Buena Vista
REGIONAL MEDICAL CENTER

HIPAA Privacy and Security

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act of 1996, known as HIPAA, is an important federal law dealing with various issues, including the privacy and security of health information. Complying with HIPAA is very important to us. There are fines and even criminal penalties if we do not take reasonable steps to comply.

HIPAA applies to our employees, contract staff, students, medical staff and volunteers. Under HIPAA, you are called our "workforce" and you play the key role! If our workforce is out of compliance, so is BVRMC.

WHAT IS PRIVACY?

Privacy refers to our duty to prevent others from seeing or using "protected health information" about our patients. Under HIPAA, we can only use and disclose protected health information for certain permitted purposes. If we use or disclose the information for any other purpose, we may have violated the law.

As a member of our workforce, this means that you should not see or obtain protected health information unless it is part of your job. You should not disclose protected health information to anyone else, unless that is part of your job. BVRMC has policies and safeguards to help you understand these rules and to limit your access to information you do not need.

HOW PRIVACY WORKS

What is protected health information?

Protected health information is any information about past, present or future physical or mental health, health care or payment for healthcare that identifies a patient. These examples help to show how much information is covered under HIPAA:

- The contents of a medical record or patient billing record are protected health information.
- The fact that a patient is scheduled for a procedure or visit on a certain date is protected health information.
- The fact that a person has been a patient of BVRMC is protected health information.
- The fact that a patient has a particular health insurance policy is protected health information.
- Information in our records that identifies the patient, like name, address and social security number, is protected health information.

What form of information is covered by HIPAA?

HIPAA applies to protected health information about patients. It does not matter what form it is in. Thus, HIPAA privacy rules apply if the information is in written, video, electronic or even oral form. Some examples are:

- A medication vial identifying a patient contains protected health information on the label and must be handled and disposed of properly.
- A calendar, scheduling patients by name, contains protected health information and is covered by HIPAA. It should be kept where only people who need the information can see and use it. This applies even if it is electronic and on a computer screen.
- A nurse's conversation with a patient after surgery includes protected health information. If visitors are present, the nurse needs to make sure it is okay with the patient to talk in their presence.

A conversation between a nurse and a lab technician ordering lab tests is covered by HIPAA. Both parties should try to avoid being overheard.

Treatment, payment and health care operations

HIPAA itself provides the authority to use and disclose protected health information for *treatment, payment and health care operations*. These are 3 very broad categories. They cover most of our uses and disclosures at BVRMC.

- Members of the dietary staff will be able to look at special dietary orders as part of treatment. BVRMC can send protected health information to a nursing facility when a patient is transferred. Nursing staff can

fax patient lab results to the treating physician. These are all permitted uses and disclosures for treatment.

- Admitting and billing staff will be able to look at employment, insurance and payment information to admit patients or bill for services. Billing staff will be able to send bills to insurance companies, even though the bills include protected health information. These are uses and disclosures for "payment" purposes.
- Hospital personnel, members of the medical staff, and consultants we hire will be able to look at patient records to perform quality improvement functions. Hospital staff will be able to review protected health information to check for compliance with Medicare rules. These are uses and disclosures for BVRMC's operation.

The key in all of these broad categories is making certain your job at BVRMC allows **you** to engage in the activity.

Minimum necessary

Under HIPAA, members of the workforce can only obtain, use and disclose the ***minimum necessary*** information to do a job or handle a request. This means the *least* information (both types of information and amount) needed for the task. This is the "need to know" rule we have always followed. The rule is the law, backed up by real penalties.

It is important to know that this rule ***does not*** *apply* when we use or disclose protected health information to *treat the patient*! It also does not apply when we disclose information to the patient or at the patient's request.

Incidental disclosures

Incidental disclosure refers to an unintended or unavoidable disclosure of protected health information that occurs as a part of a permitted disclosure. For example, if the physician speaks to the patient at bedside with the patient's okay and visitors overhear the conversation, it is an incidental disclosure. Incidental disclosures are permitted, but we should always look for ways to limit or avoid them.

