



Health Insurance Portability and Accountability Act (HIPAA) Policy

Original Effective Date: June 22, 2017	Review / Revision Date: July 16, 2018	Board of Health Resolution: 2017.06.082
--	---	---

Maintenance Steward: Privacy Officer **History:** New Revised Archived

Organizational Scope:

Full Agency Administration Community Services Environmental Health Health Services

Frequency of Review:

Annually Biennially 5 Years As Needed Other:

Location:

S-Drive: S: -> Common -> Policies, Plans & Procedures

Website: www.lucascountyhealth.com/employee-login/

Hardcopy: Policies & Procedures Manual, HR Office

Archived Version(s):

Requisite Signatures


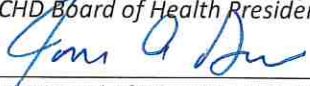





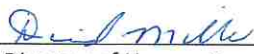
- 
 TLCHD Board of Health President Date 6-22-2017
- 
 FQHC Board of Directors President Date 6/22/17
- 
 Health Commissioner Date 06-28-17
- 
 FQHC CEO Date 6/22/17
- 
 Director of Nursing & Health Services Date 6-27-17
- 
 Privacy Officer Date 7/17/17
- 
 Security Officer Date 6-27-17
- 
 Director of Human Resources Date 6-27-17

Table of Contents

Section 1 – Administrative Requirements	12
1.1 Designation of Toledo-Lucas County Health Department as a Hybrid Entity	13
1.2 Designation of Privacy Official	14
1.3 General Staff Responsibilities	15
1.4 Training and Education	16
1.5 Submission of Complaints.....	18
1.5.1 Staff Submission of Potential Privacy Violations	18
1.5.2 Investigation of Potential Privacy Violations.....	18
1.6 Resolution of Complaints.....	20
1.6.1 Complaints Concerning Privacy Policies and Procedures	20
1.6.2 Complaints Arising from Potential Violations of Privacy Policies	20
1.6.3 Documentation of Complaints.....	21
1.7 Sanctions and Penalties	22
1.7.1 Technical Violations Not Involving Use or Disclosure	23
1.7.2 Unintentional Violations Involving Use and Disclosure	23
1.7.3 Intentional Violations Involving Use and Disclosure.....	23
1.8 Mitigation.....	24
1.9 Non-Retaliation and Protection for Whistleblowers	25
1.10 Development and Maintenance of Privacy Policies and Procedures	26
1.11 Documentation and Record Keeping.....	28
1.11.1 Retention of Records.....	28
Section 2 – Use and Disclosure of Protected Health Information	29
2.1 Use and Disclosure of Protected Health Information for Treatment Purposes	30
2.2 Use and Disclosure for Payment Purposes	31
2.3 Use and Disclosure for Health Care Operations	32
2.4 Use and Disclosure Outside the Practice	33
2.5 Use and Disclosure for Public Health Activities	34
2.5.1 Mandatory Reporting of Child Abuse.....	34
2.5.2 Mandatory Reporting of Abuse, Neglect, and Domestic Violence.....	34
2.5.3 Non-mandatory Reporting of Abuse, Neglect, and Domestic Violence	35
2.5.4 Disclosures to Schools Regarding Immunizations	35

2.6	Use and Disclosure for Specialized Government Functions	37
2.7	Use and Disclosure for Other Purposes	39
	2.7.1 Disclosure of Protected Health Information After Death	39
	2.7.2 Disclosure to Disaster Relief Agencies	39
	2.7.3 Disclosure to Coroners and Medical Examiners	39
	2.7.4 Disclosure to Funeral Directors	40
	2.7.5 Disclosure for Cadaveric Organ Donation	40
	2.7.6 Disclosure for Purposes of Research	40
	2.7.7 Disclosure to Avert a Threat to Health or Safety	41
2.8	Communications and Media Relations	42
	2.8.1 Internal Uses of Protected Health Information	42
	2.8.2 External Disclosures of Protected Health Information	42
2.9	Marketing and Fundraising	44
	2.9.1 Use and Disclosure for Marketing	44
	2.9.2 Use and Disclosure for Fundraising	44
2.10	Personal Representatives	46
	2.10.1 Designation of a Personal Representative	46
	2.10.2 Authority of Personal Representative	46
	2.10.3 Refusal to Recognize Personal Representative	46
2.11	Parental Access to Protected Health Information Concerning Children	48
2.12	Disclosure of Information to Family Members	49
2.13	Minimum Necessary Standard	50

