RYTHM DEVICES INC.

HIPAA PRIVACY POLICY

I. Purpose

Provide guidance to "Rythm" regarding the release of protected health information (PHI) for purposes requiring an individual's authorization. The individual has the right to revoke the authorization at any time.

"Rythm" may not condition the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except under very limited circumstances.

II. Policy

It is the policy of "Rythm" to compliance with all federal and state regulation regarding the use and disclosure of PHI (personal health information) and to allow disclosure of patient PHI without a patient authorization only for the purposes of treatment, payment and healthcare operations or as otherwise allowed by the Privacy Regulations or under other state and federal law.

1. Authorization Not Required:

Authorizations are not required for the following uses and disclosures. All other uses and disclosures require an authorization unless other state or federal law mandates the specific use or disclosure.

- To the individual or personal representative.
- For treatment.
- For payment.
- For health care operations activities, including:
    - Fundraising (if only limited information is used/disclosed),
    - marketing (under limited situations),
    - summary health information to plan sponsor,
    - enrollment or disenrollment information to plan sponsors.
- For facility directories.
- To family members, friends, and others an individual involves in his or her health care or payment for health care.
- For emergencies and disaster relief situations.
- For public interest activities including:
    - required by law,
    - public health,
    - victims of abuse,
    - health care oversight,
    - judicial and administrative proceedings,
    - law enforcement,
    - about individuals who have been deceased for over 50 years,
    - cadaveric organ, eye, or tissue donation purposes,
    - research (under certain conditions) avert serious threat to health or safety,
    - specialized government functions,
    - workers compensation.

- For limited data set.
- To HHS for compliance and enforcement activities.

2. Authorization Required

Authorizations are required for the following uses and disclosures. Some use and disclosure purposes also have specific individual requirements. Authorizations are not to be used to circumvent prohibited uses and disclosures, such as for the sale of PHI.

- Use and disclosure of psychotherapy notes for any purpose
- For health care operations activities, including:
    - Fundraising (if more than limited information is used/disclosed),
    - marketing (under most situations when direct or indirect payment is received),
    - release to the media or public display.
- For certain activities including:
    - About individuals who have been deceased for less than 50 years,
    - research (under certain conditions, particularly when individuals directly participate).
- For any purpose not explicitly exempted from authorization.

III. Procedure

"Rythm" must obtain a valid authorization for certain uses and disclosures and has adopted specific authorization forms for use when releasing or requesting PHI for purposes that require authorizations.

For disclosures made in response to a valid authorization, "Rythm" will disclose the information to the extent specified in the authorization. When requesting PHI that requires an authorization to use/disclose, "Rythm" will request the minimum amount of information needed to meet the purpose of the request.

A. Authorizations

a. "Rythm" may use and disclose PHI when a valid authorization is obtained.

b. For requests for authorization initiated by "Rythm", all units must use a standardized authorization form, Authorization for Release of Information, which can be accessed at the following website: rythmdigital.com/hipaa. All sections must be complete. Changes or variations to the authorization forms must be approved by the Privacy Officer of "Rythm". Treatment may not be conditioned on obtaining the authorization (unless related to approved research clinical trial).

c. If the authorization was received from the individual or third party, determine the validity of the authorization. The following elements must be present:

i. A description of the specific information to be used or disclosed.

ii. Name of the specific person or entity authorized to disclose the information.

iii. Name of the specific person or entity to whom "Rythm" may make the requested use or disclosure and, if information is to be mailed, the address of the person or entity.

iv. The date, event, or condition upon which the authorization will expire.

v. The individual's signature and date.

vi. A description of the personal legal representative's authority to sign, if applicable.

vii. A description of the purpose of the disclosure. (Not required if the individual requests disclosure for own use).

viii. A statement in which the individual acknowledges that he or she has the right to revoke the authorization, instructions on how to exercise such right, or to the extent the information is included in the covered entity's notice, a reference to the notice.

