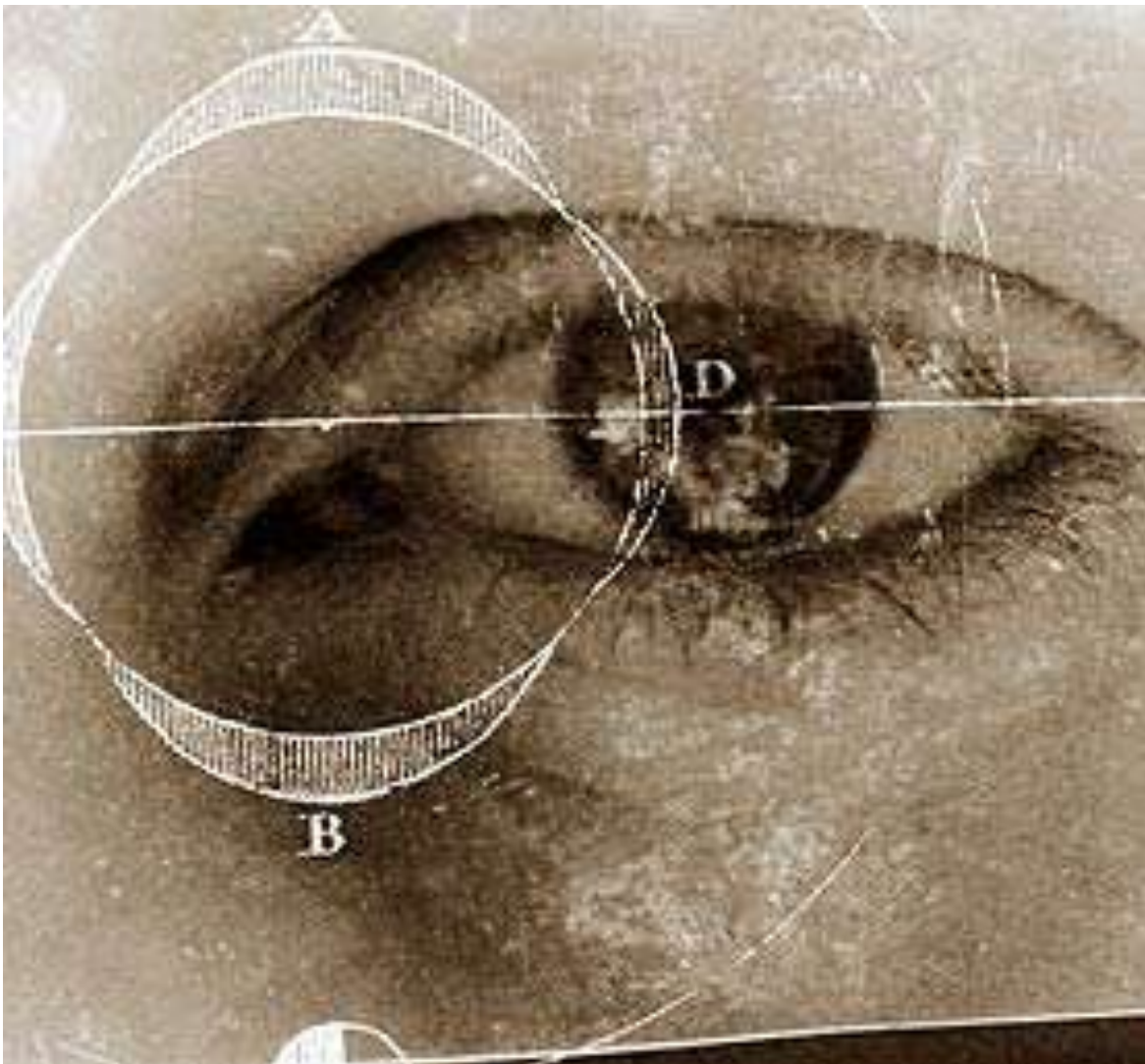


# Ethics, Privacy & Compliance Manual



Our unique vision has made us the leading provider of comprehensive patient eligibility services to America's hospitals.

800.255.0953 | [www.chamberlinedmonds.com](http://www.chamberlinedmonds.com)

 **ChamberlinEdmonds**  
Optimizing Eligibility & Enrollment

# I. ETHICS

**The Code of Ethics is the Company's statement of good corporate citizenship: we pledge to do business in an ethical manner.**

## ■ COMPLIANCE WITH LAWS

Chamberlin Edmonds conducts its business in accordance with the spirit and letter of all applicable laws and regulations. The Company provides training and supplemental materials to help employees know and comply with the laws affecting their job responsibilities. Employees are expected to promptly request guidance from the Legal Department regarding any questions of applicability or compliance.

## ■ PRIVACY & CONFIDENTIALITY

As a Company working with protected health information, employees are held to the highest standards of privacy and confidentiality. Patient financial or medical information will not be disclosed without authorization.

## ■ RECORDS ACCURACY

The Company will maintain honest and accurate records and will submit honest and accurate applications, claims and reports to the government, auditors, and stakeholders.

## ■ CONFLICTS OF INTEREST

Employees are obligated to assure they remain free of conflicts of interest in the performance of their responsibilities.