Section 3 – Notice and Authorization..... 54

3.1	Notice of Privacy Practices	55
	3.1.1 Required Contents of Notice of Privacy Practices	55
	3.1.2 Providing the Notice of Privacy Practices to Patients	56
	3.1.3 Acknowledgement of the Notice of Privacy Practices	57
3.2	Authorization of Use or Disclosure	58
	3.2.1 Required Contents of Authorization for Use or Disclosure	58
	3.2.2 Obtaining Authorization for Use or Disclosure	59
	3.2.3 Refusal to Sign an Authorization for Use or Disclosure	60
	3.2.4 Revoking Authorization for Use or Disclosure	60
3.3	Patient Requests	62
	3.3.1 Patient Requests for Confidential Communications	62
	3.3.2 Patient Requests for Restrictions on Use and Disclosure	63
	3.3.3 Termination of Restrictions on Use and Disclosure	64

Section 4 – Patient’s Rights	65
4.1 Access to Protected Health Information.....	66
4.1.1 Requests for Access to Protected Health Information.....	66
4.1.2 Review of Requests for Access to Protected Health Information	67
4.1.3 Denial of Requests to Access Protected Health Information	68
4.1.4 Approval of Requests to Access Protected Health Information.....	68
4.2 Amendment of Protected Health Information	70
4.2.1 Requests for Amendment of Information.....	70
4.2.2 Review of Requests for Amendment of Information	70
4.2.3 Denial of Requests for Amendment of Protected Health Information.....	71
4.2.4 Approval of Requests for Amendment of Protected Health Information	72
4.3 Accounting for Disclosures of Protected Health Information.....	74
4.3.1 Requests for an Accounting of Disclosures of Protected Health Information.....	74
4.3.2 Information Provided in an Accounting of Disclosures of Protected Health Information.....	75
 Section 5 – Business Associates	 76
5.1 Business Associates.....	77
5.1.1 Business Associate Agreements.....	77
5.1.2 Contractual Breaches by Business Associates.....	78
5.1.3 Termination of Business Associate Contracts.....	79
 Section 6 – Security.....	 80
6.1 Designation of Security Official.....	81
6.2 Security Management Process	82
6.3 Risk Analysis	83
6.4 Risk Management	84
6.5 Sanction Policy	85
6.6 Information System Activity Review	86
6.7 Workforce Security	87
6.7.1 Authorization.....	87
6.7.2 Clearance.....	88
6.7.3 Termination Procedures.....	88
6.8 Information Access Management.....	90
6.8.1 Access Authorization.....	90
6.8.2 Access Establishment and Modification.....	90

6.9	Security Awareness and Training	91
6.10	Security Reminders	92
6.11	Protection from Malicious Software	93
6.12	Log-in Monitoring	94
6.13	Password Management	95
6.14	Security Incident Procedures	96
6.15	Contingency Plan	97
6.16	Data Back-up Plan	98
6.17	Disaster Recovery Plan	99
6.18	Emergency-mode Operation Plan	100
6.19	Testing and Revision Procedures	101
6.20	Applications and Data Criticality Analysis	102
6.21	Evaluation	103
6.22	Business Associate Contracts	104

Section 7 – Physical Safeguards 105

7.1	Facility Access Controls	106
	<i>7.1.1 Contingency Operations</i>	<i>106</i>
	<i>7.1.2 Facility Security Plan</i>	<i>106</i>
	<i>7.1.3 Access Control and Validation Procedures</i>	<i>106</i>
	<i>7.1.4 Maintenance Records</i>	<i>107</i>
7.2	Workstation Security	108
7.3	Device and Media Controls	109
	<i>7.3.1 Disposal</i>	<i>109</i>
	<i>7.3.2 Media Re-Use</i>	<i>109</i>
	<i>7.3.3 Accountability</i>	<i>109</i>
	<i>7.3.4 Data Backup and Storage</i>	<i>110</i>

Section 8 – Technical Safeguards 111

8.1	Access Control	112
	<i>8.1.1 Unique User Identification</i>	<i>112</i>
	<i>8.1.2 Emergency Access</i>	<i>112</i>
	<i>8.1.3 Automatic Logoff</i>	<i>112</i>
	<i>8.1.4 Encryption and Decryption</i>	<i>112</i>
8.2	Audit Controls	114
8.3	Integrity	115