Authority

Under HIPAA, every use and disclosure of protected health information must be tied to some type of *authority*. Authority can come from the patient – for example, when the patient authorizes sending information to a third party or says you can speak in front of visitors.

Authority can also come from State or federal law, including HIPAA. For example, State law requires reporting child abuse. HIPAA then permits us to make reports required by law.

The key in all of these broad categories is making certain your job at BVRMC allows **you** to engage in the activity.

Quality of care

HIPAA should not interfere with the quality of patient care. Any member of our workforce who believes that our HIPAA policies and safeguards are interfering with timely, high-quality care should report the concern to a supervisor.

WHAT IS SECURITY?

Security refers to our duty to keep health information secure and available. Security also refers to steps BVRMC takes to make sure protected health information stays private. Information Systems (IS) will ensure the confidentiality, integrity and availability of information assets by adherence to the established policies and procedures based on the following principles:

- Access to information systems will be granted to authorized users based on need-to-know to perform job responsibilities.
- Access to information systems is controlled through User ID's and passwords.
- Individually assigned User IDs are required to access all confidential information.
- User IDs and passwords cannot be shared.
- Users must immediately notify management of potentially or actual inappropriate access of systems.
- Users are responsible and accountable for all activity preformed with their Unique User ID.
- Users cannot change their IDs. Passwords will be changed every 180 days.
- Access to Information Systems will be revoked upon termination of employment or business contract.
- Users should logout of the system prior to leaving a workstation unattended.
- Access to confidential systems will be logged and audited.

- An automatic logoff after a predefined period of inactivity will be enforced on all confidential systems, where possible.
- All users must log off at the close of business each day (where applicable).
- Passwords should not be written down and stored in locations where another person might discover them (i.e. stuck to monitor, under keyboard, or desk drawer). If Passwords need to be written down to be remembered, they should be stored in a secure location (i.e. purse or wallet).
- If software needs to be installed on your PC, always contact the IS Help Desk.
- All confidential data stored on removable disks, writeable CD ROMs and DVD's should be sent to the IS department for disposal.

Privacy and security go hand-in-hand. For example, our *privacy* policies prohibit members of our workforce from obtaining protected health information unless they need it to do their job. Our *security* safeguards will limit who has a key to the records room or who can log on and view patient information.

HOW HIPAA AFFECTS BVRMC

BVRMC is a health care provider. HIPAA regulates how health care providers like BVRMC use and disclose protected health information.

Our commitment

Understanding the importance of HIPAA, the BVRMC Compliance Committee and BVRMC have adopted policies firmly committing BVRMC to comply with HIPAA. These policies apply to management, employees, volunteers and temporary employees even students, residents who train at BVRMC. The Board and administration will hold everyone responsible to do their part.

Our compliance steps

Here are some of the steps BVRMC has taken to back up its commitment:

- We have adopted a ***Compliance Plan***. The Compliance Plan is made up of ***policies*** that explain the rules for using and disclosing protected health information. Members of our workforce need to know which policies apply to them, and how.
- We have prepared a ***Notice of Privacy Practices.*** This is a key document and is required by HIPAA. It tells our patients how we will use, disclose and handle their protected health information. It also applies to our workforce, since we are required by law to follow the practices we describe in the Notice.
- We have identified our biggest ***risks***. Under HIPAA, we are required to look for problem areas so we know what policies and safeguards we need. You can help here too. If you think we have missed something and it poses a risk to privacy or security, you should tell your supervisor.
- We have adopted ***safeguards*** – things like unique passwords to access our electronic records and locks on doors to sensitive areas. These are steps we have taken to deal with the risks we have found.
- We have ***classified*** members of our workforce by the amount and type of protected health information you need to do your job.

Are there penalties?

BVRMC hopes its compliance steps will be very effective.

