Visiting in the HIPAA World

The Health Insurance Portability and Accountability Act of 1996 has created an ever-changing world for how The Mended Hearts, Inc. (MHI), visiting program operates in many medical facilities. Long standing relationships have been severed, and new relationships are becoming harder to create.

Yet, MHI must continue to provide the gift of hope to heart patients, their families and caregivers just as we have for more than fifty years.

Throughout the course of this packet, you will get answers to the following questions:

- What is HIPAA?
- What does it really say/do?
- Who does it affect?
- Why was/is MHI so concerned?
- What can MHI do to limit HIPAA's effects on the visiting program?
- How can national help?
- And, much more.

This information was originally presented at the
2005 MHI National Conference in Charleston, South Carolina.
The presentation was made by Chapter 38 accredited visitor
Alberta Rogers and MHI Field Services Director
Lawrence W. Hood, Jr., on September 3rd and 4th, 2005.

Contents

I hope that you have…
gained an understanding of the limitations of knowledge.
Knowledge, no matter how much it may transform the individual,
is, in the end, not enough…
Science cannot now, and perhaps never will be able to,
give us a complete account of our ultimate nature,
or that of the physical environment in which we live.

– Harold J. Shapiro

What is HIPPA?

Discourage litigation.
Persuade your neighbors to compromise whenever you can…
As a peacemaker the lawyer has a superior opportunity of being a good man.
There will still be business enough.

– Abraham Lincoln

HIPAA is the US Federal legislation known as the Health Insurance Portability and Accountability Act of 1996. This legislation primarily concerns consumer's rights to health care privacy practices. It affects not only how your personal medical information is handled, but how you are treated when working with your doctor, health insurance provider or other medical practitioner. This is all done to protect you.

HIPAA is the government's largest and most aggressive move in healthcare since the creation of Medicare. HIPAA impacts the culture, operations and procedures throughout the healthcare industry.

The purposes of HIPAA are to:

- Ensure the portability of consumers individual medical records if he/she switches doctors, health insurance company, or employers
- Protect consumers personal health information that his/her doctors or health insurance companies keep in their files
- Streamline the process of how doctors process medical requests or payments from health insurance companies
- Simplify how medical providers do business with health insurance companies and other medical providers

There are four components to HIPAA:

- *Privacy* — ensures the privacy of individually identifiable health information and protected health information
- *Transactions and Code Sets* — creates a faster electronic system for the health care industry to process bills, confirm member eligibility, and obtain medical authorizations by establishing uniform methods to transmit patient, administrative and financial data electronically
- *Security* — protects the confidentiality and integrity of electronically transmitted or managed individually identifiable health information
- *National Identifiers* — provides health plans, providers and employers with a unique, national number used for all lines of business and with all other health care groups

What Does it Really Say/Do?

Words must be weighed,
not counted.

– Polish Proverb

The objectives of HIPAA are to:

- Improve the portability and continuity of employee health insurance
- Guarantee coverage when employees change jobs
- Protect patient's medical and personal information
- Standardize electronic transactions that contain medical data

What effects MHI visiting programs the most are the *Privacy Regulations*. Privacy Regulations apply to:

- All member records that contain individually identifiable health information *(i.e. name, address, SSN, medical details, etc.)*
- All electronic, paper and oral forms of the protected health information are covered

This specifically means:

- Providing privacy policies and procedures to patients
- Obtaining consent for use of information
- Notification to patients of how information in shared
- Instructing patients on how to access medical records

In other words, **it could be read** into the wording of HIPAA that hospitals cannot divulge the fact that room 308 has a patient in bed 2 that was admitted after complaining of severe chest pain, or that patient number 108B just had an open heart surgery.

Or, it could read to say that all patients must consent to their information being given to a Mended Hearts Accredited Visitor. And, that same patient could have the right to refuse not only a visit, but that the visitor is notified at all of his/her condition.

Lastly, it could be read to say that Mended Hearts visitors are an integral part of the overall care that an individual patient receives while in the care of that particular medical facility.

Our job, as MHI representatives, is to get all concerned parties to see it as the third option.

Who Does it Affect?

The dogmas of the quiet past are inadequate to the stormy present.
The occasion is piled high with difficulty, and we must rise with the occasion.
As our case is new, so we must think anew and act anew.
– Abraham Lincoln

HIPAA impacts everyone, as either a consumer, professional or volunteer within the medical arena, you are affected in some way. Unfortunately, the impact on organizations and programs such as MHI was not considered while the legislation was being drafted.