8.4	Person or Entity Authentication.....	116
8.5	Transmission Security	117
	8.5.1 Integrity Controls	117
	8.5.2 Encryption.....	117
8.6	Business Associate Contracts/Agreements.....	118
Section 9 – Breach Notification.....		119
9.1	Discovery of Breach	120
9.2	Breach Discovery.....	121
9.3	Risk Assessment	122
9.4	Notification	123
9.5	Breach Information Log	125
Section 10 – Unique Identifiers.....		126
10.1	Patient Identifiers	127
10.2	Provider Identifiers	128
Section 11 – Transaction and Code Sets		129
11.1	Use of Standard Transactions	130
	11.1.1 Claim Submission and Coordination of Benefits.....	130
	11.1.2 Claims Status Inquiries.....	130
	11.1.3 Remittance Advice and Electronic Funds Transfer	130
	11.1.4 Referral Authorization.....	131
	11.1.5 Eligibility Transactions	131
	11.1.6 Health Plan Enrollment.....	131
	11.1.7 Premium Payment	131
11.2	Testing and Certification of Compliance with Federal Transaction Standards	132
11.3	Trading Partner Agreements.....	133
11.4	Updating Code Sets and Practices	134
	11.4.1 Diagnosis Coding	134
	11.4.2 Physician Services Coding	134
	11.4.3 Dental Services Coding.....	134
	11.4.4 Other Health-related Services Coding	134
	11.4.5 Drug Coding	134
Record of Change.....		135

Glossary of Terms

Access

The ability or means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

Authorization

A signed form containing prescribed elements required for specific and non-routine uses of protected health information.

Breach

The acquisition, access, use or disclosure of protected health information in a manner that compromises the security or privacy of the information to the point of posing a significant risk in financial, reputational or other harm to the individual.

If the following data elements are excluded when releasing protected health information, no breach has occurred:

1. Dates of birth;
2. Names;
3. Postal address information other than town or city, state and zip code;
4. Telephone or fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate or license numbers;
11. Vehicle identifiers and serial numbers;
12. Device identifiers and serial numbers;
13. Web universal resources locators (URLs);
14. Internet protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints;
16. Full face photographic images and other comparable images

Business Associate

A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right

Client Health Record

A complete, timely and accurate account of events, that must exist to provide evidence of services provided to fulfill purposes such as communication, continuity of care, research and education.

Code Set

Any set of codes used to encode data elements such as tables of terms, medical concepts, medical diagnostic codes or medical procedure codes. This includes both the codes and their descriptions. (i.e. ICD-10-CM).

Consent

A signed form containing prescribed elements required for all routine uses including treatment, payments and healthcare operations.

Covered Entity

A health plan, a health care provider, or health care clearinghouse that transmits any health information in electronic form relating to any covered transaction.

Health Plan – An individual or group plan that provides or pays for the cost of healthcare services

Health Care Provider – A provider of medical or other services, and any other person furnishing health care services or supplies; any person or organization that furnishes, bills or is paid for healthcare services in the normal course of business.

Health Care Clearinghouses – A public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements

Data Aggregation

With respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by a business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated Record Set

A group of records maintained by or for a covered entity that is:

1. The medical and billing records about individuals maintained by or for a covered health care provider;
2. For enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
3. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

For purposes of this rule, the term *record* means any item, collection, or grouping of information that includes PHI that is maintained, collected, used or disseminated by or for a covered entity.

Disclosure

The release, transfer, provision of access to, or any divulging of information outside the entity holding it

Electronic Media

Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, or digital memory card;

Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement or removable/transportable electronic storage media. Certain transmissions, including of paper via facsimile, and of voice via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic Protected Health Information (ePHI)

Information that comes within paragraphs 1(i) or 1(ii) of the definition of *Protected Health Information*

Encryption

The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process of key

Health Care

Prevention, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that which affects the structure or function of the body; and sale or dispensing of a drug, device, equipment or other item in accordance with prescription

Health Care Operations

Includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals; conduction of or arranging for medical review, legal services and auditing functions; business planning and development, and general business and administrative activities

Health Information

Any information, including genetic information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse; and
2. Relates to the past, present or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present or future payment for the provision or health care to an individual

Hybrid Entity

A single legal entity:

1. That is a [covered entity](#);
2. Whose business activities include both covered and non-covered functions; and
3. That designates health care components in accordance with [45 CFR 164.105](#)

Identifiers

Information about an individual, either taken alone or in combination, which may be used to identify the individual. This includes but is not limited to:

1. Names;
2. Geographic subdivisions smaller than a state, i.e. street address, city, county, precinct, zip code or geocode;
3. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people;
4. All elements of dates, except the year, for dates directly related to an individual;
5. Telephone numbers;
6. Fax numbers;
7. Electronic mail addresses;
8. Social security numbers;
9. Medical record numbers;
10. Account numbers;
11. Certificate or license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web universal resource locators (URLs), either personal or professional nature relating directly to a client;
15. Internet protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images; and/or
18. Any other unique identifying number, characteristic, or code

Individually Identifiable Health Information

Information that is a subset of health information, including demographic information collected from an individual, and is:

1. Created or received by a covered entity, public health authority, employer, life insurer, school or university;
2. Related to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and
 - i. Identifies the individual; or
 - ii. There is a reasonable basis to believe the information can be used to identify the individual

Investigation

A detailed inquiry or systematic examination; the process of inquiring into or following up; research; study inquiry

Minimum Necessary

The covered entity must make reasonable efforts to limit the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request for data

Payment

Activities undertaken to obtain or provide reimbursement for health care including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review

Personally Identifiable Information (PII)

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual

Personal Representative

A person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor; or the parent, legal guardian or other person acting *in loco parentis* who is authorized except where the minor is authorized by law, to consent on his or her own or via court approval, to a health care service; or where the parent, guardian or person acting *in loco parentis* has consented to an agreement or confidentiality between the provider and the minor.

