

Essent Healthcare, Inc.

HIPAA Compliance Program

A successful compliance program addresses the public and private sectors' mutual goals of reducing fraud and abuse; enhancing health care providers' operations; improving the quality of health care services; and reducing the overall cost of health care services. Attaining these goals benefits the hospital industry, the government, and patients alike. Compliance programs help hospitals fulfill their legal duty to refrain from submitting false or inaccurate claims or engaging in other illegal practices by encouraging ethical and compliant behavior. Hospitals may gain important additional benefits by implementing an effective compliance program, including:

- Demonstrating the hospital's commitment to honest and responsible corporate conduct;
- Increasing the likelihood of preventing, identifying, and correcting unlawful and unethical behavior at an early stage;
- Encouraging employees to report potential problems to allow for appropriate internal inquiry and corrective action; and
- Minimizing any financial loss to government and taxpayers, as well as any corresponding financial loss to the hospital through early detection and reporting of compliance issues.

The Office of Inspector General (OIG) recognizes that implementation of a compliance program may not entirely eliminate improper or unethical conduct from the operations of health care providers. However, an effective compliance program demonstrates a hospital's good faith effort to comply with applicable statutes, regulations, and other Federal health care program requirements, and may significantly reduce the risk of unlawful conduct and corresponding sanctions.

In this respect, we have developed and implemented a compliance program that is specific to the Health Insurance Portability and Accountability Act (HIPAA) regulations. The purpose of the HIPAA compliance program is to prevent and detect unauthorized uses and/or disclosures of confidential information by:

1. Appropriately identifying and mitigating threats and vulnerabilities associated with accessing confidential information,
2. Providing access to confidential information only when appropriate and necessary,
3. Safeguarding information systems from tampering, malicious software, intrusion, and unauthorized access,
4. Maintaining the confidentiality, availability, and integrity of all sensitive information, and
5. Providing the training and education necessary for all workforce members to carry out their job duties while complying with all applicable laws, rules, and regulations.

Our HIPAA compliance program, as described below, contains all of the essential elements of an effective compliance program as outlined in the Federal Sentencing Commissions' *Guidelines for Organizations*. Should you have any questions about the HIPAA compliance program, or any other compliance concerns, please contact your local compliance representatives. Alternatively, you may contact the Corporate Compliance Officer or address your concerns to the compliance reporting hotline at 1-800-472-8868. Remember, when reporting compliance concerns, you can remain anonymous should you so desire.

I. Oversight

Effective oversight is an important element of any successful compliance program. Without oversight, most compliance programs quickly become ineffective due to a lack of attention and accountability. Effective oversight allows us to respond to compliance issues in a timely manner, and to make appropriate revisions to the compliance program as necessary due to changes in the regulations and/or our organization. The Corporate Compliance Officer (CCO) has overall responsibility for maintaining the HIPAA compliance program. The CCO is assisted on a day-to-day basis by the Local Compliance Directors (LCD), the Compliance Committee, and the HIPAA compliance sub-committee which is comprised of the following individuals:

- **Corporate Compliance Officer** is responsible for establishing and overseeing the HIPAA compliance program.
- **Corporate Privacy Officer** is responsible for implementation of those portions of the HIPAA compliance program that pertain to the privacy rule.
- **Corporate Security Officer** is responsible for implementation of those portions of the HIPAA compliance program that pertain to the security rule.
- **Local Privacy and Security Officers** are responsible for day-to-day operations of the HIPAA compliance program at their respective facilities.

| PRIVACY OFFICERS | | | |
|-----------------------------|--------------------|--|---------------------|
| Name | Facility | Title | Phone |
| Anna Gene O'Neal | Corporate | Essent VP/Chief Privacy Officer | 615-312-5124 |
| Pat Murtagh | Sharon | Medical Record Director | 860-364-4059 |
| Barbara Haines | Paris | Medical Record Director | 903-737-1301 |
| Gloria Swanbon | Merrimack | Quality Director | 978-521-8538 |
| Elaine Bulman | Nashoba | Medical Record Director | 978-784-9268 |
| Kim Moroski | SRMC | Compliance Officer | 724-627-2445 |
| | | | |
| SECURITY OFFICERS | | | |
| Name | Facility | Title | Phone |
| Armen Arakelian | Data Center | Essent VP/CIO | 781-472-3801 |
| Mike Orr | Sharon | CFO | 860-364-4085 |
| Carolyn Sparks | Paris | IT Director | |
| Nancy Hoffman | Merrimack | CFO | 978-521-8137 |
| Steve Roach | Nashoba | CFO | 978-784-9220 |
| | SRMC | | |
| | | | |
| COMPLIANCE COMMITTEE | | | |
| Name | Facility | Title | Phone |
| Charles Fletcher | Corporate | Corporate Compliance Officer | 615-312-5131 |
| Pat Murtagh | Sharon | Medical Record Director | 860-364-4059 |
| Cheryl Perry | Paris | Human Resources Director | 903-737-3943 |
| Nancy Hoffman | Merrimack | CFO | 978-521-8137 |
| Steve Roach | Nashoba | CFO | 978-784-9220 |
| Armen Arakelian | Data Center | Essent VP/CIO | 781-472-3801 |
| Anna Gene O'Neal | Corporate | Essent VP/Chief Privacy Officer | 615-312-5124 |
| Kim Moroski | SRMC | Compliance Officer | 724-627-2445 |