## ■ INTEGRITY IN ALL CONTACTS

Offering or giving money, services or other things of material value to government officials is strictly prohibited.

## ■ RESPECT FOR THE INDIVIDUAL

The Company values respect for the individual, courtesy, and teamwork as employees perform their duties and interact with each other, patients, hospital staff, members and personnel of managed care organizations, and government officials. Employees of Chamberlin Edmonds are expected to perform their duties in a non-discriminatory fashion and without regard to race, color, sex, religion, age, national origin, citizenship, disability, veteran status, sexual orientation, gender identity, marital status, or eligibility for public benefits.

## Compliance with Laws

Chamberlin Edmonds provides varied services in different states. These services may be provided only pursuant to appropriate federal, state and local laws and regulations. Such laws and regulations may include licenses, permits, access to medical records and confidentiality, Medicare and Medicaid regulations, and the Social Security Administration's Standards of Responsibility for Representatives.

We will comply with all applicable laws and regulations. All employees should maintain a current working knowledge about and ensure compliance with all laws and regulations. Compliance and thorough knowledge will enable the Company to maintain quality in representing patients. In assisting patients, we are careful to inform them that information provided on government applications must be truthful. Employees should immediately report violations or suspected violations to a supervisor or member of management, the Ethics, Privacy & Compliance Officer, or the HELPLINE.

These are general principles and policies. Chamberlin Edmonds will provide its employees with the information and training they need to comply fully with all applicable laws and regulations.

### INVESTIGATIONS & AUDITS

Chamberlin Edmonds will be forthright in dealing with any billing inquiries. Requests for information will be answered with complete, factual and accurate information. We will cooperate with and be courteous to all government inspectors who may be conducting an investigation and provide them the information to which they are entitled during an inspection. We will cooperate with and be courteous to all auditors in order to assure a complete and accurate evaluation of Company books, records and management.

During a government inspection or audit, employees must never conceal, destroy, or alter any documents, or lie or make misleading statements to the investigator or auditor. Employees should not attempt to cause another employee to fail to provide accurate information or obstruct, mislead, or delay the communication of information or records relating to a possible violation of law.

### EXCLUDED HEALTHCARE INDIVIDUALS & ENTITIES

The Company does not employ individuals or entities who are excluded or are ineligible to participate in federal healthcare programs, suspended or debarred from federal government contracts, or convicted of a criminal offense related to the provision of healthcare items or services. The Company's People Services Department searches the Department of Health & Human Services' Office of Inspector General's List of Excluded Individuals & Entities as well as the General Service Administration's Excluded Parties List System prior to hiring any employee (please see Appendix A). Each employee is required to annually certify that s/he is not an excluded person and that s/he is aware of the requirement to report any such exclusion to the Company.

## Privacy & Confidentiality

### HEALTH INFORMATION

The Company's primary goal is to provide quality services to our hospital, managed care organization, and government customers that enable them to provide the finest services to their patients or members. We treat all customers' patients with respect, including appropriate confidentiality of records and information, in accordance with federal and state regulations. Release or discussion of specific information must be necessary to perform services on behalf of our customers and must be authorized by the patient. Please see the Privacy section of this manual.

### RECORD RETENTION

Medical and business documents and records are retained in accordance with the law and our Record Retention Plan. It is important to retain and destroy records appropriately according to our policy. Employees must not tamper with records, nor remove or destroy them prior to the specified date.

### COMPANY-OWNED INFORMATION

Knowledge that an employee gains as a result of employment with Chamberlin Edmonds is confidential and should not be used to for the employee's own benefit or the benefit of any other person or organization. This confidential information includes Company policies, standard operating procedures, client lists, personnel data, pricing and cost data, financial data, research data, strategic plans, marketing strategies, and information pertaining to acquisitions, divestitures, affiliations and mergers. Confidential information about our organization's strategies and operations is a valuable asset, not to be shared with others outside of the company unless the individuals have a legitimate need to know this information and have agreed to maintain the confidentiality of the information.

### INSIDE INFORMATION

Employees may learn non-public information about the Company or about a customer during the course of employment. This kind of information includes strategic plans, marketing strategies, financial results, and information pertaining to acquisitions, divestitures, affiliations and mergers. Employees should not discuss this information outside the Company or even within the Company unless the employee to whom it is disclosed needs to know in order to perform his or her job.

Federal securities laws prohibit individuals from using this kind of non-public information in making decisions about publicly-traded securities and in influencing others' decisions. This information can only be used and/or discussed two days after release of the information to the public by the media. Employees who have any questions about application of this policy should contact the Legal Department.

## Records Accuracy

### APPLICATIONS FOR BENEFITS

Chamberlin Edmonds is committed to upholding the highest standards of honesty and truthfulness in our applications. We pledge to submit accurate and complete applications all of the time to the best of our ability, and to ensure that our applicants understand the importance of honesty and the consequences of fraud.

Except in specific, limited situations in which the patient is unable to sign an application, Chamberlin Edmonds does not tolerate any applications being signed by anyone other than the applicant. If there is an exceptional situation that prohibits the applicant from signing an application, employees should contact a supervisor and/or the Ethics, Privacy & Compliance Officer before proceeding.