The organizations affected the most by HIPAA are:

- Hospitals
- Doctors
- Other Medical Providers
- Payers
- Clearinghouses
- Billing Agencies
- Pharmaceutical Companies
- SUPPORT PROGRAMS

HIPAA not only affects organizations and people, but keep in mind that its objectives also have to deal with processes and informational transmittals. A few of the processes affected by HIPAA include:

- Enrollment
- Eligibility Verification
- Patient Authorization
- Diagnoses and Procedure Coding
- Claims Processing
- Premium Payments
- Ensuring Security of Medical Records
- Contract Negotiation
- Human Resources and Compliance Processes
- Member/Provider Communications

Most people think the effects of HIPAA ended on April 14, 2003. This is the date that the privacy regulations took effect. However, HIPAA is still growing. The deadlines for HIPAA on the four main components were/are: Privacy – April 14, 2003; Transactions and Code Sets – October 16, 2003; Security – April 21, 2005; and National Identifiers – May 23, 2007.

And, let us not forget that the extent of the legal ramifications for HIPAA non-compliance has yet to be fully tested in the U.S. Judicial System.

Why Was/Is MHI So Concerned?

If you have a strong case in law, talk to the judge.
If you have a strong case in fact, talk to the jury.
But, if you have no case in law or fact, talk to the wild elements and bellow like a bull.
– Judge Joe Baldwin

HIPAA was a very scary thing for a number of years, and for very good reason. In the beginning, no one truly understood HIPAA. This included what it really meant, what its true purpose was, how things were going to change, and how support programs such as MHI's visiting program fit within the new requirements. The simple fact of the matter was that there were too many unanswered questions existing for medical providers and others like MHI.

These unanswered questions were compounded by the fact that there were a slew of other questions that if asked in a room of 15 people would generate 15 different answers. A few of these types of questions still exist today, and probably will continue to exists until some type of case law is established to answer them.

This last statement is what scares hospital administrators the most. They do not want to be the defendants in these cases that will ultimately decide how to interpret HIPAA "correctly". Therefore, you get hospitals treating MHI, and other programs, different ways under the same set of circumstances. The overwhelming fear originally was that a large number of hospitals were going to take the "easy road out" and simply not allow MHI visiting programs within their facilities.

It will be some time before anyone truly knows how to read and interpret HIPAA in the way that it was intended, or will ultimately be viewed as "intended". Until such a time comes, MHI must be vigilant in ensuring that we are doing everything within our power to:

1) Stay abreast of current interpretations of the regulations
2) Continue to educate hospital administrators, and patients, on the benefits that programs such as MHI's visiting program can bring to patients
3) Continue to work with hospital administrators to ensure they are willing to allow MHI inside their medical facilities
4) Ensure that MHI is not used as one of the defendants in the inevitable court cases that are to come in regards to HIPAA.

CIVIL PENALTIES FOR VIOLATION OF HIPAA

Just as a note of caution…the civil penalties for violating HIPAA are $100 per violation with a maximum of $25,000 per year for multiple violations. As a MHI accredited visitor, you can be held personally liable.

What Can MHI Do To Limit HIPPA's Effects on the Visiting Program?

Grasp the subject,
the words will follow.

– Cato the Elder

There are several steps that local MHI visitation programs can implement on both a short term and long term basis to limit the effects that HIPAA has on them.

Continuous Steps

- Meet with hospital administrators on a regular basis to share information about:
  - Any concerns you may have
  - Any concerns the hospital may have
  - New policies that the hospital is thinking about implementing
  - Inform them of any new programs or ways to involve the hospital in the visiting process to further advance the advantages your program offers to the hospital
- Ensure key contacts within the hospital *(cardiac surgeons, cardiologists who operate within the hospital, cardiac ward nurses, etc.)* are kept abreast of what your MHI visitation program is doing. Provide these key individuals, or groups, with:
  - Number of visits you have performed year-to-date *(either MHI year-to-date or calendar)*
  - Copies of your newsletter
  - Copies of ***HEARTBEAT***
  - A sample of a PATH Pack
  - Any upcoming meeting information *(for example: date, location and speaker)*
- Ensure that the hospital, and patients, understand what data your MHI visiting program is collecting and why. Ensure that they understand we are only asking for minimal necessary information. This includes only a basic count of visits and a mailing address, if provided by the patient, to send them a newsletter for a period of three months. If the patient chooses to join, you will then add them to your distribution lists. If they choose not to join, you will destroy their mailing address.

If Problems Occur

- Offer to have your accredited visitors join the hospitals volunteer program, or at least attend the hospitals HIPAA training program. Many hospitals will allow their own trained volunteers access to information that they are uncomfortable offering volunteers of another program.
- If necessary, **and *only* if necessary**, offer to sign into a Business Associate Agreement (BAA) with the medical facility, or to provide MHI Consent Forms for visiting to patients.

