may have little impact on patient privacy in states with strong privacy laws and a significant impact in states with weak privacy laws. In addition to not preempting more protective state laws, the regulation does not preempt state laws that authorize or prohibit disclosure of health information about a minor to a parent, guardian or person acting in loco parentis. For a summary of state privacy laws see the Georgetown University Health Privacy Project's *The State of Health Privacy: An Uneven Terrain* (Health Privacy Project (July 1999) (healthprivacy.org)). As a result, advocates working in states have the opportunity to push for state legislation to strengthen the rules where they do not fully meet the needs of victims.

B. Overview of General Privacy Protections

The new regulation is the first federal medical privacy law in U.S. history of its kind. While many states have laws that protect patient privacy, the new regulation creates a federal floor for privacy protections to ensure that minimum level of protections are in place in all states. Due to the submitted comments from advocates for battered women on the regulations, there are many important provisions of the regulation directly effect victims of domestic violence.

- Who is covered?

Health care providers, health plans and health care clearinghouses that transmit information electronically are covered.

Under HIPAA, health plans, health care clearinghouses and health providers that transmit information electronically must comply with the regulation. Many entities that regularly use and disclose health information, such as employers, casualty and property insurance companies and workers compensation carriers are not required by this federal law to protect patient privacy.

- What is covered?

All health information maintained by a covered entity is protected including

Electronic and paper records as well as oral communications are protected under the regulation.

- What does the regulation require and prohibit?

Covered entities are prohibited from using and disclosing protected health information unless expressly permitted or required by the regulation

In the most general sense, the regulation *prohibits* use and disclosure of protected health information unless expressly permitted or required by the regulation. The regulation *requires* disclosure (1) to the individual who is the subject of the information and (2) to HHS for enforcement purposes.

- Do health plans and providers have to obtain consent prior to disclosing health information?

The final modifications to the regulation eliminated the fundamental requirement included in the December 2000 rule that health care providers obtain consent prior to use or disclosure of protected health information.

This requirement was replaced with a requirement that only requires entities to make a good faith effort to inform patients in a notice of privacy practices about how sensitive information is used and disclosed.

An individual must be notified of his or her rights and how information will be used and disclosed

The regulation requires a covered entity to provide individuals with a written notice of the entity's privacy practices. Providers that have a direct treatment relationship with an individual are only required to give notice at the date of the first service of delivery; and except in emergency circumstances, must make a good faith effort to obtain a written acknowledgment from the individual of receipt of the notice. Providers must also have notice posted on the premises. Health plans are required to give notice at enrollment and to notify individuals every three years that the privacy practices notice is available. Both providers and plans have special notice requirements if their privacy practices change.

The notice must be written in plain language and specifically describe the types of uses and disclosures for treatment, payment and health care operations, including one example. The notice must also describe other purposes for which information may be used and disclosed without authorization, such as in the case of mandatory reporting, and describe prohibited disclosures. The notice must contain a separate section if entities intend to contact the individual for appointment reminders or treatment alternatives or for

fundraising purposes. Individuals must also be notified that they have the right to request certain restrictions, receive confidential communications, inspect and copy records, amend information and receive an accounting of disclosures.

- How much information is shared?

A covered entity must make reasonable efforts to use and disclose only the minimum amount of information necessary

An entity must make reasonable efforts to limit the use or disclosure to that which is necessary to accomplish the purpose of the use or disclosure. Also, when making requests for information, a covered entity may only request information that is necessary to accomplish the purpose of the request. For routine uses and disclosures, a covered entity may implement policies and procedures to ensure that the minimum necessary standard is followed. Disclosures that are not routine must be reviewed on an individual basis.

This standard does not apply in a number of circumstances including 1) disclosures to or requests by health care providers for treatment, 2) disclosures to the individual who is the subject of the information, 3) disclosures to the Secretary for enforcement and compliance, 4) uses and disclosures for which the entity has received a valid authorization, and uses or disclosures required by law.