### BILLING SERVICES

As a service to some hospital customers, Chamberlin Edmonds submits bills for payment that are coded and otherwise prepared by the hospital customer. Chamberlin Edmonds does not perform any coding functions. Employees must not engage in any coding activities. Bills submitted by Chamberlin Edmonds on behalf of our customers will reflect appropriate and accurate billing to the best of the Company's knowledge. Employees should not present any claim for payment that the employee knows or has reason to suspect may be false or fraudulent.

Billing must be performed in accordance with Company policies and conform to all federal and state laws. Training and audit systems are established to ensure that these standards are upheld and that systemic issues are addressed and corrected as necessary.

### FINANCIAL REPORTING

Company policies require a high standard of accuracy and completeness in financial reporting. These records serve as a basis for managing our business and are important in meeting our obligations to patients, colleagues, and customers. They are also necessary for compliance with tax and financial reporting requirements.

All financial information must reflect actual transactions and conform to generally accepted accounting principles. Chamberlin Edmonds' Finance Department maintains a system of internal controls and external auditing to provide reasonable assurances that all transactions are executed in accordance with management's authorization and are recorded in a proper manner so as to maintain accountability of the organization's assets.

## Conflicts of Interest

A conflict of interest exists when the loyalty of a Company employee is actually or could be perceived to be divided between their responsibilities to the Company and to an outside interest. The Company reasonably expects individual loyalty and faithfulness from its employees. The Company relies on the good faith of its employees when making business decisions on behalf of the Company and fully respects the rights of employees to privacy in their personal affairs and activities. Employees of the Company shall strive to avoid situations in their personal activities that are, or might appear to be, in conflict with their responsibilities to the Company.

Employees who are uncertain if an activity may pose a conflict should call the HELPLINE before taking action. These standards do not address all the types of conflict of interest an employee may face. Employees should always speak to a supervisor or the Ethics, Privacy & Compliance Officer to seek resolution of any actual or potential conflict of interest before taking action.

### FINANCIAL INTEREST

Employees should avoid placing business with any firm that the employee or his or her family has a direct or indirect financial interest. If an employee discovers that the Company has independently placed business with a firm that with whom he or she has a financial interest, it is the employee's responsibility to notify the Company as soon as he or she becomes aware of such a relationship.

## **Integrity in all Contacts**

The Company's primary business activity includes submitting applications on behalf of needy individuals to local, state, and federal governments. The Company's policy is to make sure that all contacts with government officials are truthful and compliant with ethical and legal guidelines. Where the Company assists healthcare customers, including hospitals and managed care organizations, with billing, we will do so in compliance with law. Employees who are uncertain about whether their activity with government officials is within all applicable guidelines should contact the HELPLINE.

### **GIFTS TO GOVERNMENT OFFICIALS**

Employees of the Company should not give anything of value to an employee of a federal, state, or local agency. As a general rule, gifts worth \$20 or less are not considered to be "of value."

### **CHARITABLE GIFTS**

The only contributions that will be made in the Company's name will be authorized by the Executive Team. The focus of Company charitable giving will be to contribute to organizations that are related to health care and disease management.

### **POLITICAL CONTRIBUTIONS**

Any employee's personal financial contributions to the election campaigns of candidates of their choice will be made at the employee's sole expense. No political activities by employees shall be conducted on Company premises, on Company time, or under any circumstances that may give the appearance that the Company sponsors such activity.

## **Respect for the Individual**

Chamberlin Edmonds employees treat each other, all patients, hospital staff, vendors and suppliers, and government officials without regard to race, color, sex, religion, age, national origin, citizenship, disability, veteran status, sexual orientation, gender identity, marital status, or eligibility for public assistance. This policy also includes other criteria as designated by applicable state and local laws and regulations.

## II. PRIVACY

As a Company working with protected health information and contracts with hospitals and health plans, the Company must act in compliance with the Health Insurance Portability & Accountability Act of 1996 and the Health Information Technology for Economic & Clinical Health Act (HITECH Act) (collectively known as HIPAA). The Company has entered into Business Associate Agreements with healthcare providers so that they will legally be able to share patients' protected health information with us. In return, we have agreed to use reasonable safeguards to prevent the unauthorized use or disclosure of that protected health information. We also have to take appropriate administrative, technical, and physical safeguards to protect electronic protected health information.

Employees may only use or disclose patient health information in order to provide eligibility, business office, or managed care services pursuant to a contract, for the proper management and administration of the Company, or to carry out the Company's legal responsibilities. An employee may only access patient health information that s/he needs in order to perform his or her job. Any potential vendors or contractors must sign a Business Associate Agreement with the Company before any patient health information may be shared. Any unauthorized use or disclosure of patient health information, whether accidental or purposeful, must be reported to the Ethics, Privacy & Compliance Officer the same day that it is discovered or as soon as possible thereafter so that appropriate corrective action can be taken by the Company to lessen the effects of the use or disclosure.