How Can National Help?

Know how to ask.
There is nothing more difficult for some people,
nor for others, easier.

– Baltasar Bracian

There are a number of ways in which the national leadership *(elected, appointed and paid staff)* can assist MHI visiting programs in regards to HIPAA compliance.

1. The first of which is this packet, and previous publications that were designed in regards to HIPAA. By educating your MHI visiting program on HIPAA, its regulations, how it affects the visiting process and how to combat these effects, your MHI visitation program will be armed with the information necessary to continue providing the gift of hope to heart patients, their families and caregivers for the next fifty years.

2. Secondly, is by providing written documentation, like that in the appendices of this packet, to hospital administrators and MHI visiting program leaders to demonstrate how our program fits within HIPAA.

3. The national office is very familiar with the process of reviewing, and writing if necessary, Business Associate Agreements (BAA), confidentiality statements and consent forms. If any of these three items becomes necessary to continue visiting patients within a medical facility, the national office can work with your MHI visiting program to ensure that there is minimal downtime in the visiting of patients.

4. The final option is by personally working with, including visiting face-to-face, hospital administrators to keep, or create, visiting programs within their facilities. Please contact your Assistant Regional Director, Regional Director or Field Services Director for assistance with anything related to HIPAA and your MHI visitation program.

It is important to note that just because a hospital administrator may seem to be hesitant to continue, renew or create a relationship with your MHI visiting program does not mean that he/she does not view the process as a step in the healthy recovery from a heart event. HIPAA, and the legal world in which we currently live in, has made hospital administrators a little more "careful" than before.

And, as you know, "careful" in the medical arena is equivalent to "bureaucratic" in any other.

Visiting in the HIPAA World

Appendices

This information was originally presented at the
2005 MHI National Conference in Charleston, South Carolina.
The presentation was made by Chapter 38 volunteer
Alberta Rogers and MHI Field Services Director
Lawrence W. Hood, Jr., on September 3rd and 4th, 2005.

HIPPA Glossary

The terms listed within these pages are not an all inclusive list of terminology in regards to HIPAA and all that it entails. Instead, it is a listing of terms most related to The Mended Hearts, Inc., visitation program.

Accounting – A list of disclosures for other than treatment, payment or healthcare operations.

Authorization – A detailed, customized document executed by the member that gives permission to use PHI or IIHI for a specific purpose, for a specified period of time or event.

Business Associate – An individual or entity which has a contract to perform a function or activity for a covered entity involving the use or disclosure of PHI or IIHI.

Compound Authorization – An authorization for use or disclosure of PHI that is combined with another document. For the purposes of MHI, this type of authorization is only allowable when the authorization was created for research that includes treatment of the individual.

Covered Entity – A health plan, healthcare clearinghouse or healthcare provider who transmits any health information in electronic form with a HIPAA transaction.

De-Identification – Health information for which there is no reasonable basis to believe that the information can be used to identify an individual.

Department of Health and Human Services (HHS) – Federal agency responsible for implementing HIPAA.

Designated Record Set – A group of records maintained by a medical facility that is the enrollment, payment, claims adjudication, and case or medical management record systems used to make a payment or medical decision about a patient.

Designated Representative – A relative or close personal friend that the member names as someone who is directly involved in their health care and the member allows to have PHI and IIHI disclosed to them.

Disclosure – The release, transfer, provision of access to, or divulging of PHI or IIHI in any other manner, electronic, verbal or in writing, to an individual, agency or organization outside of the covered entity.

Electronically Maintained – Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted – Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and "faxback" systems. It does not include

"paper-to-paper" faxes, person-to-person telephone calls, video teleconferencing or messages left on voice-mail.

Emancipated Minor – A child who has not reached full legal age, but under applicable law, has been legally designated to be either temporarily or permanently independent from parental control.

Individually Identifiable Health Information (IIHI) – Information, including demographic information, that relates to past, present or future physical or mental health or condition of a member and can be used to identify the member.

In Loco Parentis – A person legally designated to undertake temporary care and control of another in the absence of their supervision by natural parents.

Marketing – A communication about a product or service, the purpose of which is to encourage recipients of the communication to purchase or use the product or service.

Minimum Necessary – The principle that PHI and IIHI should only be used and disclosed to the extent needed and is practical to support the purpose of the disclosure. *(NOTE: For MHI, this means do not ask or look for more PHI or IIHI than you need to do a visit.)*

Notice of Information – A document defining the uses and disclosures of PHI/IIHI and how individuals can have access to this information.

Office of Civil Rights (OCR) - The HHS entity responsible for enforcing HIPAA privacy rules.