All Other Workforce Members are required to actively participate in the HIPAA compliance program by attending training sessions, following the policies and procedures, and reporting non-compliant behavior and/or unauthorized uses or disclosures of confidential information.

Policies Related to HIPAA Oversight

- ISP-000 Oversight for HIPAA Security
- ISP-014 Ongoing monitoring and administration
- ISP-021 Business Associates
- HIPAA-012 Accounting for Disclosures
- HIPAA-013 Business Associates
- HIPAA-015 Privacy Officers
- HIPAA-1010 Use/Disclosure of PHI for Treatment, Payment, or Operations
- HIPAA-1020 Use/Disclosure with Authorization

II. Written Standards and Procedures

In order to ensure an effective compliance program, the compliance committee has developed and implemented written standards and procedures to be followed by all Essent workforce members. Each Essent workforce member is responsible for knowing and understanding all of the policies and procedures that apply to his/her workplace. Additional written standards and procedures are available on the Essent web site at: <http://essent-web/index.htm>. Written standards and procedures related to the HIPAA compliance program include the following:

1. Privacy Policies
2. Privacy Notice
3. Security Policies
4. Essent Employee Guide to Privacy and Security
5. Essent Employee Guide to Compliance
6. Essent Code of Conduct

III. Reporting Mechanism

In order to be effective, a compliance program must include a mechanism whereby workforce members can report instances of known or suspected non-compliance. To facilitate this effort, we have implemented an anonymous, toll-free, 24-hour compliance reporting hotline that is available to all workforce members, patients, and/or visitors. It should be noted that our Code of Conduct requires all workforce members to report known or suspected non-compliance. Reports can be made anonymously by using the compliance reporting hotline (1-800-472-8868), or by contacting one of your local compliance representatives.

In addition, our Privacy Notice encourages the reporting of HIPAA violations and contains the following language: “You have the right to complain to the hospital and/or to the Secretary of Health and Human Services if you believe your rights to privacy have been violated. If you feel your privacy rights have been violated, please submit your complaint in writing to...” The

privacy notice then gives the appropriate contact information for the facility CEO or privacy officer, and/or the Department of Health and Human Services.

All privacy and/or security complaints/violations shall be logged and investigated by the appropriate Privacy and/or Security Officer. Privacy Officers and Security Officers are reminded to encourage the filing of formal, written complaints (in lieu of verbal complaints). Complaints/violations shall be logged using the Patient Safety Expert (PSE) software. This software will allow for improved communication (automatic email notification) and will provide a standardized tracking and reporting mechanism. Complaint/violation logs shall be maintained for a period of six years from the date of final issue resolution.

Policies Related to Reporting

ISP-012 Security Incident Reporting

HIPAA-011 Privacy Complaint Log Policy

IV. Training and Education

In an effort to ensure ongoing compliance, we have implemented an awareness program to keep our workforce informed about HIPAA and other compliance issues. The awareness program is designed to focus attention on the importance of maintaining effective privacy and security measures and how to report violations or questionable situations. The awareness program consists of:

- Orientation training for new employees
- System user training (application training)
- Instructor led compliance presentations and training seminars,
- Periodic security reminders (such as emails, posters and/or pamphlets),
- Annual training programs (safety fairs, etc...)
- Warning banners on the certain system log-in screens.

All workforce members will receive mandatory HIPAA security “roll-out” training before the April 20th implementation deadline. The roll-out training will include a summary of the HIPAA regulations and requirements and an overview of the related Essent policies and procedures.

Additionally, all system users are given application specific training during their first few days on the job. This training begins with new employee orientation and allows the employee to learn the system that he/she will be using as part of his/her day-to-day activities. The CISD maintains a help desk to assist users with problems and/or questions.