Assisting with Social Security and healthcare benefits applications involves more than just medical information. We also process a large amount of patients' sensitive financial information, including employer wage statements, tax returns, life insurance and mortgage documents. To prevent identity theft due to negligent use or disclosure of financial information, we use the same precautions and safeguards with patient financial data as we do with patients' protected health information. This protection extends to Social Security numbers as well as any identifying financial information.

### What is protected health information under HIPAA?

#### CONTENT

HIPAA applies to any medical information that identifies or reasonably could be expected to identify a patient. Some examples of medical information are diagnosis, reason for hospitalization, medical treatment, procedures, tests, or even the fact that a patient was in the hospital. Some examples of information that reasonably could be expected to identify a patient include name, date of birth, date of death, date of admission or discharge from a hospital, Social Security number, hospital account number, member number, medical record number, address, telephone number, or other account numbers.

#### FORM

HIPAA applies to electronic, written, and verbal communication about a patient that contains medical information that reasonably could be expected to identify the patient. The most relevant examples of electronic communication at CEA are email about a patient and access to computer systems containing patient information. Some examples of written communication are medical records, "face sheets" or demographic referral sheets, internal reports, and applications for benefits. Some examples of verbal communication are face-to-face conversation with patients or with other CEA staff, and telephone conversations with patients, patients' friends and family, or other healthcare providers.

## Reasonable Safeguards: Electronic Media

### EMAIL

Email that could reasonably be expected to identify a patient and contains medical information must be protected under HIPAA. Therefore reasonable safeguards must be taken to prevent unauthorized use or disclosure. Due to the vulnerability of the Internet, CEA has implemented an encrypted internal email system and virtual private network for logging in through the internet. (For detailed information, please see Appendix B). Electronic media safeguards may be adjusted to accommodate technological development.

### ACCEPTABLE USE

Using any information system to gain access to protected health information is against the law unless it is necessary to complete a work-related task. To obtain access to protected health information of family members, CEA employees will use the customary channels used by members of the public and will not take advantage of access to a hospital information system.

### PASSWORDS

Using another person's unique logon or user id and password to access any information system is against Company policy (please see Appendix C). Even if the purpose is to accomplish work-related tasks, sharing passwords is prohibited because it undermines the audit trail that the unique logon was designed to create.

## Reasonable Safeguards: Written Documents

Written documents are more secure than electronic communication but must still be used with reasonable safeguards.

### MAIL

Protected health information sent through the mail should be protected with a cover sheet that identifies the information attached as confidential. The cover sheet should also contain the intended recipient's name if known and not just the name of their unit or company, and should contain the sender's name and contact information in case the information becomes lost or misdirected. Any shipments of patient information that arrive damaged must be reported immediately to a supervisor and/or the Ethics, Privacy & Compliance Officer.

### FAXING

Use of facsimile machines for transmitting HIPAA-protected information is not forbidden, but use of reasonable safeguards is critical due to the risk of mis-dialing a fax machine. Faxes of HIPAA-protected information should always have a cover sheet identifying the information as confidential. As with mail, the cover sheet should also contain the intended recipient's name if known and not just the name of their unit or company, as well as the sender's name and contact information and instructions regarding contact and destruction in the event of mistaken receipt. Any instances of confirmed faxes to a mis-dialed number must be reported immediately to a supervisor and/or the Ethics, Privacy & Compliance Officer.

Some kinds of health information have stricter protection under state law than HIPAA affords and should not be faxed at all. Examples of this kind of information include psychiatric diagnoses and treatment, HIV/AIDS diagnoses and treatment, information from a federally-funded substance abuse center, and genetic diagnoses. These kinds of information should be sent by mail or by overnight courier if time is of the essence.

### DISPOSAL

Protected information that does not have to be kept should never be thrown in a trash can. The appropriate way to dispose of protected information is to use a shredder or a secure document disposal service. Most Company facilities have disposal containers specifically for disposal of protected information. For more information on records retention and disposal, see the Records Retention Plan.

## Reasonable Safeguards: Verbal Communication

### FACE-TO-FACE CONVERSATION

Any conversation regarding protected health information should take place within Company premises or should not contain any cues that reasonably could be expected to identify a patient. When in a hospital or other premises, reasonable safeguards must be taken to prevent unauthorized parties from overhearing protected health information. These reasonable safeguards include lowering your voice, pulling a privacy curtain if available, and moving to an empty room if one is available.

### TELEPHONE CONVERSATION

A caller who calls the Company seeking protected health information, including admission information and/or application status, must be authenticated as having a right to the information. A caller who identifies himself as a CEA client should be asked for his Social Security number as a means of verifying that the caller is the person he claims to be. A caller who identifies himself as a friend or family member of the client should be checked against the contact information in CEA's information system and files.