Personal Representative – A person legally designated to make decisions through execution of an Authorization Form, Power of Attorney and/or Durable Power of Attorney.

Physical Safeguards – Mechanisms put into place to ensure the safety of PHI.

Privacy – The right of an individual to keep his/her individual health information from being disclosed.

Privacy-Related Complaint – Any verbal or written expression of dissatisfaction about the handling of PHI/IIHI.

Protected Health Information (PHI) – Individually identifiable health information that has been maintained or transmitted in any form.

Public Health Authority – An agency or organization authorized by law to collect or receive PHI for the purpose of preventing or controlling disease, injury or disability. This includes, but is not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, investigations, interventions and disaster relief efforts to the extent information is required to deal with an emergency.

Reasonable Reliance – Making reasonable efforts to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose of the request.

Record – Any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by a covered entity.

Research – A systematic investigation, including development, testing and evaluation, designed to develop or contribute to generalized knowledge.

Sensitive Medical Information – Information or documentation of any diagnosis, sign or symptom of a medical condition of an individual. Care must be made to ensure that all communications with sensitive medical information, specific to a patient, will be protected and processed confidentially.

TPO – Treatment, payment and health care operations.-

Trading Partner – An individual, organization, or vendor who conducts transactions with or for the a covered entity through the exchange of electronic or hard copied PHI or IIHI utilizing HIPAA standard transaction file format.

Treatment – Arranging for the provision of, coordinating or managing the health care of patients or potential patients.

Use – How covered entities share, employ, utilize and examine PHI or IIHI within their facility.

Frequently Asked Questions/Common Situations
- Hospitals -

- -

Question: *We have a visiting program by a Mended Hearts chapter that is not in compliance with our HIPAA - Privacy Standards. We discovered this when our Privacy Officer reviewed the visiting practices. How do we maintain the visiting program?*

To maintain the visiting program, the visitors have three options:

1. Mended Hearts visitors can become volunteers of the hospital. As volunteers of the hospital system, many hospitals have viewed the visitors as part of the health care entity and/or the care coordination process. Therefore, a consent form is not required and the volunteer visitors are privy to limited patient information.

2. Contact the Field Services Director at the Mended Hearts National Office to discuss additional measures that can be implemented to maintain the chapter's visiting program. An example is the recent recommendation offered by the Office of Civil Rights, which is a government entity charged with guiding healthcare entities on HIPAA. The Office of Civil Rights suggests that providers, such as Mended Hearts, sign an agreement with the hospital allowing the hospital the right to provide patient information to Mended Hearts visitors. The agreement is called a Business Associate Contract.

3. The visitors can offer the consent form to the hospitals so that it may be offered to patients (at admission or discharge). ***For reasons noted earlier, we do not recommend implementing the consent form method unless it is mandated by the health care entities.***

Question: *Can covered entities provide medical information to a third-party for the purpose of marketing?*

No…this is very type of thing that HIPAA was designed to prevent. Additionally, this is the reason many medical facilities feel that MHI visiting programs are not allowed under HIPAA.

Covered entities can provide contact information to a third-party for the purposes of helping the covered entity communicate with a patient about his/her benefits. However, this must be constructed and/or mailed in a secure manner to ensure privacy. This is where the Business Associate Agreement comes into effect.

Frequently Asked Questions/Common Situations
- MHI Visitation Programs -

- -

Question 1: *We have a wing dedicated to heart patients. Do we need to collect a patient's name and room number?*

No, the National office has no need for you to collect this data. However, for visitors in healthcare entities that do not have that accommodation, you will need to work with your healthcare liaison on how to be directed to patients who would desire a peer visit.

Question 2: *We send newsletters and conduct phone follow up visits. How are we supposed to obtain patient information?*

If your healthcare entity provides you with patients' personal information, you still need to ask the patients if they would like to receive a newsletter or phone follow-up visits. If the healthcare entity offers you more information than name, address and phone number, those records should be shredded on a regular basis.

If the healthcare entity does not provide you with patients' personal information, during your visit with the patients and/or family members, you can ask for verbal consent. If the person provides this information to you, you have to be very clear as to how you will use that information. An example, "We will mail you our newsletter for three months and then your personal information will be destroyed."

Whether or not the healthcare entity offers you the patients' personal information, National recommends that you maintain minimal information such as name, address and phone number for a limited time period (average of 3 months). No health conditions should be written down.