Protected Health Information (PHI)

Individually Identifiable Health Information:

1. Except as provided in paragraph (2) of this definition, that is:
 - i. Transmitted by electronic media;
 - ii. Maintained in electronic media; or
 - iii. Transmitted or maintained in any other form or medium.
2. Protected Health Information excludes [Individually Identifiable Health Information](#):
 - i. In education records covered by the Family Educational Rights and Privacy Act
 - ii. In records described in 20 U.S.C 1232g(a)(4)(B)(iv);
 - iii. In employment records held by a covered entity in its role as employer; and
 - iv. Regarding a person who has been deceased for more than 50 years

Protected Personally Identifiable Information (Protected PII)

An individual's first name or first initial and last name in combination with any one or more of types of information including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed.

Public Health Authority

An agency or authority of the United States, a State, territory, a political subdivision of a State or territory, or an Indian Tribe; a person or entity acting under a grant from or in contract with such a public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Security

Ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss. Under HIPAA, this includes administrative procedures (access control, contingency planning), physical safeguards, technical security and network security measures (internet, dial-in-lines, etc.)

Subcontractor

A person to whom a [business associate](#) delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Transaction

Transmission of information between parties to perform health care related financial or administrative activities

Treatment

The provision, coordination, or management of health care and related services; consultation between providers relating to an individual, or referral of an individual to another provider for health care

Use

With respect to [individual identifiable health information](#), the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information

Violation

Failure to comply with an administrative simplification provision

Workforce

Employees, volunteers, trainees, and other persons who conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate

Section 1 – Administrative Requirements

1.1 Designation of Toledo-Lucas County Health Department as a Hybrid Entity

Policy

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and regulations promulgated thereunder by the United States Department of Health and Human Services establishes standards to protect the privacy of individually identifiable health information (the HIPAA Privacy Regulations). These Standards for Privacy are applicable to health care plans and to all persons and entities that are health care providers that transmit any health information in electronic form in connection with a transaction covered by the Privacy Rule.

The Toledo-Lucas County Health Department has determined that certain portions of its operations are obligated to comply with HIPAA and the HIPAA Privacy Regulations. Under the Privacy Rule, a single legal entity that engages in both covered and non-covered functions shall designate itself a [hybrid entity](#).

The Toledo-Lucas County Health Department hereby declares itself a hybrid entity and has established those portions of the single legal entity that will be required to comply with the Privacy Rule. The following are officially designated as covered components:

The Division of Health Services, its participating physicians and clinicians, and all department employees who provide management, administrative, financial, legal and operational support services to or on behalf of the Toledo-Lucas County Health Department to the extent that such employees use and disclose individually identifiable health information in order to provide administrative and support services and would constitute a “business associate” of the Toledo-Lucas County Health Department if separately incorporated.

All other employees and personnel of the department are excluded from the covered component.

Regulation

45 CFR 164.105

1.2 Designation of Privacy Official

Policy

It is the requirement of each organization to designate a privacy official responsible for development and implementation of privacy policies and procedures, and a contact to whom requests for additional information and complaints can be directed. It is the policy of the Toledo-Lucas County Health Department to appoint a Privacy Officer to fulfill these requirements.

Procedure

- A. The Privacy Officer is responsible for the development and implementation of policies and procedures to safeguard the privacy of patient's health information consistent with federal and state laws and regulations.
- B. The specific responsibilities of the Privacy Officer include:
 - 1. Developing procedures as provided in [Section 1.10](#)
 - 2. Developing and conducting training programs on privacy policies and procedures
 - 3. Responding to questions from staff and patients concerning the privacy policies and procedures
 - 4. Receiving complaints concerning the privacy practices described in the Notice of Privacy Practices
 - 5. Auditing compliance with privacy policies and procedures
 - 6. Investigating and correcting violations of privacy policies and procedures
- C. The Privacy Officer may assign any of these responsibilities to other staff members or contractors but is responsible for making sure these responsibilities are carried out.

Regulation

45 CFR 164.530(a)(1)

1.3 General Staff Responsibilities

Policy

It is the policy of the Toledo-Lucas County Health Department to create assurances that all staff and associates act in an appropriate and compliant manner to protect patient information.