## III. COMPLIANCE PROGRAM

### Purpose

The Ethics, Privacy & Compliance Program demonstrates the Company's commitment to an organizational culture that encourages ethical conduct and compliance with the law. The elements of the Program include:

- ◆ Establishing standards and procedures to prevent and detect criminal conduct
- ◆ Educating employees, management and the Board of Directors about the content and operation of the Program
- ◆ Making reasonable efforts to ensure that personnel who exercise substantial authority have not engaged in illegal activities or other conduct inconsistent with an effective Program
- ◆ Conducting effective training programs periodically to communicate standards and procedures of the Program, and otherwise disseminate information appropriate to individuals' respective roles and responsibilities
- ◆ Monitoring and auditing to detect and prevent criminal conduct and to ensure that the Program is being followed
- ◆ Evaluating periodically the effectiveness of the Program
- ◆ Operating and publicizing retaliation-free reporting channels, including a confidential telephone and fax reporting system and anonymous mail reporting system available to all employees
- ◆ Promoting the Program throughout the organization with appropriate incentives to perform in accordance with the Program, and enforcing it throughout the organization with appropriate disciplinary measures for criminal conduct
- ◆ Conducting and/or overseeing investigations of matters that merit investigation under the Program and making appropriate recommendations as to whether such investigations should be done internally or externally, depending upon the issue involved and available resources
- ◆ If criminal conduct is detected, taking reasonable steps to respond and to prevent further similar criminal conduct, including making any necessary modifications to the Program

## Individual Responsibility

As a Company and as a team, we each have a part in our success. We need to be sure that each employee understands Chamberlin Edmonds' commitment to ethics, which means thinking about and doing the right thing, as well as complying with our legal duties and obligations. We believe that compliance occurs as the result of good business practice and that our Code of Ethics reflects our desire to identify these practices.

The Code of Ethics summarizes the key portions of our Ethics, Privacy & Compliance Program. It also serves as a reference to each employee to better understand the Program. As you perform your duties within the Company, you should always feel that you are working within the guidelines of the Code of Ethics. If at any time you feel that you are not working with our Code of Ethics or if you are not sure, please discuss the issue with your supervisor or the resources listed in this document. Our collective commitment to the Ethics, Privacy & Compliance Program is critical to the success of the Company.

Each employee has an individual responsibility for reporting activity by any other employee or contractor that appears to violate laws or policies outlined within this document.

## Management Responsibility

The Company's managers and supervisors must take responsibility for their employees' actions. Managers are not only expected to understand and follow the ethical standards in the Code of Ethics, but also to ensure that the employees they supervise understand and follow these standards.

## How to Make Reports

Ideally, concerns will first be addressed with a person's immediate supervisor. However, if this uncomfortable or inappropriate, the following options are available:

- ◆ Contacting the People Services Department
- ◆ Calling the HELPLINE at 404-279-5140 or toll-free at 1-800-255-0953 x5140
- ◆ Sending a fax to the Compliance confidential fax line at 404-965-9162 or toll-free at 1-866-537-8143
- ◆ Mailing an anonymous report using a blue, self-addressed, postage-paid Chamberlin Edmonds return correspondence envelope to the attention of Compliance. These envelopes are used for all return correspondence within the Compliance Office and so would not alert anyone in the mailroom that a compliance report was enclosed. Also, the Compliance Office opens all mail pieces marked in this fashion; no other staff open or see the contents of the mail.

## Assurance of Confidentiality of Report

The Company will make every effort, within the law, to protect the identity of persons reporting possible misconduct or participating in an investigation.

## Assurance of No Retaliation

The Company will make every effort, within the law, to protect the identity of persons reporting possible misconduct or participating in an investigation. No retribution or discipline for anyone who reports a possible violation in good faith will be tolerated. Prohibited retaliation includes demotion, termination of employment, harassment, or intimidation in response to a report or participation in an investigation. Any colleague who deliberately makes a false accusation with the purpose of harming or retaliating against another colleague will be subject to discipline.

## Assurance of Internal Investigation

The Company is committed to prompt and thorough investigation of all reports according to policy (please see Investigation Protocol attached as Appendix D) and to implement necessary corrective actions, should issues be discovered. All employees are expected to fully cooperate with investigative and corrective efforts.

## Corrective Action

All employee violations of the policies and laws described in this manual are subject to disciplinary action. The specific corrective action for a given violation will depend on the nature, severity, and frequency of the violation and may result in any of the following disciplinary actions:

- ◆ Verbal warning
- ◆ Written warning
- ◆ Termination of employment
- ◆ Restitution

## Internal Audit & Monitoring

The Company is committed to the regular monitoring of compliance with policies. These monitoring systems include quality control efforts, regular training initiatives, and internal or external financial monitoring.

## Acknowledgement of the Program

As a condition of employment, new employees are required to sign an acknowledgment confirming they have received the Code of Ethics and understand that it represents mandatory policies of the Company.

## Education

All employees should receive initial Ethics, Privacy & Compliance training covering this document and its associated policies within thirty days of starting employment with the Company. This education may take the form of live training or web-based presentation. At the end of this training, all employees should sign an attestation of their attendance and complete a quiz developed by the Compliance Office to demonstrate understanding of the training. A score of 90% correct is the minimum required to demonstrate adequate understanding of the concepts presented, and lower scores require repeat testing.

After the calendar year in which an employee was hired and completed initial Ethics & Compliance training, all employees should receive update education annually. The curriculum of this training is developed by the Ethics, Privacy & Compliance Officer based on review of reported incidents during the last year and new policies and laws. This education may take the form of live training or web-based presentation. Employees must sign an attestation of attendance and pass a quiz as stated above. Additionally, each employee is required to annually sign an attestation that:

- ◆ S/he is not aware of the Company or any of its employees or business associates having violated the law or the Ethics, Privacy & Compliance Manual or other related policies;
- ◆ S/he has not been excluded from participation in any federal health care program and understands that s/he is required to report to the Company any exclusion under the U.S. Department of Health & Human Services (HHS) or General Services Administration (GSA) rules.