ix. A statement that treatment may not be conditioned on obtaining the authorization, unless it is research related and disclosure of the information is for the particular research study. If for purposes of research, where treatment may be conditioned on obtaining the authorization, a statement about the consequences of refusing to sign the authorization.

x. A statement in which the individual acknowledges that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by federal privacy law.

xi. If the authorization is for marketing purposes and the marketing is expected to result in direct or indirect remuneration to "Rythm" from a third party, a statement of this fact.

xii. If the disclosure requested involves mental health, substance abuse, HIV/AIDs, or reproductive health information, the authorization must also include (incorporate other federal and state law provisions here):

d. An "authorization" is not considered valid if it has any of the following defects:

i. The expiration date has passed.

ii. The form has not been filled out completely.

iii. The authorization is known by "Rythm" to have been revoked

iv. The form lacks any required element.

v. The information on the form is known by "Rythm" to be false.

vi. Treatment was conditioned upon obtaining the authorization (except for research purposes).

e. If the authorization is signed by a legal representative or other person authorized to act for the individual, the request must be accompanied by documentation of the representative's legal authority to act on behalf of the individual.

f. A patient who has executed an authorization for disclosure or use of individual health information may revoke the authorization at any time by sending a written notice to "Rythm" as described in the Notice of Privacy. The written notice must refer to the specific authorization being revoked (e.g., "my authorization of January 27, 2002") and be signed and dated by the individual or his or her legal representative. The revocation becomes effective upon receipt by "Rythm", with the exception of uses or disclosures made by "Rythm" prior to receipt.

g. For research-related health information:

i. The core elements of an authorization as described below may be combined with the informed consent to participate in the research.

ii. An authorization for a research study may be combined with another authorization or other written permission for the same or another research study.

iii. “Rythm” may condition the provision of research related treatment (related to the clinical trial) on obtaining authorization.

iv. “Rythm” may use and disclose for a specific research study, PHI that is created or received before and after HIPAA's compliance date (April 14, 2003), and/or prior to the new authorizations being implemented, as long as some other express legal permission to use and disclose the information for the research study was obtained.

v. Archived information may continue to be used and disclosed for the research study if an individual had originally signed an informed consent to participate in the research study, or IRB waived informed consent, in accordance with the Common Rule or FDA's human subject protection regulations.

vi. An accounting of all disclosures made under an authorization must be documented and maintained. See “Rythm” policy, 00-01-15-20:00, Accounting of Disclosures of Health Information

B. Authorization for Release to Third Party:

If “Rythm” receives a request from a third party for release of PHI for other than treatment, payment, healthcare operations or as otherwise authorized by law or for public interest purposes exempted from authorization, the request will be routed to (specify position or department). The [specific “Rythm” authority] will review the request and determine if a specific authorization is needed.

1. The (specify position or department) will review the request and determine if specific authorization is required.

2. If specific authorization is required, the specify position or department) will contact the patient, plan member or authorized representative in a written letter explaining the nature of the request for release and send the appropriate authorization form with the letter.

3. The letter will state that if authorization is granted by an authorized personal representative, the returned authorization form needs to be accompanied by appropriate documentation validating the personal representative has the authority to represent the patient or the member.

4. If authorization is granted, the (specify position or department) will notify the third party requesting the information that authorization has been granted and will include requested information with the letter.

5. If the patient, plan member or authorized personal representative denies release, the (specify position or department) will notify the third party requesting the information that authorization has been denied by the patient, plan member or authorized personal representative. Notification will be in writing.

6. All letters and signed acknowledgement forms shall become part of the patient or plan member’s permanent record.

C. “Rythm” Request for Third Party Release of Information:

If “Rythm” requires access to third party PHI for purposes other than treatment, payment, healthcare operations, as allowed by law or for public interest purposes exempted from authorization, the workforce member will first document the need and purpose for release.

1. The appropriate authorization form will be mailed or transmitted to the third party specifying in as much detail as possible the PHI requested accompanied by a letter specifying the reason for the release of PHI.