Recommendation: Although de-identification is not required by the Privacy Regulation, personal identifiers (such as an individual's name, address, telephone number, birth date and Social Security Number) should be removed to the fullest extent possible, before the information is used or disclose.

Although the regulations generally require entities to take steps to limit disclosure of protected information to those who most need the information, it has numerous exceptions. In general, limit access to personally identifiable health information on a need – to-know basis and limit disclosures to the minimum amount necessary. If possible the entire record/chart should not be released to process a claim, only the information that is necessary to secure payment should be disclosed.

- How Can Health Care Providers Use Health Information?

Health care *providers* may use and disclose protected health information for their own treatment, payment and health care operations without obtaining an individual's consent and may disclose information to other covered entities (health plans, clearinghouses and other health care providers) for specified purposes.

The regulation permits health care providers to use and disclose an individual's protected health information for its own treatment, payment and health care operations without obtaining an individual's consent. Providers may also disclose protected health

information, without an individual's permission, to other covered entities for treatment by or payment of another health care provider, payment activities of another covered entity and for certain other health care operations of another covered entity, if both entities have or have had a relationship with the individual who is the subject of the information and the information requested pertains to that relationship.

For example, a provider who treats a patient that has disclosed abuse may feel that information is important to ensuring appropriate care for the patient and pass that information on to a mental health or other specialist for treatment purposes without the patient's consent.

Recommendation: Providers should only share information about domestic violence that is necessary to the appropriate care of the patient and preferably with the patients consent.

- Can patients receive an accounting of who their records have been disclosed to?

Individuals have the right to inspect, copy, amend and receive an accounting of disclosures.

An entity must permit individuals to inspect and copy records. Individuals may also amend their records and receive an accounting of disclosures for up to the last six years. The right to an accounting only extends to "disclosures" (outside of an entity) and not to "uses" (within a covered entity). There are additional exceptions to the right to receive an accounting, including a temporary suspension of the right when there has been a disclosure to a law enforcement agency.

For example, an individual would not have a right to a list of all hospital employees who have had access to his or her health information.

Recommendation: Particularly when a patient is a victim of abuse a health staff person should review the privacy policies of the health system, the patients rights and options **verbally,** in a language they understand or with the assistance of an interpreter to be sure the patient fully understands her/his options to protect the privacy of her/his medical records.

- Can Patients Agree to, Object to or Restrict Disclosures?

An individual must be *informed in advance and be given an opportunity* to agree to, object to or restrict certain uses and disclosures

An individual must be informed (either in writing or orally) of his or her opportunity to agree, prohibit or restrict the disclosure of health information before the information is used in a health care facility directory or disclosed to persons involved in the individual's care.

These opportunities include:

- Use of information in a health care facility directory

A patient has the right to restrict or object to the used of information in a health care facility directory.

For example, a victim of domestic violence admitted in a hospital may choose not to have her name listed at all in the directory – if for example, she feels that this may put her at risk from her abusive partner.

If an individual does agree to have his or her information included in a health care facility directory, the entity may only include the individual's name, location, condition and religious affiliation in the directory. An entity may only disclose an individual's religious affiliation to clergy. All other information may be disclosed to others who ask for the individual by name unless the individual objects.

If an individual is incapacitated or receives emergency treatment and consent cannot practicably be given, an health care system may use the information for directory purposes, if the use of the information is consistent with the patient's prior preference (if any is known to the provider) and in the patient's best interest. When it becomes practicable, a provider must inform the individual of his or her rights and give the individual an opportunity to object to being included in the directory.

Recommendation: Individuals who are capable of opting out or limiting the amount of information to be included in the directory should be given the opportunity to exercise their right to do so upon admittance. Directory use should be explained to patients who are victims of abuse so they can make informed decisions about whether to opt out. If an individual opts out of the directory information, health care staff should also use care when making comments or using names on emergency department boards.