## Board Reports

The Compliance Officer will provide a report to the Board of Directors no less than annually. As appropriate, the Compliance Officer will notify management of confirmed violations of law, regulation, or legal guidance and provide remedial recommendations. In the event that the Compliance Officer concludes that a report to management is not appropriate, the Compliance Officer shall report violations to the Chairperson of the Compliance Committee.

# APPENDIX A: Excluded Healthcare Individuals & Entities

DATE: 6/17/02

---

Background investigations will be conducted on all new hires and will include:

- ◆ Criminal records check, both state and federal
- ◆ Cumulative sanction report check (maintained by HHS/OIG)
- ◆ List of parties excluded from federal programs check (maintained by General Services Administration (GSA))
- ◆ Reference checks

## PEOPLE SERVICES PROCEDURES

- ◆ All job postings must include the following statement: “Any job offer will be contingent upon the results of an updated background investigation.”
- ◆ During the interview process, applicants must be informed that a background investigation will be performed.
- ◆ A release form for background investigations must be completed and signed by the applicant at the time of the conditional job offer.
- ◆ If a background investigation has been completed within the prior 24-month period, it is not necessary to conduct another investigation.
- ◆ Background investigations are a condition of the job offer. A negative report disqualifies the applicant for the position.

# APPENDIX B: Email

DATE: 8-6-01

REVISED: 5-11-04, 7-30-04, 5-20-05, 10-31-08, 2-1-10

---

## INTRODUCTION

The Company has adopted this email policy to comply with HIPAA and its regulations to protect the security of electronic health information, as well as to fulfill our duty to protect the confidentiality and integrity of confidential client health information as required by law, professional ethics, and accreditation requirements of the hospitals we service.

All individuals who are authorized to use the email system (hereinafter referred to as “users”) of the Company must be familiar with this policy. Demonstrated competence in the requirements of this policy is an important part of every user’s responsibilities.

## ASSUMPTIONS

- ◆ Email can be immediately broadcast worldwide and be received or intercepted by many intended and unintended recipients.
- ◆ Recipients can forward email messages to other recipients without the original sender’s permission or knowledge.
- ◆ Users can easily misaddress an email.
- ◆ Email is easier to falsify than handwritten or signed documents.
- ◆ Backup copies of email may exist even after the sender or the recipient has deleted his or her copy.

## GENERAL POLICY

Any email that identifies or reasonably could be expected to identify a client and also contains information about the diagnosis or treatment of his or her medical condition is protected health information.

- ◆ The Company will treat all email messages sent or received that concern the diagnosis or treatment of a client’s medical condition with the same degree of confidentiality as other pieces of health information.
- ◆ No email may contain any of the following in the subject line. Any email containing any of these elements will be returned to the sender with instructions to delete identifying information.
  1. Name
  2. All geographic subdivisions smaller than a state (including street address, city, county, ZIP code)
  3. Birth date, admission date, discharge date, date of death, and all ages over 89
  4. Telephone number
  5. Fax number
  6. Email address
  7. Social Security number
  8. Medical record number
  9. Health plan beneficiary number
  10. Account number
  11. Certificate/license number
  12. Vehicle identifier or serial number, including license plate number
  13. Device identifier or serial number
  14. Web Universal Resource Locator (URL)
  15. Internet Protocol (IP) address number
  16. Biometric identifier (including finger and voiceprint)
  17. Full-face photographic image
  18. Any other unique identifying number, characteristic, or code
- ◆ Company employees using a hospital email system must comply with the privacy procedures of that facility. Please work with your managers to ensure that you are trained in the hospital’s procedures.
- ◆ The Company email system is secure, so at this time password protection is not required for Company communications.

# APPENDIX C: Sharing Passwords Prohibited

DATE: 6/12/02

---

## PURPOSE FOR POLICY

The purpose of a login user name and password is to tell a computer the identity of a user and to give it a way to verify that identity. It is important for security reasons for healthcare companies to have this way of limiting access to computers that contain patients' protected health information and other sensitive and confidential information to only those people who need to know.

## PROHIBITED ACTIONS

It is very important that employees not share passwords verbally or in writing with anyone because it could compromise our promise to patients that we will safeguard their private medical and financial information. Similarly, if an employee works for CEA in a hospital, and the hospital issues the CEA employee a login id and password to use the hospital computer, the employee is prohibited from sharing that password with anyone. We have specifically agreed in hospital contracts that we will not:

- ◆ Share unique individual login id's and passwords with other individuals.
- ◆ Enable other individuals to access applications, software, and systems via unique individual login id's and passwords or otherwise. **This includes access to the Internet.**

Any violation of this policy can result in discipline, including termination of employment.