Procedure

- A. All staff are responsible for safeguarding the privacy of patient health information. Specific staff responsibilities under these privacy policies and procedures will be listed in the staff member's job description. All staff members must:
1. Use and disclose protected health information only as authorized in their job description or as authorized by a supervisor
 2. Conduct oral discussions of personal health information with other staff or with patients and family members in a manner that limits the possibility of inadvertent disclosures
 3. Complete privacy training (see [Section 1.4](#))
 4. Report suspected violations of the policies and procedures established in this manual by staff members as detailed in [Section 1.5.1](#)
 5. Report suspected violations of a business associate's contractual obligations to safeguard protected health information (see [Section 5.1.2](#))
- B. The job description of all staff members who require routine access to protected health information to perform their job-related duties must identify:
1. The job functions that require the use or disclosure of protected health information
 2. The classes of protected health information the position will use or disclose
 3. Any restrictions on the protected health information the position can use or disclose
 4. Procedures to use or disclose protected health information not routinely available to the position
- C. These requirements may be satisfied by referring to standard job classes the Privacy Officer may establish under [Section 6.3](#) to define the positions authorized to routinely use or disclose standard categories or protected health information.

Regulations

45 CFR 164.514(d)(2)(ii)

45 CFR 164.530(c)(2)(ii)

1.4 Training and Education

Policy

All staff and associates will be trained on the HIPAA privacy regulations and our organization's privacy practices and any revisions in the policies will be communicated via refresher training.

Procedure

- A. The Privacy Officer, or a designated staff member, will develop a privacy policy orientation and training program.
- B. The purpose of this program is to make sure that all staff members are familiar with the privacy policies and procedures adopted by the Toledo-Lucas County Health Department.
- C. The training and orientation program will cover:
 1. The definition and identification of [protected health information \(PHI\)](#)
 2. Providing the Notice of Privacy Practices to all patients
 3. Obtaining a written acknowledgement of receipt of the notice
 4. Use and disclosure of PHI for treatment, payment, and health care operations
 5. How to obtain authorization, when required, for use and disclosure of PHI
 6. Procedures for handling suspected violations of privacy policies and procedures
 7. Penalties for violations of privacy policies and procedures
 8. Documentation required by the policies and procedures manual
- D. Staff members will:
 1. Receive a summary of the medical practice's privacy policies and procedures
 2. Have an opportunity to review the policies and procedures manual
 3. Have an opportunity to ask questions about the privacy policies and procedures
- E. All staff members must complete the privacy policy orientation and training program during their probationary period.
 1. Completion of the privacy policy orientation and training program will be documented in the employee's personnel file by the Privacy Officer or designated staff member who conducts training.
 2. Until staff members complete the privacy policy orientation and training program, their supervisors will closely monitor their use and disclosure of protected health information.
 3. Before the end of a staff member's probationary period, his or her supervisor should confirm that he or she has completed privacy training.
 4. The probationary period of any new employee who has not completed the privacy policy orientation and training program will be extended, and the employee will be ineligible for benefits that would have become available upon completion of the probationary period. In some cases, an employee who does not complete the privacy policy orientation and training program before the end of his or her probationary period will be required to complete the program before resuming normal job duties.

- F. If the privacy policies are revised, or if there is a change in regulations requiring additional training, the Privacy Officer, or designated staff member, will develop training materials on new or revised privacy policies and procedures.
1. Staff whose job responsibilities are affected by a change in privacy policies and procedures must complete training on the revised policies and procedures within one month of their effective date.
 2. Completion of training on revised policies and procedures will be documented in the employee's personnel file.

Regulation

45 CFR 164.530(b)

1.5 Submission of Complaints

Policy

To ensure that, in compliance with HIPAA regulations, there is a process by which complaints regarding potential privacy violations can be submitted for investigation.

Procedure

- A. A patient or other individual who wants to file a complaint concerning the agency's privacy policies and procedures, or a suspected disclosure of protected health information that violates state or federal law should:
 - 1. Be directed to the Privacy Officer for answers to questions about filing complaints.
 - 2. Receive a copy of the complaint form from the Privacy Officer, or another staff member, to be returned by mail to the address printed on the form, or in person to the Privacy Officer.

1.5.1 Staff Submission of Potential Privacy Violations

- A. Employees and associates will be responsible for reporting any suspected [violations](#) of privacy policies or procedures.
- B. All staff members should report possible violations of privacy policies and procedures to their supervisor. If the supervisor determines that a violation occurred or that the situation warrants further investigation, the possible violation should be reported to the Privacy Officer.
 - 1. Violations involving the staff member's supervisor should be reported directly to the Privacy Officer.
 - 2. Violations involving the Privacy Officer should be reported to the Director of Health Services.
- C. Staff members always have the right to contact the Department of Health and Human Services Office for Civil Rights directly as well, at OCRcomplaint@HHS.gov
- D. Reportable offenses include use and disclosure of protected health information that may violate:
 - 1. The practices described in the Notice of Privacy Practices form
 - 2. A patient's authorization
- E. Discussion of protected health information in public areas should be reported only if the discussion involves the disclosure of a substantial amount of protected health information and it would have been practical to conduct the discussion in a private area.
- F. The staff member reporting the violation should briefly describe the possible violation in writing or should arrange a meeting with the supervisor and/or the Privacy Officer to discuss the possible violation.