All users are required to sign confidentiality statements prior to being granted access to sensitive information to ensure that they are aware of their responsibilities for protecting the confidentiality of such information. Annual confidentiality statements and acknowledgements of the Code of Conduct will be obtained from all workforce members as part of the security awareness program.

Policies Related to Training and Education

- ISP-013 Security Awareness

V. Auditing and Monitoring

Ongoing auditing and monitoring are an essential part of any compliance program. For purposes of the HIPAA compliance program, ongoing monitoring will include device and media controls, content filtering, periodic risk assessments, Periodic review of the HIPAA Compliance Program, and periodic audits.

Device and Media Controls require that we monitor the acquisition, maintenance, and disposition of all hardware and software that is used to access to PHI. Additionally, all storage devices are monitored to ensure that data is properly backed up and that it is retrievable in the event of an emergency. Device and media controls require that we maintain inventories of all hardware, networks, applications, and users so as to prevent unauthorized access to or destruction of PHI.

Content Filtering has been implemented to mitigate the risk posed by malicious software such as computer viruses and/or worms. Content filtering blocks users from entering certain web sites (for example porn sites and online gaming sites), prevents certain PHI from being transmitted to non-authorized individuals, and prevents unwanted solicitations/emails from flooding the system. Content filtering programs can also be used to log user activities and identify individual users who are using the system inappropriately.

Risk Assessments are conducted on an annual basis to ensure the ongoing effectiveness of the compliance program. Risk assessments are designed to identify and prioritize the various threats and vulnerabilities that might impact our information systems. Based on the results of the risk assessment, safeguards will be implemented to mitigate the risks identified by the assessment.

Periodic Review of the HIPAA Compliance Program will be conducted to ensure that the program continues to meet the changing needs of our organization and/or changes in the law, rules, or regulations.

Routine Audits will be conducted periodically to ensure compliance with this HIPAA compliance program. Monthly privacy audits will be conducted to verify that individuals accessing particular records or other sensitive information have a legitimate business need for that information. In addition, we will periodically audit the access authorization process to ensure that only those individuals with a legitimate business need have access to PHI; and we will conduct other audits as needed to ensure ongoing compliance.

Policies Related to Auditing and Monitoring

- ISP-003 Device and Media Controls
- ISP-004 Content Filtering
- ISP-009 Risk Assessment
- ISP-019 Audit Policy
- HIPAA-010 Privacy Audits

VI. Response and Prevention

Response and Prevention activities are a cornerstone of our HIPAA compliance program. We have developed and implemented a contingency plan for responding to an emergency or other natural disaster. Our contingency plan will allow us to maintain operations in the event of an emergency while addressing the resources needed to restore full operating capability while preventing unauthorized access.

We have implemented numerous policies and procedures aimed at preventing unauthorized use or disclosure of PHI. Prior to being granted access to any Essent information system, all workforce members must sign a confidentiality statement that outlines the responsibilities of all users to protect the confidentiality of sensitive information. In addition, users are reminded not to share passwords with anyone.

Policies governing workstation use and security have also been implemented. These policies require that workforce members properly secure their workstations and limit personal use of company resources. Prevention activities also include the use of encryption/decryption software and requirements for documenting system maintenance and upgrades.

Policies Related to Response and Prevention

- ISP-001 Access Authorization
- ISP-002 User ID and Passwords
- ISP-005 Data Backup and Storage
- ISP-006 Access to IT Facilities
- ISP-007 Workstation Use
- ISP-008 Workstation Security
- ISP-011 Electronic Communications
- ISP-015 Transmission Security
- ISP-016 Encryption
- ISP-017 Disaster Recovery and Contingency Plan
- ISP-018 System Updates and Maintenance

VII. Enforcement and Discipline

We have implemented a sanction policy to set forth guidelines for disciplining workforce members who fail to comply with the policies and procedures implemented under this HIPAA compliance program. It is our policy that discipline will be consistent across all facilities and all class of workers and that a progressive disciplinary system is used. Our progressive disciplinary process does not prevent us from immediately terminating workforce members for certain egregious, or intentional violations.

Under the Essent Code of Conduct, *all workforce members are required to report misconduct*. Employees are reminded that each facility has a Compliance Officer, Privacy Officer, and Security Officer who are available to address questions of concerns. The Corporate Compliance Officer is available at all times to address concerns or answer questions regarding the compliance program and can be reached at Charles.Fletcher@Essenthealthcare.com or (615) 312-5131.

Policies related to Enforcement and Discipline

- ISP-010 Sanctions