InfoHandler

Model HIPAA Privacy Rule Policy

Effective Date: March 23, 2016

Contents

Introduction

InfoHandler has adopted this HIPAA Compliance Privacy Rule Policy ("Policy") as of the effective date on the front page of this document. All workforce members are required to read and comply with this Policy. We will train all workforce members regarding the contents contained herein. However, workforce members have an affirmative duty to ask our Compliance Officer ("CO") questions and / or clarifications regarding this Policy, prior to signing that they have read and understood it.

Our Compliance Officer, the executive team, and all InfoHandler managers are responsible for the enforcement of this Policy. Workforce members that do not comply with this Policy will be sanctioned according to the Sanction Policy contained herein, and may be terminated if the facts surrounding the HIPAA Privacy Rule ("the Rule") violation warrant it.

Uses and Disclosures

Uses and Disclosures of protected health information ("PHI") may be permitted, required, or authorized under the Rule. It is our Policy only to allow Uses and Disclosures as provided for by the Rule. The permitted Uses and Disclosures under the Rule are contained in sections § 164.502 through § 164.514.

Violation of the Rule

It is our Policy to adopt, maintain, and fairly implement a methodology for determining when the Rule has been violated. Our methodology will be based on industry best practices and will be used each time a Rule violation determination is made. Our CO will be responsible for developing, maintaining and implementing the methodology as required.

It is our Policy to fully document each Rule violation, or allegation of same, and to provide a rationale indicating the grounds upon which a Rule violation was either found or not found. Our CO is the party responsible for ensuring that this documentation is created and stored according to our Policy.

Authorizations

It is our Policy only to Use and Disclose PHI requiring an Authorization consistent with the Authorization as provided by the patient. Our CO will ensure that all Authorizations meet the requirements of the Rule and that our staff is trained regarding those instances of Uses and Disclosures wherein Authorizations are implicated.

De-identification

It is our Policy only to allow a workforce member or a business associate ("Statistician") with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable for the purposes of de-identification to perform de-identification of PHI on our behalf.

The Statistician will be required to apply statistical principles and methods in a manner that results in a very small probability that the information could be re-identified and likewise required to remove all the identifiers specified by the Rule.

The Statistician, in collaboration with our CO, will be required to document the methods used to de-identify the information and the purposes for which the de-identified information will be used.

It is our Policy to insert a re-identification code into each de-identified record that meets that requirements of the Rule, which allows us to re-identify a patient's PHI should such a need arise.

Minimum Necessary

It is our Policy concerning Uses and Disclosures of PHI consistent with the principle of "minimum necessary," to identify the persons or classes of persons within our workforce who need access to PHI in order to carry out their job duties, the categories or types of PHI needed, and conditions appropriate to such access. Where the entire medical record is necessary (e.g. for

clinicians) it is our Policy to identify this requirement in our minimum necessary policies and procedures and to provide the rationale for this requirement.

It is our Policy to establish standard protocols for routine requests and to limit the PHI disclosed or requested to the minimum necessary for that particular type of disclosure or request. Non-routine Disclosures and requests will be reviewed on a case-by-case basis in accordance with the requirements of the Rule. As permitted by the Rule, for certain requests we may rely on the professional judgment of the requestor in determining the minimum necessary PHI to be provided, after making a determination that such a request is reasonable.

It is our Policy, where appropriate, to consider using a limited data set as a guiding principle for determining the minimum necessary requirement, but only in those cases wherein we have a data sharing agreement in place as required by the Rule.

Opportunity to Agree or Object

It is our Policy to provide patients the opportunity to agree or object regarding Uses and Disclosures of their PHI when provided for in the Rule. If the patient is present and has the capacity to make an informed decision then we will ask permission before: 1) disclosing PHI to friends and family; 2) using the patient's PHI in a facilities directory; and 3) using the patient's PHI for the purpose of notifying family members. If the patient is not present, or is incapacitated, then we will Use our professional judgment to Use and Disclose PHI in a manner that we believe is in the best interest of the patient, consistent with the principle of the minimum necessary.

Public Policy Disclosures

It is our Policy to Use and Disclose PHI for public policy reasons as permitted or required by the Rule. We will Use our professional judgment, consistent with the principle of minimum necessary, when making these Disclosures. However, we will also consider, and rely upon, where reasonably appropriate, the professional judgment of the government agencies and/or other stakeholders permitted to make such requests under the Rule (i.e. as to their input regarding the kinds of PHI required).