- Disclosure of other health information to persons involved with the individual's care

Patient information may be disclosed to a family member, other relative, or close personal friend involved in the individual's health care if (1) the individual agrees, (2) the individual is given an opportunity to object and does not, or (3) the entity reasonably believes from the circumstances that the individual does not object.

If the individual *is not present, is incapacitated or an emergency exists*, information may be disclosed if a covered entity determines that it is in the best interest of the individual. In such cases, only that health information directly relevant to the person's involvement with the patient's health care may be disclosed.

For example, if a patient who is a victim of domestic violence does not want information shared with her abusive partner s/he has the right to limit that information.

Recommendation: Access to information by next-of-kin should be granted only with the explicit and informed consent of the patient. Providers should verify who is requesting the information as next of kin.

- Can a patient restrict disclosures for treatment, payment and health care operations?

An individual must be given an *opportunity* to restrict uses and disclosures for treatment, payment and health care operations.

An individual may request that the use and disclosure of information for treatment, payment and health care operations be restricted. For example, a patient may request that information about a particular condition or procedure be kept confident and not shared with others. Providers are not required to agree to such requests. Covered entities that do agree to limitations on use and disclosure may not use information in violation of that restriction, except in limited emergency situations.

For example, a victim of abuse could request that the domestic violence not be shared with other providers or health plans. The provider is not required to agree but may agree to such a limitations.

Recommendation: Providers and health plans should comply with patients who are victims of abuse requests to limit disclosures for treatment, payment and health care operations out of respect of her/his own privacy and autonomy.

- Can individuals alter the way providers communicate with them?

Health care providers and plans must *accommodate reasonable requests* by patients about how and where to communicate with them

A health care provider must accommodate reasonable requests by an individual to receive communications about protected health information by alternative means or at alternative locations. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card, as an alternative means. A provider may not require an explanation for the basis for such requests.

For example, a victim who does not want her partner to know about treatment for domestic violence injuries may request that the provider communicate with her by mail to a different address, or by phone to a designated phone number.

A health plan must also accommodate reasonable requests about how and where to communicate with the individual if the individual states that disclosure could endanger

the individual. Other than requiring a patient to make this statement, health plans cannot ask about particular circumstances. They must accommodate the request.

For example, the plan must accommodate a request to send an explanation of benefits about particular services to a designated address rather than a home address because the individual is concerned that a member of the individual's household (i.e. the named insured) might read the explanation of benefits and may retaliate against her.

Recommendation: ideally all victims should be notified in person of the option to send information to alternate addresses or communicate with her in an alternate fashion and offered assistance in securing safe alternatives. If insurance information is sent to the abuse, make other billing arrangements according to the situation.

- Can health plans or providers refuse to treat a person as the patients personal representative?

Entities may refuse to treat a person as a patient's personal representative with respect to health information if the entity believes that the representative has or may subject the patient to abuse or neglect or that the patient would be endangered by the disclosure

A covered entity may refuse to treat a person (including a parent or spouse) as a patient's personal representative if the entity believes that (1) it is in the best interest of the patient and (2) either the person has subjected or may subject the patient to abuse or neglect, or (3) treating the person as the patient's personal representative would endanger the patient.

Recommendation: Providers should exercise discretion when possible to ensure the privacy of victims.

- Can health plans or providers refuse to provide a patients health information to a a patients personal representative?

Entities may refuse to provide personal representatives access to a patient's health information

Even if a person is generally treated as a patient's personal representative, an entity may deny the personal representative (including a parent or spouse) access to the patient's health information if the entity believes that the disclosure is reasonably likely to cause substantial harm to the patient or another person.

For example, if a provider treating a patient who is a victim of domestic violence has decided to refer the patient to an on-site domestic violence advocate, they can choose not to share that information with the patient's spouse if they feel that sharing information may harm the patient.

Entities exercising this option, however, must inform the personal representative of the basis of the denial in writing within thirty days.

Recommendation: Health care providers should have broad discretion to withhold information from third parties when disclosure could harm the patient who is the subject of the information.