Question 3: *Our visiting program has been discontinued at the hospital. As a result, our chapter is not gaining new members and current members are losing interest due to their inability to visit heart patients. What can we do to attract new members? And, is there any way we can offer a visiting program?*

Network with cardiologists or hospitals to set up displays consisting of brochures, posters and ***HEARTBEAT*** magazines about Mended Hearts services. One chapter convinced their hospital to display PATH Paks as an FYI to heart patients at their hospital. The National Office has designed posters that can be used to increase public awareness and establish community interest at your local level.

If there is a cardiac rehabilitation center in your area, consider approaching them to offer a visiting program and support group meetings. While the visits at the cardiac rehabilitation center

will differ from the visits at the hospitals, many patients are now able to focus on the recovery process and obtain much needed support.

Another option is to develop a satellite at a different hospital. Mended Hearts can then work with that hospital to offer a visiting program.

Question 4: *My hospital liaison told me that Mended Hearts visitors are a part of the patient care process and as a result, we have access to patient information and do not need National's consent form. Is this true?*

Each hospital will view and implement HIPAA Privacy Standards differently. If your hospital is allowing you to access patient information, you need to follow their policies. ***National recommends that you do not maintain records of patients' names and health conditions***. Any records that you are given with the patients' name and health conditions should be shredded on an average of 3 months.

It is still beneficial to educate the visitors about HIPAA Privacy Standards and to implement a "check" system to ensure adherence to the policies.

Question 5: *As a visitor, I can't make an intelligent visit without knowing the patient's health conditions. How am I to visit?*

With HIPAA, hospitals/health care entities may not release the patients' health information.

However, a successful visit does not require knowledge of the patients' health conditions. The basic premise of a visit includes the visitor telling the patients and/or family members the following:

1. Who you are and that you are with Mended Hearts.
2. Why you are there.
3. Inform them you are a recovering heart patient.
4. Then, it is time for you to listen to the patients and/or family members.

Depending on the comfort level of the patients or family members, they may share their concerns with you.

MHI Sample Business Associate Agreement

- -

This Business Associate Agreement dated to be effective this, the _____ day of _____, 200__ ("Effective Date") is entered into by and between _____ ("Health Facility") located _____and the _____ chapter of The MendedHearts, Inc. ("MHC" and/or "Mended Heart Chapter") ("BA" and/or "Business Associate"), located at_____.

Recitals

WHEREAS, Health Facility is a hospital engaged in providing health care services in _____ (city, state); and,

WHEREAS, in order to effectively carry out its operations, it is necessary for Health Facility to contract with entities who provide, at a local chapter level; and,

WHEREAS, the _____ BA is an independent local chapter of The Mended Heart, Inc, a not-for-profit organization located at 7272 Greenville Avenue, Dallas, Texas 75231-4596; and,

WHEREAS, BA offers emotional support to open heart surgery patients ("Patients") during hospitalization; and,

WHEREAS, BA is desirous of offering emotional support to Health Facility Patients during hospitalization at Health Facility; and

WHEREAS, Health Facility recognizes the value to open heart patients of emotional support during hospitalization; and,

WHEREAS, Health Facility has engaged BA to carry out such identified services, which include the use and disclosure of Protected Health Information ("PHI");

WHEREAS, the disclosure of certain individually identifiable health information will be regulated by the Health Insurance and Portability Act of 1996 ("HIPAA"), as amended from time to time, and the regulations promulgated thereunder; and,

WHEREAS, Hospital Facility may from time to time disclose to BA certain protected health information that is subject to protection under HIPAA; and,

WHEREAS, Health Facility and BA desire that their Business Associate of Agreement complies with the applicable provisions of HIPAA and the Privacy Rule, including, but not limited to Title 45, Sections 160 and 164 of the Code of Federal Regulations ("CFR").

Agreement

NOW THEREFORE, in consideration of the mutual promises and covenants contained herein and in order to assure compliance with 45 C.F.R. Parts 160 and 164 on patient privacy and confidentiality, the parties mutually agree as follows:

DEFINITIONS

A. "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. §164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502 (g).

B. "Privacy Rule" shall mean the Standards of Privacy for Individually Identifiable Health Information at 45 CFR parts 160 and 164, Subparts A and E. Additionally, any references herein to the Privacy Rule mean the section as in effect or as amended, and for which compliance is required.

C. "Protected Health Information," ("PHI") as defined by 45 C.F.R. §164.501, and as may be periodically revised or amended by the United States Department of Health and Human Services, the U.S. Congress or other federal agency, means information that is received from, or created or received on behalf of, Health Facility and is information about an individual which relates to the past, present or future physical or mental heath or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health caret to an individual. PHI also either identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. Protected Health Information pertains to both living and deceased individuals.

D. "Required by Law" shall have the same meaning as the "required by laws' in 45 CFR §164.501.

E. "Secretary" shall mean the Secretary of the Department of Health and Human Services ("HHS") and any other officer or employee of HHS to whom the authority involved has been delegated.