2. The “Rythm” authorized workforce member will follow up by phone with the third party if no response has been received within two weeks from the date of the request. The phone call will be documented and become a part of the patient or plan member’s permanent record.

3. If the authorization is granted and the PHI forwarded to “Rythm” the released PHI shall only be used for the purposes documented. The authorization form received from the third party shall become part of the patient of plan member’s permanent record.

4. If the authorization is denied, the request will be forwarded to (specify position or department) for review and to decide if “Rythm” intends to contact the specific patient or plan member to directly request authorization.

5. If it is determined the PHI requested is critical, (specify position or department) will contact the patient or plan member in writing detailing the information requested and the reason for the release of PHI. The letter will be accompanied with the appropriate authorization form.

6. If authorization is granted, (specify position or department), the third party will be contacted in writing. The letter to the third party shall be accompanied by a copy of the completed authorization request.

7. If the authorization is denied, all documentation will become part of the patient or member’s permanent record and “Rythm” will be required to take appropriate action depending on the situation. This could include doing nothing, proceeding with the activity the information is to be released for without the requested PHI or, if the purpose of release is directly related to legal action, pursue obtaining a subpoena demanding release of specified information.

D. “Rythm” Request for Individual Authorization to Release Information:

If “Rythm” requires access to an individual’s PHI for purposes other than treatment, payment, healthcare operations, as allowed by law or for public interest purposes exempted from authorization, the workforce member will first document the need and purpose for release.

1. The appropriate authorization form will be mailed or transmitted to the individual specifying in as much detail as possible the PHI requested accompanied by a letter specifying the reason for the release of PHI.

2. The “Rythm” authorized workforce member will follow up by phone with the individual if no response has been received within two weeks from the date of the request. The phone call will be documented and become a part of the patient or plan member’s permanent record.

3. If the authorization is granted, “Rythm” shall only use the PHI requested for the purposes documented. The authorization form received from the individual shall become part of the patient or plan member’s permanent record.

4. If the authorization is denied, the response will be forwarded to the original requester and this response will be recorded in the patient or plan member’s permanent record. No further action to obtain or use the information will be made by “Rythm”.

E. Individual Authorization to Release Information:

An individual can request “Rythm” to release his/her own PHI to a third party for any purpose at any time. The individual must complete an authorization for this release, and “Rythm” must, in almost all cases, honor the request.

1. The individual must complete the appropriate authorization form specifying in as much detail as possible the PHI requested. No reason for the release is required.

2. Any PHI release authorized by the individual must be granted. “Rythm” (specify position or department) will send the PHI directly to the third party upon individual request. A letter to the third party shall be accompanied by the PHI and a copy of the completed authorization request. The authorization and response letter will be documented and become a part of the patient or plan member’s permanent record.

IV. Definitions

"Rythm" Privacy Officer: the individual appointed by "Rythm" to be the HIPAA Privacy Officer under s.164.530(a)(1) of the HIPAA Privacy Rule. HIPAA: Health Insurance Portability and Accountability Act of 1996 Electronic Protected Health Information (ePHI): Electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. ePHI does not include students' records held by educational institutions or employment records held by employers, or records for persons deceased for over 50 years.

Individually Identifiable Health Information (IIHI): Information that is a subset of health information, including genetic information and demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- That identifies the individual; or
- With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI): Individually identifiable health information or health care payment information maintained or transmitted in any medium, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. PHI does not include students' records held by educational institutions or employment records held by employers, or records for persons deceased for over 50 years.

Treatment: the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

Payment: the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:

- Determining eligibility or coverage under a plan and adjudicating claims,
- risk adjustments,
- billing and collection activities,
- reviewing health care services for medical necessity, coverage, justification of charges, and the like,
- utilization review activities; and
- disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

Operations: certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities, which are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501, include:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and nonhealthcare professionals, accreditation, certification, licensing, or credentialing activities;
- Underwriting enrollment, premium rating and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
- Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity. General Provisions at 45 CFR 164.506.