PSYCHOTHERAPY NOTES

- How are psychotherapy notes treated in the new regulations?

Entities must obtain *authorization* from the individual to use and disclose psychotherapy notes:

A covered entity must obtain an authorization from the patient to use and disclose psychotherapy notes for treatment, payment and health care operations, except where the notes are used by the person who wrote them, or for training purposes by the covered entity in which students, trainees or practitioners in mental health are under supervision to practice or improve their skills. A covered entity may not condition treatment on the signing of such an authorization.

Psychotherapy notes can be disclosed under the following circumstances:

Covered entities *may* disclose psychotherapy notes without an authorization for other purposes including (1) to defend a legal action or other proceeding brought by the individual, (2) to comply with a compliance investigation by the Secretary when required by law, (3) for oversight activities authorized by law, including audits, and civil, administrative, or criminal investigations, (4) for inspections, licensure or disciplinary actions, (5) for civil, administrative or criminal proceedings, (6) when the disclosure is about decedents, and (7) when the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person reasonably able to prevent or lessen the threat.

MINORS

- What about access to and disclosures of protected health information related to minors?

Generally, a parent is the personal representative of an unemancipated minor and is deemed to be able to exercise the rights associated with the minor's health information. In most cases, the minor would not have the rights associated with his or her own medical information.

There are circumstances, however, in which an unemancipated minor has the exclusive right (with the possible exception of disclosures to his or her parents) to authorize disclosure of related health information. An unemancipated minor controls access under the following circumstances:

- The minor is authorized by law to consent to treatment and has consented to care (with or without the consent of the parent); or

- The minor may lawfully obtain health care without the consent of a parent or guardian, and the minor, a court or another person authorized by law consents to such health care; or

- The parent or guardian assents to an agreement of confidentiality between the provider and the minor.

The issue of disclosure and access to a minor's health information is largely governed by state law. The new federal regulation allows covered entities to disclose a minor's health information to a parent (or provide the parent with access to such information) if such disclosure (or access) is permitted or required by state law. Similarly, such access would not be permitted if prohibited by state law. Where state law is silent or unclear with respect to access by parents, the regulation permits a covered entity to provide or deny access to the parent so long as that action is consistent with state law and the decision is made by a licensed health care professional.

Recommendation: Those states that do not have laws to prevent the release of minor's records to parents should advise patients who are minors about the limits of confidentiality and/or push to enact laws that further protect the privacy of a minor's medical records.

REPORTING REQUIREMENTS

- How do the new regulations impact child abuse and domestic violence reporting laws?

Health information may be disclosed without authorization for limited public policy purposes, including abuse reporting laws, if certain requirements are met

There are several circumstances where covered entities may use or disclose protected health information without the written consent or authorization of the individual, including disclosures to report child abuse and neglect; about a victim of abuse, neglect or domestic violence under certain circumstances; for law enforcement purposes; and for judicial and administrative proceedings.

- Entities may disclose child abuse and neglect information to the appropriate government authority for public health purposes

A covered entity may disclose health information for public health purposes to a public health authority authorized by law to receive such a report. Entities may disclose information pertaining to injury and child abuse or neglect to a government authority authorized by law to receive such reports.

- Entities may disclose information about abuse (other than child abuse), neglect or domestic violence under certain circumstances

A covered entity may disclose protected health information about a victim of abuse (other than child abuse), neglect, or domestic violence to an authorized government authority if (1) the individual agrees, or (2) the disclosure is (a) required by state law (mandatory reporting laws) or (b) expressly authorized by statute or regulation.

Mandatory reporting laws fall under the provision relating to disclosures *required by law*. This provision does not change the actual reporting from provider to the appropriate authority, but requires that providers consider the circumstances of the victim (see the section on notice below) prior to reporting.