GENERAL

BA shall take all necessary actions consistent with HIPAA's requirements to safeguard the PHI that Health Facility discloses to BA in connection with BA's services provided under this Business Associate of Agreement. BA may not use or further disclose PHI in a manner that would violate HIPAA's requirements if done by the Health Facility.

PERMITTED USES AND DISCLOSURES

BA is permitted to use and disclose PHI from the Health Facility in Mended Heart's Visiting Program.

I. DUTIES AND OBLIGATIONS OF BUSINESS ASSOCIATE

A. BA shall not use or further disclose the information other than as permitted or required by Business Associate of Agreement or as required by law.

B. BA shall use appropriate safeguards to prevent use or disclosure of PHI disclosed by Health Facility other than s provided for by this Business Associate of Agreement.

C. BA shall provide The Mended Heart visiting program.

D. BA and its volunteers, employees and agents shall be considered invitees of the Health Facility, and at all times be subject to and required to comply with all of the Health Facility policies, rules, regulations and procedures regarding Patient information. Health Facility, BA and The Mended Heart, Inc, each shall continue their respective independent corporate existence and shall continue their business and affairs under the control of their respective officers and directors. Neither Health Facility or BA shall, by virtue of this Business Associate of Agreement be construed as an agent or representative of the other, neither party shall represent itself as an agent of the other.

E. BA shall have appropriate procedures in place for mitigating, to the extent practicable, any deleterious effect from the use or disclosure of PHI in a manner contrary to this Business Associate of Agreement or the Privacy Regulations.

F. As soon as reasonably practical, BA shall report to Health Facility any use or disclosure of the information not provided by this Business Associate of Agreement of which BA becomes aware.

G. BA shall make available PHI in accordance with rules regarding access of individuals to information under HIPAA.

H. BA shall ensure any MHC affiliate or agent to whom MHC provides PHI because of the services provided under this Business Associate of Agreement or created/received as a result of the relationship between BA and Health Facility will agree to the same restrictions and conditions that apply to BA with respect to PHI.

I. BA shall make available PHI for amendment and incorporate any amendments to PHI in accordance with HIPAA.

J. BA shall make available the information required to provide an accounting for disclosure in accordance with HIPAA.

K. BA shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created/received by BA on behalf of Health Facility to Department of Health and Human Services ("HHS") Secretary for the purpose of determining Health Facility's compliance with HIPAA. BA shall immediately notify Health Facility upon receipt or notice of any request by the HHS Secretary to conduct an investigation with respect to PHI received from Health Facility.

USES AND DISCLOSURES FOR THE PROPER MANAGEMENT OR LEGAL RESPONSIBILITIES OF BUSINESS ASSOCIATE

BA may, if necessary, use and disclose PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA. However, in order to disclose PHI:

A. The disclosure must be required by law; or

B. BA must obtain reasonable assurances from person or entity to whom the PHI is disclose the requirement by law or for the purpose for which it was disclosed to the person or entity; and

C. The person requesting such disclosure must notify BA of any instance of which it is aware in which the confidentiality of the PHI or information being disclosed has been breached.

II. DUTIES OF HEALTH FACILITY

A. Health Facility engages BA to provide The Mended Heart visiting program service. Health Facility grants BA permission to use the PHI from the Health Facility in the carrying out of the Mended Heart Visiting Program.

B. The Health Facility shall notify BA of any changes in, or revocation of permission by Patient of Health Facility to use or disclose PHI to the extent that such change will affect BA's use or disclosure of PHI.

C. The Health Facility shall notify BA of any restriction to the use or disclosure of PHI that the Health Facility has agreed to, to the extent that such restriction may affect the BA's use or disclosure of PHI.

RIGHT TO AUDIT

Health Facility and its representatives shall be entitled, within ten (10) business days prior written notice to BA, to audit BA from time to time to verify BA's compliance with the terms of this Business Associate of Agreement. Health Facility shall be entitled and enabled to inspect the records and other information relevant to BA's compliance with the terms of this Business Associate of Agreement. The Health Facility shall conduct its review during normal business hour of BA, as the case may be, and to the extent feasible without unreasonably interfering with such normal operations of BA.

III. TERMINATION AND PHI

Either party to this Business Associate of Agreement may terminate this Business Associate upon thirty-day (30) day written notice to the other Party of intent to terminate.