## REPORTING

An employee who has a reasonable basis to believe that another CEA employee is improperly sharing his or her password or allowing others to use a CEA or hospital computer with his or her password is obligated to report it immediately to the Corporate Compliance Officer or to a supervisor, who should then report it to the Corporate Compliance Officer. A reporting employee will not be fired, demoted, harassed, or otherwise discriminated against because s/he reported this concern. The Corporate Compliance Officer will perform an investigation that will be reviewed by senior management in order to determine what corrective action needs to be taken.

# APPENDIX D: Investigation Protocol

DATE: 6/11/02  
REVISED: 5/20/05

---

## INTRODUCTION

Chamberlin Edmonds has set in place a mechanism for employees and staff to freely and, to the extent possible, anonymously communicate corporate compliance concerns and questions to the Corporate Compliance Officer. An integral part of the Corporate Compliance Officer's responsibility is the timely and thorough investigation of any reports of compliance-related concerns, including but not limited to detailed inquiry via interviews and/or systematic examination of relevant documents.

## GENERAL POLICY

### 1. Initial identification of need for investigation

Compliance issues needing investigation may be identified via calls to the Compliance Hotline, reports to supervisors or People Services, review of data, or employee surveys.

- ◆ Compliance Responsibilities: The Compliance Officer will assume primary responsibility for Ethics, the full range of Healthcare Laws, Regulations and Policies, Privacy, Confidentiality, HIPAA and Records management. People Services will assume primary responsibility for issues related to Discrimination, Harassment and Labor/Wage & Hour Laws. The full resources of the Company will be available to assist the Compliance Office and People Services.
- ◆ Issues disclosed to personnel other than the Corporate Compliance Officer: Potential healthcare or privacy compliance issues reported to management or People Services should be referred to the Compliance Officer immediately for review to determine priority and necessity for outside counsel involvement.
- ◆ Issues disclosed to the Compliance Officer: A log of all compliance-related contact is maintained by the Compliance Officer and notes the date, issue, and recommendation. Each contact is assigned a Report of Contact (RC) number that appears on all follow-up documentation in the file.

### 2. Review techniques

Once a potential issue has been identified by the Compliance Officer as an investigation priority, s/he he will determine which review techniques to utilize. These may include:

- ◆ On-site visits
- ◆ Interviews with management and/or operations
- ◆ Questionnaires developed to solicit impressions of a broad cross section of staff
- ◆ Review of charts and/or files
- ◆ Review of financial records
- ◆ Trend analysis data that identifies deviations in a given area over a period of time

### 3. Investigation Files

Compliance investigation files will be referenced using the assigned Report of Contact number and will include any of the following documents, where applicable:

- ◆ Description of the discovery of the potential issue (i.e. initial report)
- ◆ Documentation of the alleged issue or violation
- ◆ Description of the investigative process
- ◆ Log of persons interviewed or documents reviewed
- ◆ Copies of interview notes or key documents
- ◆ Results of the investigation (e.g. unfounded, confirmed)
- ◆ Recommendations for corrective action (i.e. disciplinary action, re-training specific to employee, company-wide training, self-disclosure)

# APPENDIX E: Safeguarding Patient Information Outside CEA or Customer Environments

DATE: 11/16/05

REVISED: 2/1/10

---

## INTRODUCTION

In some cases, it may be appropriate for an employee to transport or access patient information from home, a hotel while traveling, or another remote location, as approved by that employee's manager. Because Chamberlin Edmonds employees typically handle protected health information (PHI) as defined by the Health Insurance Portability & Accountability Act of 1996 (HIPAA) Privacy & Security Rules, it is important for employees who work from a remote location to take reasonable administrative, physical, and technical safeguards to prevent the unauthorized use or disclosure of this PHI. In any case, transport or access to patient information should be held to the minimum amount necessary to do your job.

## GENERAL POLICY

### 1. ACCESS TO INFORMATION

#### ◆ Physical security:

- An employee who is working from a remote location must segregate all paper PHI to a locked room, cabinet, or drawer to which family members or other unauthorized people will not be able to gain access.
- Work must be conducted in a physically secure and separate location from common family rooms. Computer screens should be facing away from traffic flow into and out of the area.
- Employees must not store laptop computers or paper containing PHI in a vehicle overnight unless stored out of sight in a locked trunk without window access.

#### ◆ Technical security:

- An employee who is working from a remote location must password-protect all PHI stored on a computer or other electronic device so that family members or other unauthorized people will not be able to gain access. This can be accomplished by saving documents with a password or selecting encryption from the security options menu.
- An employee who is working from a remote location must log into Chamberlin Edmonds computer system via a keyfob with a Personal Identification Number to ensure secure access. The keyfob and PIN must be stored in a secure manner such that unauthorized parties cannot gain access.
- Employees must not reveal work-related PINs or passwords to family members or other unauthorized parties.
- Access to CEA information systems or any other electronic PHI must not be shared with family members or other unauthorized parties.
- Employees working remotely must lock or log out of information systems containing PHI when leaving the workstation. Employees must install a password-protected screen saver or automatic log-off feature for when the computer is not in use.
- If equipment owned by the employee and containing PHI must be repaired, all PHI must be removed from the hard drive, if feasible. A record should be kept of who made the repairs.
- Employees working remotely must not use wireless networks unless encryption is installed.
- Computers with internet access must have current versions of the following installed:
  - ◆ Anti-virus program
  - ◆ Operating system updates
- Software programs such as games and music programs that allow file sharing must not be installed on any computer on which PHI is used.
- Employees must not download patient-identifiable information onto their personal computers, especially not through personal email accounts.