Personal Representatives

It is our Policy that, if under applicable law, a person has authority to act on behalf of a patient who is an adult or an emancipated minor in making decisions related to healthcare, we will treat such person as a personal representative under the Rule, with respect to PHI relevant to such personal representation.

It is our Policy that if under applicable law a parent, guardian, or other person acting in *loco parentis* has authority to act on behalf of a patient who is an un-emancipated minor in making decisions related to healthcare, we will treat such person as a personal representative under the Rule, with respect to PHI relevant to such personal representation, except that such person may not be a personal representative of an un-emancipated minor, and the minor has the authority to act as a patient directly, with respect to PHI pertaining to a healthcare service, if: a) the minor consents; b) the minor may obtain such healthcare without the consent of parent, guardian, or other person acting in *loco parentis* and the minor, a court, or another person authorized by law

consents; or c) a parent, guardian, or other person acting in *loco parentis* assents to an agreement of confidentiality between us and the minor with respect to such healthcare service.

It is our Policy, notwithstanding our recognition that minors have certain rights under the Rule, to provide a parent, guardian, or a person acting in *loco parentis* of an un-emancipated minor, PHI pertaining to the minor if such Use and disclosure is provided for under applicable state law or is consistent with applicable state law.

Business Associates

It is our Policy only to share PHI with a business associate after performing our requisite due diligence to ensure that the business associate is meeting all statutory and contractual requirements. A written contract ("Contract"), one that meets all the requirements of the Rule, and other applicable law, will be executed with each business associate. The Contract will be reviewed on a yearly basis, or more frequently at the discretion of our CO, to ensure that the business associate is not in material breach, and is otherwise complying with applicable law.

It is our Policy to have clauses in our Contract that give us the right, upon adequate notice, to inspect and audit the compliance records of the business associate. Further, our Contract will provide that the parties jointly develop a breach notification communications plan ("Plan") within a specified time period after execution of the Contract. Our CO will review the Plan with the respective business associate on yearly basis to ensure it is adequately maintained.

Patient's Bill of Rights

Federal law provides a patient several important rights regarding PHI. The following sections summarize our Policy regarding a patient's rights and provide information regarding how a patient may exercise them. Protecting a patient's PHI is an important part of the services we provide. We want to ensure that our workforce understands that a patient has a number of rights under the Rule. We are committed to delivering notification, access and all other patient rights in a timely manner. Under the Rule, the Patient's Bill of Rights is contained in sections § 164.520 through § 164.528.

Notice to Individuals

Since InfoHandler is a clearinghouse it is not our Policy to provide a Notice Of Privacy Practices (NOPP) to patients at any time when a request for the NOPP is made.

Restriction Requests

Patient have a right to request restrictions pertaining to the Uses and Disclosures of their PHI. However, without express written consent from our CO, it is our Policy only to allow those restrictions that are required by law.

It is our Policy to ask for all restriction requests regarding treatment, payment and operations to be in writing. Any restriction granted will be honored until such time as it is formally revoked. All restriction revocation requests must also be writing, including any revocation requests that we may initiate consistent with applicable law.

Restrictions add to our administrative burden in that they must be referenced prior to each instance of using or disclosing a patient's PHI, otherwise we run the risk of using or disclosing

PHI in violation of a restriction. It is our Policy only to agree to restrictions not required by law when there is a compelling reason to do so, as determined by our CO.

A written statement regarding the disposition of the restriction request will be provided to the individual making the request. If we deny the request, then our rationale for doing so will be included in the disposition statement. It is our Policy to respond to restriction requests within thirty (30) days of receipt.

Confidential Communications Requests

It is our Policy to ensure that patients clearly understand, whenever we communicate with them regarding confidentiality, that they have a right to request alternative means of confidential communications pertaining to: 1) their care; and 2) the Uses and Disclosures of their PHI.

It is our Policy to ask for all confidential communications requests to be in writing. An email from the patient is sufficient to meet the writing requirement as long as it can be reasonably authenticated. We will accommodate all reasonable requests according to the Rule.

Access Requests

It is our Policy to facilitate a patient's right to access, inspect and obtain a copy of their PHI in a designated record set except where such right is excluded by applicable law. All patient requests for access to PHI must be made in writing. Under a limited set of circumstances, we may deny a patient's request. It is our Policy that any denial of a request to access PHI will be communicated to the patient in writing.

Further, it is our Policy to inform the patient in writing concerning their rights to access PHI including the right to have a denial by us reviewed by a licensed third party healthcare professional under certain conditions. It is our Policy to comply with the decision made by the designated professional.