In addition, Health Facility may immediately terminate this Business Associate of Agreement if Health Facility determines BA has violated a material term of this Agreement and has failed to provide

satisfactory assurances to Health Facility within ten (10) days of notice by Health Facility to BA of such material violation that the violation has been cured and steps taken to prevent the recurrence, or, conversely, if Health Facility determines that continuation of this Agreement would pose a threat to the health, safety, privacy or welfare of its patients, staff or visitors.

At termination of this Business Associate of Agreement, BA shall return or destroy all PHI received from or created by BA on behalf of the Health Facility that BA still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, BA must continue to protect PHI in accordance with this Agreement and limit further uses and disclosure to those purposes that make the return or destruction of the information feasible. This provision shall apply to PHI that is in the possession of agents, related parties or subcontractors of BA.

FURTHER ASSURANCES

In order to ensure that this Business Associate of Agreement is consistent with HIPAA, BA agrees that this Business Associate of Agreement may be modified from time to time upon written notice from Health Facility to BA as to the revisions required, to make this Agreement consistent with HIPAA.

Nothing expressed or implied in this Business Associate of Agreement is intended to confer, nor shall anything herein confer, upon any person other than BA and Health Facility and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

Both BA and Health Facility agree that the individual's names appearing below have the both the legal capacity and authority to enter into a binding contract on behalf of the entities they represent.

SURVIVAL, ASSIGNMENT AND WAIVER OF BREACH

The provisions of this Business Associate of Agreement shall survive termination of the Business Associate of Agreement between Health Facility and BA.

This Business Associate Agreement may not be assigned by either party without the prior written consent of the other party. Except for the prohibition of assignment contained in the preceding sentence, this Business Associate Agreement shall be binding upon and inure to the benefits of the heirs, successors and assigns of the parties hereto.

The waiver of breach or a violation of this Business Associate Agreement shall not operate as, or be construed to be, a waiver of any subsequent breach of same or other provision hereof. No waiver shall be effective against any party hereto unless in writing and signed by that party.

In the event that any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall have no effect on any other provisions, and the Agreement shall be construed as if such invalid, illegal, or unenforceable provision had never been contained in it.

LIABILITY AND INDEMNIFICATION

Neither party of this Agreement shall be liable to the other party, or to anyone who may claim any right due to its relationship with the parties of this Agreement, for any acts or omissions on the part of BA or Health Facility, or their respective officers, governors, directors, trustees, agents or employees,

consultants, thereof, in the performance of the services provided and received under this Agreement, except when such acts or omissions are due to willful misconduct or gross negligence.

Parties mutually agree that in the event a party to this Business Associate Agreement is found to be in violation of 45 C.F.R. Parts 160 and/or 164 arising from an alleged use or disclosure of PHI by a party of this Business Associate Agreement, or its agents or subcontractors, the violating party agrees to indemnify, defend and hold harmless the other party and their respective officers, governors, trustees, agents, employees, or consultants, from any alleged claim or penalty against the other party arising from any allegation of uses or disclosure of PHI in violation of 45 C.F.R. Parts 160 and/or 164.

GOVERNING LAW

This Business Associate of Agreement has been executed in, and shall be governed by and interpreted in accordance with, the laws of the state in which the Health Facility is domiciled. Any controversy or claim arising from or related to this Business Associate of Agreement shall be brought in the courts in the state in which the Health Facility is domiciled.

NOTICES

All notices, demands, approvals, and other communications required or permitted by this Business Associate of Agreement shall be in writing and sent by certified mail or by personal delivery. Such notices shall be deemed given on any date of delivery by the United States Postal Service. Any notice shall be sent to the following addresses:

If to Health Facility:

_____
Name and Title

_____
Street Address

_____
City, State Zip Code

If to BA:

The Mended Heart, Inc., Local Chapter # _____

_____
Street Address

_____
City, State Zip Code

EXECUTION AND AUTHORIZED AGREEMENT

This Agreement may be executed in multiple counterparts, each of which will be fully enforceable as an original. A facsimile will also be fully enforceable as if an original. The undersigned, an officer of the Company, has been duly authorized to execute and deliver this Agreement, and all other instruments executed and delivered on behalf of the Company relating to this Agreement; and the signature of the undersigned is binding upon the Company.

IN WITNESS WHEREOF, each of the undersigned has caused this Business Associate of Agreement to be duly executed in its name on its behalf to be effective, on the day and year first above written.

HEALTH FACILITY: _____

Signature _____

Date _____

THE MENDED HEART, INC. LOCAL CHAPTER #_____

Signature_____

Date _____

MHI Sample Consent Form

- -

Who We Are
Mended Hearts is a national nonprofit organization with a 50-year history of offering support, encouragement and hope to heart patients, their families and caregivers during hospital visits and through support group meetings.

Our Mission
To inspire hope in heart disease patients and their families.