1.5.2 Investigation of Potential Privacy Violations

- A. All potential privacy violations will be [investigated](#) by the Privacy Officer or a delegate assigned by the Privacy Officer.

- B. Upon being notified of a potential violation of privacy policies and procedures by a staff member or patient, the Privacy Officer will:
1. Review any documentation
 2. Meet with the staff member or patient who reported the possible violation
 3. Meet with the staff member(s) who may have violated the policies and procedures
 4. Determine what, if any, protected health information was used or disclosed
 5. Determine whether the use or disclosure violated policies and procedures
 6. Determine whether the violation was accidental or intentional
 7. Recommend to the staff member's supervisor the disciplinary action, if any, that should be taken
 8. Document the findings of the investigation and action taken

Regulation

45 CFR 164.530(d)

1.6 Resolution of Complaints

Policy

To resolve every complaint raised by an individual. All potential violations of privacy will be investigated.

1.6.1 *Complaints Concerning Privacy Policies and Procedures*

- A. The procedures for resolving the complaints submitted by patients or other individuals concerning the privacy practices of the Toledo-Lucas County Health Department or the policies and practices established in this manual are outlined below:
1. Upon receiving a complaint, the Privacy Officer or designated staff member will review the complaint, evaluate the specific details of the complaint, and determine whether it warrants a change in the privacy policies or procedures.
 2. If a change appears to be warranted, the staff member conducting the evaluation will develop a recommendation and submit it to the Privacy Officer, who will then determine whether an immediate change in policies or procedures is needed to prevent the violation of federal or state privacy standards, laws, or regulations.
 3. If it is determined that a change in policies and procedures is necessary, a revised policy will be prepared following the procedures outlined in [Section 1.10](#).
 4. The Privacy Officer should prepare a response and send it to the individual submitting the complaint. The response should thank the individual for his or her interest. It should indicate that the suggestion has been evaluated and the agency believes that its current procedures comply with federal and state requirements.
 5. If a change does not appear to be warranted, the Privacy Officer will prepare a response and send it to the individual submitting the complaint. The response should thank the individual for his or her interest and indicate that the suggestion has been evaluated, but the agency believes that its current privacy procedures comply with federal and state requirements and are sufficient to protect patient privacy.
 6. Receipt of the complaint and its final disposition should be documented.

1.6.2 *Complaints Arising from Potential Violations of Privacy Policies*

- A. The procedures for resolving complaints submitted by patients or other individuals concerning the disclosure of [protected health information](#) are outlined below:
1. A staff member who receives a complaint from a patient or other individual that concerns a possible use or disclosure of protected health information that violates the agency's privacy policies and procedures, or that violates federal and state law, should immediately refer the complaint to the Privacy Officer.
 2. The Privacy Officer will review the complaint and determine whether a violation occurred and, if so, whether the violation involves only privacy policies and procedures or if it also involves a violation of federal and state privacy laws and regulations.

3. If the Privacy Officer determines that the complaint may involve a violation of federal or state standards and legal requirements, he or she will immediately forward the complaint to the Lucas County Prosecutor's Office for evaluation. The request for evaluation should specify a date by which the evaluation should be completed.
4. The Privacy Officer should follow up and track the status of the referral. If the evaluation indicates that federal or state standards may have been violated, the mitigation procedures established in [Section 1.8](#) should be followed.
5. If the Privacy Officer determines that the complaint does not involve a violation of federal or state standards or legal requirements, he or she will determine whether the privacy policies and procedures were violated.
6. If policies and procedures have been violated, the disciplinary procedures established in [Section 1.7](#) should be initiated.
7. The Privacy Officer should contact the person submitting the complaint and notify him or her of the actions being taken to address the complaint.
8. Evaluations of complaints should generally be completed within 30 days of a receipt.
9. The receipt of the complaint and the final disposition should be documented.

1.6.3 Documentation of Complaints

- B. The Privacy Officer will establish and maintain files containing documentation of all complaints received. This documentation will include the actions taken to address or resolve the complaint, including any written correspondence with the person submitting the complaint.

Regulation

45 CFR 160.410(b)(2)(ii)(A)

45 CFR 164.530(d)

1.7 Sanctions and Penalties

Policy

Following a full investigation, appropriate sanctions will be brought against employees and associates who have been found to have violated the privacy practices of the Toledo-Lucas County Health Department.