It is our Policy to charge a patient a reasonable fee for providing a copy of their PHI, but only after communicating the fee to be charged prior to delivery, and otherwise consistent with applicable law.

Amendment Requests

It is our Policy to allow patients to amend their PHI for as long as we maintain it. All such requests must be made in writing and the patient must provide us a reason that supports the requested amendment. Under certain conditions we may deny a patient's request to amend including, but not limited to, when the PHI: 1) was not created by us; 2) is excluded from access and inspection under applicable law; or 3) is accurate and complete.

It is our Policy that upon acceptance of the amendment we will work with the patient to identify other healthcare stakeholders that require notification and provide the notification. If we deny the amendment we will provide written reasons for denial and afford the patient an opportunity to submit a statement of disagreement.

Disclosure Requests

It is our Policy to promptly provide an accounting of a patient's PHI Disclosures made by us during the time period specified by applicable law, prior to the date on which the accounting is requested. Patients must make requests for an accounting in writing.

It is our policy not to provide any PHI excluded by applicable law from an accounting of Disclosures. We will provide one accounting within any twelve (12) month period to a patient at no charge. For additional accountings, we will charge a reasonable fee. We will notify the patient of any fee to be charged at the time of the request.

It is our Policy only to provide the disclosure information required by applicable law unless, on a case-by-case basis, our CO determines that more information should be provided. Under such circumstances our CO must document in writing why more information is being provided. If we deny a request for Disclosures it is our Policy to communicate the denial to the patient in writing.

Administrative Requirements

The Administrative Requirements are our organizational policies that apply to the totality of the Rule. Under the Rule, in general, these requirements are encompassed in section § 164.530.

Privacy Officer

It is our Policy to name an experienced staff member as our HIPAA Privacy Officer. We refer to this individual as our Compliance Officer ("CO") because his/her responsibilities generally encompass more than the Privacy Rule (e.g. responsibilities may include the HIPAA Security Rule as well as compliance with state laws and regulations). This individual functions as the point person for the executive management team with respect to Privacy Rule enforcement.

It is our Policy to designate and maintain, at all times, a HIPAA Privacy Officer. This individual's job description will be updated to reflect that the individual's responsibilities include, but are not limited to, the following: 1) training members of our workforce, including those members of our workforce that require specialized training; 2) writing all privacy policies and procedures and ensuring that they remain updated as per applicable law; 3) interacting with state and federal agencies and corporate counsel as required; 4) developing and enforcing our sanctions policy in collaboration with human resources; 5) managing the processes directly related to fulfilling patient requests (e.g. requests for access to PHI); 6) investigating security incidents and notifying patients and other stakeholders of a breach when warranted by applicable law; 7) managing all privacy related complaints; and 8) otherwise administering our privacy program.

Workforce Training

It is our Policy to provide workforce training regarding the permitted Uses and Disclosures of PHI according to the requirements as set forth in §164.530(b)(1) and (2).

In addition, it is our Policy to provide our workforce training on the HIPAA Breach Notification Rule as contained in 45 CFR §164 Subpart D. Further it is our policy to provide our workforce the training required by law when new statutes and/or rules are promulgated and finalized.

Individual members of our workforce who manage specialized processes required by the Rule will be provided the advanced training needed to fulfill their job responsibilities. It is our Policy

to train all workforce members on Privacy Rule and Breach Notification basics, including the executive management team. At the discretion of our CO, workforce members whose only interaction with protected health information is "incident to" their job responsibilities (e.g. housekeeping) may receive specialized training as dictated by their job functions.

It is our Policy to develop and maintain a privacy awareness program that is separate and distinct from our privacy-training program. Our awareness program will ensure that recognizing the importance of privacy becomes part of our workforce's day-to-day operations. Our CO will have wide discretion to implement our awareness program using enabling electronic technologies and other awareness building methodologies.

Our Policy is to have our workforce trained/re-trained within thirty days of the Effective Date of this Policy. Further, it is our Policy to train new workforce members within two days of their date of hire.

Workforce Sanctions

It is our Policy to enforce workforce sanctions as required by the Rule. Our CO, in conjunction with human resources, will ensure that proper sanction policy and procedures are developed and maintained. Workforce members who egregiously and/or repeatedly violate the Rule may be terminated according to the facts and circumstances surrounding the violation(s).

It general, it is our Policy to provide for an escalating scale of sanctions for violations of the Rule as determined by our CO. Our sanctions scale may range from a violation due to being misinformed (e.g. insufficient training) to willful and intentional illegal activity. All sanctions will be fully documented according to our Documentation Policy and stored in the workforce member's personnel file.