Before disclosing information that is *expressly authorized by statute or regulation*, the entity may only disclose that which is authorized under the law and must believe that the disclosure is necessary to prevent serious harm to the individual or other victims. For example, Wisconsin elder law (Wis. Stat. §36.90(4)) states that any person may report to a county agency or state official that he or she believes that abuse or neglect has occurred. Under the federal regulation, an entity may make a report only if the specific type of the report (e.g. elder abuse) is included in the law authorizing the report.

In cases where an individual is incapacitated and the statute expressly authorizes disclosure, a law enforcement or other public official must represent that information is not intended to be used against the victim and that immediate law enforcement activity depends on the disclosure.

- <u>In most instances, entities must inform a victim of abuse or neglect (other than child abuse or neglect) that a report has been or will be made</u>

When disclosing information, providers must *promptly inform* the individual or their personal representative (either orally or in writing) that such report has been made or will be made. **For example, in order to comply with the new regulation, health plans and providers should establish policies that require prompt notice to the individual when reporting domestic violence to law enforcement.**

Covered entities *do not have to inform* individuals if 1) they believe that informing the individual *would place the individual at serious risk of harm*, 2) or the entity would be *informing a personal representative* (such as the abusive partner) and the entity reasonably believes that the personal representative is responsible for the abuse, neglect, or other injury. The entity must also believe that informing the personal representative would not be in the best interest of the individual.

- <u>Entities may disclose health information to law enforcement officials under certain circumstances</u>

Entities may, however, disclose information to law enforcement officials without informing the subject of the information pursuant to a court order or court-ordered warrant or a subpoena, summons issued by a judicial officer, grand jury subpoena, or an administrative request.

Except when required by law, entities may only disclose information for the purpose of identifying or locating a suspect, material witness or missing person in response to a law enforcement request. The entity may only disclose the name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, if applicable, and a physical description of the person.

In cases other than domestic violence, child abuse or neglect or other types of abuse or neglect, entities may also disclose health information in response to a law enforcement request about an individual who is or who is suspected to be the victim of a crime if (1) the individual agrees, (2) the individual is unable to agree because of incapacity or emergency, if the law enforcement official represents that the information is not intended to be used against the victim and that immediate law enforcement activity depends on the disclosure.

In addition, health care providers may disclose health information to report a crime in an emergency. **Child abuse and neglect may be disclosed under this provision but domestic violence and other types of abuse and neglect may not.**

- Individuals seeking health information in judicial and administrative proceedings must make reasonable efforts to notify individuals who are the subject of the information that their health information has been requested or meet other privacy protective requirements

A covered entity may disclose protected health information in response to a court or administrative tribunal order. Information may also be disclosed in response to a subpoena or discovery request if the party seeking the information has made reasonable efforts to notify the subject of the information that his or her information has been sought. In lieu of notice, the party seeking the information may secure a protective order, or the parties may stipulate that they will not use or disclose the information for any purpose other than the litigation or proceeding. As part of a protective order or stipulation, the parties must also agree to return the information to the covered entity or destroy it at the end of the litigation or proceeding.

For example, if a perpetrator is requesting health information about a victim of domestic violence as part of a court order or subpoena they must make reasonable efforts to notify the victim that these records are being requested.

Recommendation: In all cases, victims of abuse should be informed of any disclosure of information that could put them at risk of harm. Where state law and federal regulations permit, this information should only be released with the consent of the patient.

EMPLOYERS

- How do employers have to treat health information of their employees?

Employers with health care components and those that sponsor group health plans must erect firewalls, adopt policies and identify which individuals can have access to health information to ensure that information is not used in employment determinations

Although employers are not covered by the regulation, some employers perform health care functions that will require the health care component of the employer to comply with the regulation.

For example, an onsite clinic of an automobile part manufacturer would be a health care component because the clinic provides health care services. The health care component cannot disclose protected health information to other divisions of the company and must adopt policies and procedures that designate which individuals can have access to health information.