Procedure

- A. There are two types of violations of privacy policies and procedures:
1. Technical violations that do not result in the use or disclosure of protected health information
 2. Violations that do involve the use or disclosure of protected health information. There are two types of violations that involve use of disclosure:
 - i. Unintentional or accidental
 - ii. Intentional and deliberate
- B. Incidental disclosures of information, such as disclosures that occur when a patient asks a question in a public area, do not need to be reported, documented, or investigated. No sanction will be imposed for incidental disclosures of information. Staff members should, nevertheless, make reasonable efforts to minimize incidental disclosures.
- C. The severity of penalties varies with the type of violation. The most severe penalties apply to the intentional disclosure of protected health information in violation of policies and procedures. The least severe penalties apply to unintentional technical violations of policies that do not result in the disclosure of protected health information.
- D. Examples of violations include:
1. Technical Violations – When obtaining an authorization, a staff member fails to notice that the patient signed but did not date the authorization form
 2. Accidental Disclosure – Information on the wrong patient is accidentally sent to a third-party payer
 3. Intentional Disclosure – A staff member provides a drug company representative a list of patients with an identified medical condition without obtaining the patient’s authorization for this disclosure
- E. The Privacy Officer shall establish and maintain files that document all actions taken to impose sanctions under this section. This information shall include:
1. A description of, and documenting evidence for, the violation
 2. A statement clarifying the nature of the violation, specifically indicating whether it was technical or involved the use or disclosure of protected health information, and whether the violation of policies was accidental or intentional
 3. A description of the sanction that was imposed

- F. An unproven or unsubstantiated allegation of a violation of privacy policies and practices does not have to be documented.

1.7.1 Technical Violations Not Involving Use or Disclosure

- A. A staff member who commits a technical violation of privacy policies and procedures that does not result in any use or disclosure of protected health information will:
 - 1. Meet with his or her supervisor to review the policies and procedures that were violated
 - 2. Demonstrate to the satisfaction of the supervisor that he or she understands that policies and procedures that should be followed in similar circumstances
- B. The violation will be documented in the staff member's personnel file. A pattern of repeated technical violations, even if none result in the inappropriate use or disclosure of protected health information, may result in transfer to another position, suspension, or termination of the staff member.

1.7.2 Unintentional Violations Involving Use and Disclosure

- A. A staff member who unintentionally uses or discloses protected health information in violation of the privacy policies and procedure will:
 - 1. Meet with his or her supervisor to review the use or disclosure of protected health information that violated the policies and procedures or the staff member's authority to use or disclose information
 - 2. Demonstrate to the satisfaction of the supervisor that he or she understands the uses and disclosures that he or she is authorized to make under the agency's policies and procedures
- B. The violation will be documented in the staff member's personnel file. A pattern of repeated unauthorized use or disclosure of protected health information will result in transfer to another position, suspension, or termination of the staff member.

1.7.3 Intentional Violations Involving Use and Disclosure

- A. The intentional violation of privacy policies and procedures may result in immediate suspension, pending further investigation and termination.
- B. Documentation of the investigation of the violation must show clear evidence that the disclosure of information was intentional and deliberate. That is, the staff member must have disclosed the information knowing that the disclosure violated the policies and procedures of the agency.
- C. If the staff member has previously disclosed the same or similar type of information under the same or similar circumstances, it will be presumed that the disclosure was intentional and deliberate.

Regulation

45 CFR 164.530(e)

1.8 Mitigation

Policy

To mitigate, to the extent possible, any harmful effects resulting from the use or disclosure of protected health information that violates policies and procedures of the Toledo-Lucas County Health Department or the requirements of federal law.

Procedure

- A. When the Privacy Officer determines that a use or disclosure of protected health information has violated the policies and procedures established by this manual, the case will be referred to the Lucas County Prosecutor's Office to:
 - 1. Determine action needed to mitigate harm that may result to the patient
 - 2. Evaluate the agency's legal exposure and recommend a course of action
 - 3. Follow up with the patient

- B. All communications with the patient concerning use or disclosure of protected health information that legal counsel determines may violate federal or state standards and legal requirements should be handled by legal counsel.

Regulation

45 CFR 164.530(f)

1.9 Non-Retaliation and Protection for Whistleblowers

Policy

To ensure that no retaliatory action will be taken against patients, staff, or any others that bring to the organization's attention a potential privacy violation.

Procedure

- A. As an organization, the Toledo-Lucas County Health Department does not partake in any type of intimidation, threats, coercion, discrimination, or other retaliatory action against any persons that bring to the attention of the organization or the HHS OCR potential issues in privacy practices.
- B. Any issues brought directly to the Privacy Officer will be investigated, and appropriate sanctions will be applied in the event an issue is found.