Safeguards

It is our Policy to reasonably safeguard PHI from any intentional, unintentional or incidental Uses or Disclosures that are in violation of the Rule. It is also our Policy to limit, as much as practicable, incidental Uses or Disclosures made pursuant to an otherwise permitted or required Use or disclosure.

It is our Policy to safeguard PHI in whatever form or medium it may exist. Specifically, with respect to electronic PHI ("ePHI"), it is our Policy to implement all the Administrative, Technical and Physical safeguards of the Security Rule necessary to reasonably and appropriately protect ePHI.

Documentation

It is our Policy to maintain all the documentation required by the Rule in electronic form and in a manner consistent with our need to meet our burden of proof ("Documentation Policy"). All documentation subject to our Documentation Policy will be maintained for six years from the date of its creation or the date when it last was in effect, whichever is later.

It is our Policy to maintain evidence of process results consistent with our Documentation Policy and to archive the results in a manner that facilitates retrieval for internal purposes or for the purpose of making the results available to other stakeholders (e.g. the Secretary of HHS).

It is our Policy to maintain all documentation in electronic form, converting from paper into electronic media as a scanned PDF when required. It is our strategic objective to natively capture in electronic media, as much documentation as is practicable, improving our ability to do so over time.

It is our Policy to make all documentation required by the workforce readily available to it. Where appropriate, all documentation will be stored in a centralized repository on our Intranet so that the workforce members know where it is located and how it can be accessed. The repository will contain only final released versions of the documentation (e.g. Notice of Privacy Practices) so that the workforce may rely on its currency.

Complaints

It is our Policy to be completely transparent with respect to the rights that individuals and workforce members have under the Rule. An individual has the right to file and all workforce members will be trained to answer in the affirmative should an individual inquire about their right to file a complaint under the Rule, and under our privacy program.

It is also our Policy to train our workforce members that they also have a right to file a complaint under the Rule, both to a government agency and, under our privacy program, directly with us. We welcome all such feedback. It is our policy to handle complaints fairly and in a timely manner. We have adopted a zero tolerance position regarding any workforce member who retaliates against a patient, or another workforce member, for filing a complaint or exercising any other right under the Rule.

It is our Policy to cooperate fully with HHS, should an externally filed complaint result in an investigation. Our CO and legal counsel are responsible for working directly with HHS and shall represent our interests for the entirety of the investigation. They will be responsible for reporting to the executive team regarding the ongoing status of the investigation.

It is our Policy that all complaints must be submitted in writing and that the disposition of each complaint must be provided via a written response to the complainant.

Policies and Procedures

It is our Policy to make modifications to our policies and procedures as necessary and appropriate to comply with applicable law, including the standards, implementation specifications, and other requirements of the Rule.

It is our Policy to make modifications to our policies and procedures that pertain to all protected health information created by us prior to the effective date of the modifications. We have reserved the right to make such changes in our NOPP for this very purpose as permitted by the Rule.

It is our Policy that all relevant members of our workforce read and sign off on those policies and procedures that are directly applicable to them as determined by our CO.

Mitigation

It is our Policy to take all steps within our power to reasonably and appropriately mitigate any harmful effect of: 1) a wrongful Use or disclosure of PHI; 2) a violation of our privacy program;

or 3) a violation of the Rule. Mitigation steps will be taken whether one of our workforce members or one of our business associates caused the harm.

It is our Policy to enumerate more specific steps for certain kinds of harms in other policy documents (e.g. our Breach Notification Policy). In all cases our CO will take the lead role in managing mitigation efforts on our behalf.

Internal Audits and Reviews

It is our Policy to conduct internal audits and reviews of our privacy program at least once a year and on and as needed basis at the discretion of our CO. The CO shall report to the executive team each time an internal audit or review is conducted. Internal audits will be conducted by using our compliance checklists and any other policies and procedures our CO develops related to this strategic objective.

It is our Policy to conduct an internal review after all security breaches and an internal audit after a security breach that triggers notification to patients and other stakeholders. The policies, procedures and tracking mechanisms implicated by the breach will be reviewed and modified where necessary to prevent similar breaches from occurring in the future.

Conclusion

InfoHandler is committed to protecting the PHI of its patients and expects all its workforce members to demonstrate a similar commitment. InfoHandler recognizes that compliance with the Rule is not a onetime event but rather a continuous process. We encourage workforce members to provide our CO feedback regarding this Policy, the organizational processes that underpin it, and the tracking mechanisms we have put in place to capture process results.