Employers that sponsor a group health plan will also be affected by the regulation. Group health plans include (1) Employee Retirement Income Security Act (ERISA) plans that have fifty or more participants, and (2) ERISA plans, regardless of size, that are administered by an entity other than the employer who established and maintains the plan. As a sponsor of a group health plan, employers may perform certain activities that are similar to that of a group health plan—often requiring access to individual health information held by the group health plan. Even though activities of employers are not directly covered, the effect of the group health plan provisions is that information can only be shared with the employer as plan sponsor in limited circumstances and only when certain requirements are met. For instance, when an employer sponsored group health plan contracts with a health insurance company or HMO, the employer needs access to little information such as a summary of health information to solicit bids from a new insurer or to modify the plan.

Where the employer/plan sponsor needs greater access to protected health information, such as where the employer/plan sponsor approves or pays for a health claim, a group health plan can only disclose limited information. To ensure that information is not improperly used or disclosed, group health plan documents must specifically describe the permitted uses and disclosures of health information and specify that information may only be disclosed when the plan sponsor certifies that it has agreed to restrict the use and disclosure of health information, including not using the information for employment-related actions. Plan sponsors must also erect firewalls to (1) identify the employees or classes of employees who will have access to protected health information, (2) restrict access solely to the employees identified and only for the functions performed on behalf of the group health plan, and (3) provide a way to resolve issues when the plan sponsor does not comply with the agreement.

SHARING INFORMATION FOR BROADER PURPOSES

- Can health information be shared for purposes other than treatment, payment and health care operations?

Entities must obtain *authorization* to use and disclose health information for purposes other than treatment, payment and health care operations

Except for limited public policy purposes (discussed below), covered entities are prohibited from using and disclosing information for purposes other than treatment, payment and health care operations. In order to use information for these other purposes, the entity must obtain the individual's authorization. Generally, an entity may not condition treatment on the signing of an authorization. A provider may, however, condition research-related treatment on the individual signing an authorization. A valid authorization must include—a specific description of the information and the purposes of the use or disclosure, the identity of the person or class of persons authorized to make the requested use or disclosure, the identity of the person or class of persons to whom the covered entity may make the requested use or disclosure, a statement of the person's right to revoke the authorization and the patient's signature and date of the authorization.

- How does this impact enrollment and eligibility for benefits or payment of claims?

Health plans may condition enrollment in a health plan, eligibility for benefits or payments of claims for certain benefits on the individual signing an authorization to disclose information.

Health plans may *condition enrollment in* a health plan or *eligibility for* benefits on an individual signing an authorization if the authorization sought is for the plan's eligibility or determinations relating to the individual for its underwriting or risk rating determinations**.** Health plans cannot condition enrollment or payment of a claim on the individual signing an authorization to use or disclose psychotherapy notes.

A *health plan* may condition *payment of a claim* for specified benefits on the individual signing an authorization permitting another covered entity to disclose information to the plan for treatment, payment or health care operations if the disclosure is necessary for payment of a claim.

IV. CONCLUSION

These new regulations provide important federal privacy protections for domestic violence victims. It is imperative that victims, domestic violence service agencies, health care providers and health care facilities be aware of these protections and to consider the implications of improper disclosure and the impact on victims.

The Family Violence Prevention Fund has also produced a "Summary of New Federal Medical Privacy Protections for victims of DV" and "Sample Business Agreement" (available mid June, 2003). If you have further questions about this issue, you can contact us at www.endabuse.org.

Rodney Hudson, JD, an associate at Drinker Biddle & Reath in San Francisco, California will be available to answer questions about the law and guidelines. From 1999-2001 he worked in the Federal Legislation Clinic at Georgetown Law Center and assisted the Family Violence Prevention Fund in developing recommendations to the administration on the inclusion of protections for victims of domestic violence in the Privacy Regulations, and has continued to help analyze the issue and draft the documents listed above.

[i] Privacy Act of 1974 (5 U.S.C. 522a), Electronic Communications Privacy Act (18 U.S.C. 2701 et seq.), Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), Cable Communications Act (47 U.S.C. 551), Videotape Privacy Protection Act (18 U.S.C. 2710) and the Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.),