- BVRMC faces potential fines for each violation of the HIPAA privacy (and security) safeguards. These can grow to millions of dollars for a single violation.
- The individual also faces possible civil and criminal penalties. For example, if a covered entity intentionally obtains protected health information about a patient by using a false identity, the offense could bring a criminal fine of up to $100,000 and 5 years in jail.
- Maybe worst of all, *we risk losing the trust of our patients*. This is why BVRMC has made a full commitment to compliance with HIPAA and will count on you to do your part.
- Violations may result in disciplinary action, up to and including termination.

BVRMC'S COMPLIANCE PLAN

Here are the key features of our Compliance Plan you should know.

Privacy Officer, Security Officer, Compliance Officer

BVRMC has appointed a "Privacy Officer," "Security Officer," and "Compliance Officer." The Privacy Officer will lead our efforts to comply with HIPAA and other privacy issues. All assigned officers will also be able to help with training and answering questions. The Privacy Officer is **DIRECTOR OF HIM (ext. 8687)**. The

Security Officer is **DIRECTOR OF INFORMATION SYSTEMS (ext. 8666)**. The Compliance Officer is **EXECUTIVE DIRECTOR OF QUALITY (ext. 8632)**. The Compliance Hotline is extension 8012. All officers will welcome questions, concerns and even complaints, because your comments will help us make our Compliance Plan stronger.

Mandatory reporting
BVRMC *requires* you to report if you have first-hand knowledge that there has been a breach of our HIPAA policies or an improper use or disclosure of protected health information. You may report to your manager. You may also report directly to the Privacy Officer, Security Officer, or the Compliance Hotline at extension 8012.

Permissive reporting
BVRMC also encourages reporting or asking questions any time you have questions or concerns about how well the Compliance Plan is working. These questions and reports can be raised with your manager or with the Privacy Officer. BVRMC needs to know what you know to be sure its compliance efforts are effective.

Protection for reporting and compliance activities
Our policies prevent BVRMC from retaliating against you in any way because you file a mandatory or permissive report. BVRMC's policies and the law also protect you from engaging in certain good faith compliance activities, such as participating in government investigations of BVRMC.

BVRMC's policies do permit disciplinary action if you do not report a known HIPAA breach.

HOW HIPAA AFFECTS YOU?

If you are wondering what role you play in BVRMC's compliance effort, just think about what protected health information you see or learn each day in your job. You see patients. You see names. Depending on your job, you may see care being rendered or actually provide it yourself. You may have access to a little information or a lot. Here is a simple summary of what we expect from you:

- Take patient privacy and security seriously. Be the "patient" and imagine what you would want people in your job to do.
- Complete all required training. We will hold you to this and we will follow your progress.
- Be familiar with the policies and procedures that apply to you.
- Ask your supervisor if you are unsure how HIPAA or BVRMC's policies apply to you.
- Do not handle protected health information that is outside your job classification.
- Only use or disclose protected health information for *permitted* purposes. Our policies describe what is permitted. Ask a manager if you have questions.
- Promptly report any first-hand knowledge you have of a violation of HIPAA or a breach of BVRMC's privacy and security policies.
- This includes reporting any improper use or disclosure of protected health information you know about.
- Tell a supervisor if you believe HIPAA or our policies and safeguards are harming patient care. HIPAA is supposed to protect privacy, not interfere with care.
- Never share a password with another person; never allow another person to access information under your identity; never access information under another person's identity; and always comply with BVRMC's access controls.
- Never retaliate or discriminate against a patient who files a complaint or exercises rights permitted by HIPAA or BVRMC's policies.
- Never retaliate against another member of the workforce who files a report, makes a complaint or exercises rights permitted by HIPAA or BVRMC's policies.
- Promptly notify a supervisor of any HIPAA-related complaint, oral or written, made by a patient or someone on behalf of a patient.
- Cooperate in surveys, assessments and investigations by BVRMC seeking information about compliance with its HIPAA Compliance Plan or HIPAA.
- BVRMC has developed policies and procedures to assist in meeting our compliance requirements. These policies are available on the BVRMC Intranet for viewing or printing.