Our Members
We are like the very people we serve – heart patients and families – sharing our experiences as we offer hope. Healthcare professionals also join our mission by providing their expertise and support.

Our Method
We partner with hospitals and rehabilitation clinics across the nation to help those affected with heart disease to have a positive patient-care experience.

Visiting Service
Mended Hearts visitors serve heart patients by being there to listen, share their experiences and offer encouragement to concerns.

I have read, understand and agree to have a Mended Hearts visitor contact me.

Participant's Signature: _____

Printed Name: _____

Date: _____

The Mended Hearts, Inc., honors patient confidentiality requirements. We recognize your medical information is confidential and protected by law. The Mended Hearts, Inc., does not maintain a national patient database. Your name will not be given or distributed to any other organization.

MHI Sample Confidentiality Statement

- -

The Mended Hearts, Inc., honors patient confidentiality requirements. We recognize patient medical information is confidential and protected by law.

The Mended Hearts, Inc.'s, National Office does not maintain a patient database. Local chapters, with the consent of the patient, are allowed to keep the patient's name, address and telephone number for the purpose of follow-up visits and/or newsletter mailing for a period of three months. Exchange of visiting information between chapter members or officers is to be conducted in a confidential setting.

Maintenance of patient health information or records is not allowed. The patient's name, address or telephone number is not to be distributed to any other organization.

I have read, understand and agree to the terms of this Agreement.

Participant's Signature: _____

Printed Name: _____

Date: _____

Chapter Number & Name: _____

MHI Message to Healthcare Entities

(Originally Written and Distributed in December 2002)

- -

The Mended Hearts, Inc.

Healthcare Entities and the Mended Hearts Visiting Programs in Relation to the HIPAA – Privacy Standards

GENERAL UNDERSTANDING

We realize that each health care entity will have its own set of policies with regard to HIPAA and will have varying interpretations of HIPAA itself. Therefore, we are advising each local Mended Hearts chapter to work with their healthcare liaison, including, where applicable, a privacy officer, to ensure that policies are being followed.

MENDED HEARTS NATIONAL GUIDELINES FOR CHAPTERS REGARDING HIPAA – PRIVACY STANDARDS

We are advising our chapters to be active in learning and adhering to their healthcare entity's policies regarding the HIPAA - Privacy Standards. Local Chapter Presidents or Visiting Chair Persons should conduct the following:

* Ask to meet with the health care entity privacy officer or liaison to discuss the healthcare entity's HIPAA policies as they relate to Mended Hearts.
* Become familiar with the health care entity's policies and follow the rules.
* Inform the healthcare entity that the data being maintained are minimal and do not conflict with the Privacy Standards. (Please review the Mended Hearts National Office Data Requirement of the Visiting Program below. Mended Hearts does not have and has never maintained a national database of patient names or conditions.)
* Advocate that Mended Hearts volunteers join the health care entity volunteer organization, if applicable.

NATIONAL OFFICE DATA REQUIREMENTS

The only information that is maintained by the Mended Hearts National Office is the following:

* The number of visits chapter members make (how many visits were made during a day, month or year)
* Whether the visit was made to a patient or to a family member
* Type of visit (face-to-face, phone, or internet)

CONSENT FORM

A few health care entities are requiring Mended Hearts visiting programs to provide them with a consent form, which the hospital can present to the patient on Mended Hearts behalf. The Mended Hearts National office has developed the visiting consent form for your use. Please see the attachment.

However, we do not advocate implementing the consent form method unless it is deemed absolutely necessary. Visiting programs that are now operating under the health care entity mandated consent form method have observed a significant decrease in patients being visited. Thus, less heart patients are benefiting from the needed peer support that can assist in increasing patient self-efficacy and improving the overall quality of life.

HIPAA PRIVACY TRAINING FOR VISITORS

Our goal is to have a successful partnership with you to help heart patients deal with the emotional aspects of recovery. The following procedures have been initiated:

* The National office will incorporate training for the HIPAA - Privacy Standards as part of its overall accredited visitor-training program.
* All currently accredited visitors must participate in the HIPAA privacy-training portion.
* Visitors are required to sign the Mended Hearts confidentiality form.
* Each visiting program has been informed to adhere to the healthcare entity policies and that patient confidentiality is to be maintained.
* We have also recommended that the chapters develop a "check" system to ensure that visitors are adhering to the HIPAA - Privacy Standard and take appropriate measures against volunteers who fail to comply.

RESPONSE TO PRIVACY INFRACTIONS

We understand that as the health care entity, you have the right to relinquish a volunteer from the visiting program or even close the entire visiting program for violations to the privacy standards as determined by your system.