



essent Employee Guide to

# Privacy & Security

*“An ESSENTial part of caring for our patients”*



## Dear Fellow Employees:

In the fast paced world of the 21<sup>st</sup> century, it seems harder than ever to maintain the privacy of one's personal information. From credit bureaus to Wal-Mart, almost every business imaginable is collecting and maintaining an ever increasing amount of information about their customers. Grocery stores use their "loyal customer cards" to track the spending patterns of their customers, credit bureaus monitor your payment history in an effort to track your financial health, and, in an effort to improve the emergency 911 system, cell phones can now be used to pinpoint your exact location at all times. Is it any wonder that privacy complaints and identity theft are on the rise?

*At Essent, it is our goal to become a trusted and essential part of every community in which we operate. We recognize that every patient that comes to one of our facilities is entrusting us with information that is personal and confidential. In many cases, not even family members or close personal friends are aware of the information that may be contained in a patient's medical record.*

Our patients have an expectation of privacy with regard to their medical records; and we have an obligation to honor that privacy at all times. Accessing and/or disclosing confidential information without authorization is both unethical and illegal.

This booklet will provide you with an overview of the laws, rules, and regulations regarding the confidentiality, privacy, and security of sensitive information. In addition, Essent has many detailed policies and procedures regarding privacy and confidentiality. As a member of our workforce, it is your responsibility to comply with our policies and protect the privacy of our patients at all times.

If you have any questions or concerns about confidentiality or patient privacy, you should contact your Facility Privacy Officer (FPO). Additionally, the compliance department maintains a 24-hour, toll free hotline **(1-800-472-8868)** for reporting known or suspected misbehavior, including privacy violations. I urge you to review this information carefully and to immediately report any privacy violations that you may become aware of. The quality of the care that we provide, and ultimately our reputation, depends on your good judgment and discretion. Thank you in advance for your adherence to our high ethical standards.

*Charles J. Fletcher*

Charles J. Fletcher  
Vice President for Corporate Compliance

## **Overview of Privacy and Security**

Privacy and security mean different things to different people. Within the healthcare industry, when we talk about privacy and security, for the most part we are talking about the **Health Insurance Portability and Accountability Act (“HIPAA”)**. This legislation required all “*covered entities*” to protect the confidentiality, integrity, and availability of much of the information that they create, maintain, transmit, or receive. *Covered entities* include health plans, health care clearinghouses, and health care providers such as hospitals and physicians.

### **HIPAA is comprised of four major initiatives:**

#### **1. Administrative Simplification (transaction code sets)**

- Requires standardization of all healthcare transactions so as to lower the overall cost of administering healthcare.
- Effective October 16, 2003.

#### **2. Privacy Rule**

- Requires that providers maintain the confidentiality of **Protected Health Information (“PHI”)** and that patients be allowed to access and review their medical records.
- Effective April 14, 2003.

#### **3. Security Rule**

- Requires that providers implement safeguards to maintain the confidentiality, integrity, and availability of all electronic PHI (“ePHI”) that they create, maintain, transmit, or destroy.
- Effective April 20, 2005.

#### **4. National Identifiers**

- Requires employers and providers to obtain a unique, 10-digit national identifier so as to eliminate the need for providers to keep up with multiple identifiers for multiple health plans.
- To be phased from 2004 through 2007

While the administrative simplification and national identifiers may impact some of our employees in their day-to-day job activities, the privacy and security rules apply to every member of our workforce including certain business associates. The remainder of this brochure focuses exclusively on the HIPAA privacy and security rules. For more information on the HIPAA administrative simplification and/or national identifiers, please visit The Centers for Medicare and Medicaid Services (“CMS”) web site at <http://www.cms.hhs.gov/hipaa/hipaa2/>; or contact the Corporate Compliance Officer at [charles.fletcher@essenthealthcare.com](mailto:charles.fletcher@essenthealthcare.com) or call 1-800-472-8868.

## The Privacy and Security Rules

Many health care providers and professionals have long made it a practice to ensure that reasonable safeguards are in place to protect the privacy of their patients. For example:

- By speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
- By avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
- By isolating or locking file cabinets and records rooms; and/or
- By providing additional security, such as passwords, on computers that access or house sensitive information.

The Health Insurance Portability and Accountability Act ("HIPAA") includes provisions related to the protection of patient privacy and the security of electronic patient information. The *Privacy Rule* became effective on April 14, 2003. The privacy rule requires that all covered entities implement policies and procedures to maintain the confidentiality of any "*individually identifiable health information*" held or transmitted by the covered entity, in any form or media, whether electronic, paper, or oral.

Individually identifiable health information includes many common identifiers such as name, address, birth date, and Social Security Number. HIPAA refers to this information as "*Protected Health Information (PHI)*." Protected Health Information (PHI) is any information, including demographic data, which relates to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual.

The *Security Rule* is effective as of April 20, 2005. The Security Rule supplements the Privacy Rule by requiring covered entities to implement additional measures to safeguard the confidentiality, availability, and integrity of all *electronic* PHI (ePHI).