**2. TRANSMISSION OF INFORMATION**

- ◆ Fax transmission of PHI must be preceded by a fax cover sheet identifying the information as confidential.

**3. DISPOSAL OF INFORMATION**

- ◆ In order to work from home, an employee who uses a computer connected to a printer must have a shredder on-site. All paper PHI that is no longer needed must be shredded as opposed to simply thrown in the trash.
- ◆ Employees who need to destroy technical media such as disks or hard drives that contain PHI should bring those to CEA Information Technology staff for destruction.

**4. THEFT OR LOSS OF PHI**

- ◆ If software, hardware, or data are stolen or lost by an employee working remotely, the Ethics, Privacy & Compliance Officer will be notified by that employee immediately.

**5. TRANSPORTING PHI**

- ◆ If an employee needs to transport patient health information, such as from one worksite to another or to a CEA office or government agency, the PHI should be transported in an opaque container capable of being secured, such as an envelope, portfolio, storage clipboard, briefcase, or box. If the employee temporarily leaves the vehicle, the PHI should be locked in the trunk.

# APPENDIX F: Identity Theft Prevention

DATE: 1/21/09  
REVISED: 2/1/10

---

## **What is identity theft?**

Identity theft occurs when a person steals another person's name, Social Security Number (SSN) or other personal information and uses it to make fraudulent charges on the victim's account or to apply for new credit accounts. It can take a victim anywhere from three months to more than a year to clear his or her credit when this happens.

Patients in hospitals are further vulnerable because of the rise of medical identity theft. Medical identity theft occurs when a person steals another person's personal information and uses it to obtain medical care. Medical identity theft can cause erroneous entries in the victim's existing medical record or creation of fictitious medical records in the victim's name. When a patient is victimized in this way, his or her insurance claim file can be affected and cause coverage denials. Medical identity theft can also cause health care providers to submit false claims for payment. Perhaps the gravest result is that this fraud can cause serious hospital safety issues, when drug allergies, blood types or medical histories of the victim do not match those of the perpetrator.

Self-pay patients in particular are vulnerable to identity theft because a variety of identifying information is needed to apply for government benefits such as Social Security disability and Medicaid. The applications typically require name, date of birth, and SSN. With the increasing emphasis on investigating Medicaid fraud and abuse, applications now require more verifying documents than ever before, showing evidence both of identity and citizenship as well as financial eligibility for needs-based programs. Identity and citizenship verifications can include photo identification, birth certificate, and passport. Financial verifications can include bank statements, wage stubs from an employer, W-2 and other tax documents, and information about life insurance policies.

As the risk of identity theft increases, CEA's customer hospitals grow increasingly vulnerable to the risks of erosion of patient trust, reputational damage, financial losses, and increased regulatory scrutiny that identity theft can cause. CEA would like to partner with our customer hospitals to help prevent and detect identity theft so that these risks can be minimized.

## **FACTA Red Flags Rule**

Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), also known as the Red Flags Rule, on October 31, 2007. This legislation requires that all organizations subject to the legislation must develop and implement a written Identity Theft Prevention Program to detect, prevent and lessen the effects of identity theft. While Chamberlin Edmonds & Associates, Inc. ("CEA") is not a "creditor" according to the definition in the legislation, many of the hospitals with whom we contract have indicated that they are "creditors" subject to FACTA due to treatment of patient accounts. Among other things, FACTA requires a creditor to ensure that its service providers that handle patient accounts have an Identity Theft Prevention Plan and are following it. A service provider must detect, prevent and lessen the effects of identity theft just like a FACTA creditor.

This Plan sets out CEA's policies and procedures to identify "Red Flags," defined as a pattern, practice or specific activity that indicates the possible existence of identity theft, and to communicate those Red Flags to our hospital customers to assist them with preventing and detecting identity theft. CEA will update this Plan periodically to reflect changes in reasonably foreseeable identity theft risks identified by our hospital customers. CEA will train our employees about the Plan and will update our employees as needed regarding changes to the Plan.

### **SUSPICIOUS DOCUMENTS**

We partner with our customer hospitals to help them comply with FACTA and to help prevent identity theft by notifying hospital staff when a patient shows us “suspicious documents” as defined FACTA.

CEA employees regularly see a wide variety of identifying documents required to submit applications to Medicaid.

Therefore we can report to hospitals if we see the following types of suspicious documents:

- ◆ Documents provided for identification that appear to have been altered or forged;
- ◆ Documents that appear to have been destroyed and reassembled;
- ◆ A photograph or physical description on a patient’s identification that is not consistent with the patient’s appearance.

### **SUSPICIOUS PERSONAL IDENTIFYING INFORMATION**

- ◆ Information on documents provided by a patient that is not consistent with information provided by the patient;
- ◆ Information on documents provided by a patient that is not consistent with readily-accessible information on file with the hospital, such as the demographic information entered by the hospital’s registration department.