As we move away from paper records in favor of electronic medical records, it becomes more and more important that we secure this electronic information in a safe and confidential manner. In addition to the risks that we would normally associate with a medical record (i.e. theft, fire, flood...), there are additional threats that are unique to electronic records. For example, without the proper protections in place, a computer virus could alter or destroy sensitive patient information that is needed for patient care.

For these reasons, it is imperative that all workforce members:

- Log-off of any system or application when it is not in use;
- Log-off of any workstation when it is to be left unattended;
- NEVER share your password with anyone;
- NEVER write your password down where someone might find it;
- NEVER use your computer privileges to access information that you do not have a legitimate business need for;
- ALWAYS report any instance of unauthorized system access immediately!

**Both the Privacy Rule and the Security Rule require that Protected Health Information be safeguarded from all reasonably anticipated threats and vulnerabilities.** Failure to maintain the confidentiality of PHI (whether in paper, electronic, or any other format) can result in serious damage to our reputation and may result in civil or criminal penalties. In addition, there are many State and Local Laws related to patient privacy. To the extent that any Local or State Law is more stringent than the HIPAA regulations, we are obligated to follow the more stringent State or Local Law.

The remainder of this brochure outlines some of the uses and disclosures that are permitted by HIPAA and/or uses that require an authorization under HIPAA. While no educational brochure can address every conceivable scenario that might arise in our course of work, this brochure outlines many of the basic principles of the privacy and security rules and gives numerous examples of permitted and prohibited activities.

Each Essent facility has a Compliance Director, a Privacy Officer, and a Security Officer who are available to address your questions and/or concerns about this brochure or any other rules and regulations. All Essent workforce members are reminded of their obligation to report any instance of non-compliance. Reports can be made anonymously by calling the 24-hour compliance reporting hotline at 1-800-472-8868, or by contacting your local compliance representatives who are listed below.

PRMC Compliance Director  
PRMC Privacy Officer  
PRMC Security Officer

Cheryl Perry  
Barbara Haines  
Carolyn Sparks

(903) 737-3943  
(903) 737-1301  
(903) 737-

## **Disclosures Required by HIPAA**

HIPAA requires that we disclose PHI under certain circumstances. All covered entities *must* disclose protected health information in the following two situations:

1. To individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information;
2. To HHS when it is undertaking a compliance investigation or review or enforcement action.
3. As required by State or local regulations.

## **Disclosures Permitted by HIPAA**

A covered entity is permitted to use and disclose protected health information without authorization if the disclosure is being made to the individual who is the subject of the information. In addition, covered entities are allowed to use and disclose PHI without authorization for *Treatment, Payment, or Health Care Operations*.

*Treatment* is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and/or the referral of a patient by one provider to another.

*Payment* activities include the following:

- a. Activities undertaken by a health plan to obtain premiums and/or determine its responsibility for coverage/payment;
- b. Activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care;
- c. Eligibility determinations;
- d. Billing, collections, and claims management activities; and/or
- e. Utilization review activities such as pre-certification and chart review.

*Health care operations* include any of the following activities:

- a. Quality assessment and improvement activities, including case management and care coordination;
- b. Competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation;
- c. Conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance reviews;
- d. Specified insurance functions, such as underwriting, risk rating, and reinsuring risk;
- e. Business management and general administrative activities of the covered entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising activities for the benefit of the covered entity.

Most uses and disclosures of **psychotherapy notes** for treatment, payment, and health care operations purposes require written authorization.

### **Uses and Disclosures that Require an Opportunity to Agree or Object**

Patients must be given the opportunity to agree or object to certain uses or disclosures as described below. In these cases, informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree or object to the disclosure. This is normally accomplished by issuing the patient a copy of the Hospital Privacy Notice which outlines our policy with respect to these types of disclosures.

Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual. Examples of situations requiring an opportunity to agree or object include the following:

*Facility Directories* - It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered entity may rely on an individual's informal permission to list the individual in its facility directory. The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

Directory information must be limited to the following:

- The name of the individual
- His/her location in the hospital (i.e. medical/surgical unit or ICU)
- His/her general condition (i.e. critical, stable...)
- His/her religious affiliation (to be released only to members of the clergy)

*For Notification and Other Purposes* - A covered entity also may rely on an individual's informal permission to disclose PHI to the individual's family, relatives, or friends, or to other persons who may be involved in the care of the individual. This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying family members of the individual's location, general condition, or death.

It is our policy to list patients in our hospital directories and to disclose PHI as necessary for notification or other purposes unless the individual specifically requests that we not do so.

## Incidental Uses and Disclosures

The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of PHI that occurs as a result of, or as “incident to,” an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards to protect the information, and the information being shared was limited to the “*minimum necessary*”.

For example, a hospital visitor may overhear a provider’s confidential conversation with another provider or a patient, or may glimpse a patient’s information on a sign-in sheet or nursing station whiteboard. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices and, thus, does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards.

*Minimum Necessary Standard* - The minimum necessary standard, a key provision of the Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a particular function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.

The Privacy Rule’s requirements for the minimum necessary standard are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity. The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual’s authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

## Disclosures Related to Public Interest and Benefit Activities

The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for the 12 national priority purposes listed below. These disclosures are permitted, although not required, in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

1. **Required by Law** - Covered entities may use and disclose PHI without individual authorization as *required by law*.
2. **Public Health Activities** - Covered entities may disclose PHI to:
  - a. Public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability;
  - b. Public health or other government authorities authorized to receive reports of child abuse and neglect;
  - c. Entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance;
  - d. Individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and
  - e. Employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or similar state law.
3. **Victims of Abuse, Neglect or Domestic Violence** - In certain circumstances, covered entities may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.
4. **Health Oversight Activities** - Covered entities may disclose PHI to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.
5. **Judicial and Administrative Proceedings** - Covered entities may disclose PHI in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.

6. **Law Enforcement Purposes** - Covered entities may disclose PHI to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions:
  - a. As required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;
  - b. To identify or locate a suspect, fugitive, material witness, or missing person;
  - c. In response to a law enforcement official's request for information about a victim or suspected victim of a crime;
  - d. To alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death;
  - e. When a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and
  - f. By a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.
  
7. **Decedents** - Covered entities may disclose PHI to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.
  
8. **Cadaver Organ, Eye, or Tissue Donation** - Covered entities may use or disclose PHI to facilitate the donation and transplantation of cadaver organs, eyes, and tissue.
  
9. **Research** - is defined as any systematic investigation designed to develop or contribute to generalized knowledge. The Privacy Rule permits a covered entity to use and disclose PHI for research purposes, without an individual's authorization, provided the covered entity obtains either:
  - a. Documentation that an alteration or waiver of individuals' authorization for the use or disclosure of PHI about them for research purposes has been approved by an Institutional Review Board or Privacy Board;
  - b. Representations from the researcher that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any PHI from the covered entity, and that PHI for which access is sought is necessary for the research; or
  - c. Representations from the researcher that the use or disclosure sought is solely for research on the PHI of decedents, that the PHI sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individual about whom information is sought.

10. **Serious Threat to Health or Safety** - Covered entities may disclose PHI that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.
11. **Essential Government Functions** - An authorization is not required to use or disclose PHI for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.
12. **Workers' Compensation** - Covered entities may disclose PHI as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

### **Uses and Disclosures Requiring an Authorization Under HIPAA**

A covered entity **must** obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.

*An authorization must be written* in specific terms. It may allow use and disclosure of PHI by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.

*Psychotherapy Notes* - A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions:

- The covered entity who originated the notes may use them for treatment.
- A covered entity may use or disclose psychotherapy notes, without an individual's authorization, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law.

*Marketing* - Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service. The Privacy Rule carves out the following health-related activities from this definition of marketing:

- Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication;
- Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan;
- Communications for treatment of the individual; and
- Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.

A covered entity must obtain an authorization to use or disclose PHI for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact.

## Penalties for Non-Compliance

Violations of HIPAA can lead to immediate termination of your employment and both civil and/or criminal prosecution. Penalties for non-compliance are as follows:

1. **Inadvertent Work Related Disclosure** – Any individual who inadvertently makes an unauthorized disclosure of PHI is subject to a written reprimand. Examples of inadvertent unauthorized disclosure include faxing PHI to the wrong fax number, e-mailing PHI to the wrong email address, accessing ones own records without authorization, or other acts of carelessness that lead to an unauthorized disclosure.
2. **Intentional Work Related Disclosure** – Any individual who knowingly or intentionally discloses PHI that is obtained as a result of their employment is subject to disciplinary measures as outlined in the sanctions policy. Examples of such disclosure include sharing PHI with co-workers who are not involved in caring for the person who is the subject of the PHI, accessing the PHI of a co-worker or family member if you are not involved in caring for that person, or accessing the PHI of any other individual (including yourself and/or your minor children) without a legitimate business need for that information. Intentional disclosures may also result in civil and/or criminal prosecution.
3. **Civil Money Penalties** - HHS may impose civil money penalties on a covered entity of \$100 per failure to comply with a Privacy Rule requirement. That penalty may not exceed \$25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.
4. **Criminal Penalties** - A person who knowingly obtains or discloses PHI in violation of HIPAA faces a fine of \$50,000 and up to one-year imprisonment. The criminal penalties increase to \$100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.

## ACKNOWLEDGEMENT STATEMENT

I, \_\_\_\_\_, have received, read and understand the *Essent Employee Guide to Privacy and Security*. I understand my responsibility not to disclose any confidential company information without proper authorization. I will not share my information system log-on ID or password with anyone, and I will safeguard all company information that I am entrusted with at all times. Regardless of the level of access that I am granted as part of my employment, I will not access (or attempt to access) any confidential information without a legitimate business need for that information. I understand that I am required to report any instance of unauthorized use or disclosure of confidential information to the compliance reporting hotline or my local compliance representatives.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Title/Department

\_\_\_\_\_  
Date