Regulation

45 CFR 164.530(g)

1.10 Development and Maintenance of Privacy Policies and Procedures

Policy

The Toledo-Lucas County Health Department is responsible for developing and maintaining written privacy policies and procedures pursuant to the HIPAA privacy standards.

Procedure

- A. The Privacy Officer will develop policies and procedures that are reasonably designed to ensure compliance with federal and state standards for protection of the privacy of health information. The Privacy Officer may delegate this responsibility to a staff member, but such delegation must be reflected in that staff member's job description, and the Privacy Officer will supervise the development of all privacy policies and procedures.
- B. The Privacy Officer must:
 1. Monitor changes in federal and state law and regulations that may require changes in privacy policies and procedures.
 2. Notify the Toledo-Lucas County Board of Health of the issuance of new or revised federal or state requirements and describe the need to modify policies and procedures, including the date by which revised policies and procedures must be implemented.
 3. Take the initiative to develop new or revised policies and procedures as necessary to meet the requirements of new laws and regulations.
 4. Identify any revisions needed in the privacy orientation and training program to reflect revised policies and procedures.
- C. Before a revised policy or procedure is submitted for approval, the Privacy Officer will review the Notice of Privacy Practices form and determine whether the notice must be revised to reflect the new privacy policies or procedures.
- D. The effective date of a revised policy or procedure must not be earlier than the date on which the revised notice of privacy practices is posted and made available to patients.
- E. All policies and procedures must be approved by the Toledo-Lucas County Board of Health before they can be implemented.
- F. New or revised policies and procedures are to be communicated to staff through the following:
 1. An all-staff memorandum from the Privacy Officer will announce the adoption of the new or revised policies and indicate affected staff functions. This memorandum should describe the new policy, indicate its effective date, and indicate the date on which the new policy will be available for staff review.
 2. The Privacy Officer or a designated representative will announce the adoption of the new policies at appropriate staff meetings and provide appropriate training.

3. A memorandum from the Privacy Officer to those staff members whose job responsibilities are directly affected by the new policies should indicate whether training or orientation meetings or programs will be held and whether background information on the new policies is available.
4. A copy of the revised policy should be attached to the memorandum, or staff should be directed to consult the updated policy and procedure manual.
5. Copies of the revised policy will be distributed to staff members for updating their copies of the policy manual.

Regulation

45 CFR 164.530(i)

1.11 Documentation and Record Keeping

Policy

To establish and maintain systems for maintenance of documentation under the HIPAA privacy regulations. Documentation will be retained for the appropriate timeframes based on the regulations.

Procedure

- A. The Privacy Officer will establish and oversee record-keeping systems to maintain the documentation required by the HIPAA privacy regulations as discussed in this manual.
- B. The information to be maintained in written documentation includes, but is not limited to:
 - 1. The policies and procedures contained in this policy manual
 - 2. The Notice of Privacy Practices and the signed acknowledgement of receipt of the notice
 - 3. Signed authorization forms
 - 4. Records of disciplinary actions against staff members for violations of privacy policies/procedures
 - 5. Records of actions taken to enforce compliance with contract provisions by business associates
 - 6. Complaint forms received from patients or other individuals and associated written correspondence
 - 7. Requests for an accounting of disclosure of protected health information and related records
 - 8. Requests for amendment of protected health information and related records

1.11.1 Retention of Records

- A. All documentation of actions called for by other policies and procedures contained in this manual will be retained for a minimum of six years from the date the information was created.
- B. In the case of policies and procedures, the six-year retention period will be measured from the date of the most recent version of the policy. In other words, when the new policies are issued, a copy of the policies that are superseded should be retained for reference purposes for six years following the last day the policy was in effect.

Regulation

45 CFR 164.530(j)

Section 2 – Use and Disclosure of Protected Health Information

2.1 Use and Disclosure of Protected Health Information for Treatment Purposes

Policy

The Toledo-Lucas County Health Department uses protected patient information pursuant to its Notice of Privacy Practices and under the guidance of the HIPAA privacy regulations for purposes of patient treatment. The use and disclosure of information for the purpose of treatment does not require specific authorization.

Procedure

- A. The [use](#) of information for [treatment](#) purposes is described in the [Notice of Privacy Practices](#).
- B. Before nonemergency treatment is initiated, an effort must be made to obtain the patient's written acknowledgement of having received the Notice of Privacy Practices.
- C. Obtaining the written acknowledgment is the responsibility of the front desk staff.
- D. If the patient's acknowledgment cannot be obtained, the attempt to obtain an acknowledgment should be documented in writing.
- E. Procedures for obtaining the acknowledgment are described in [Section 3.1.3](#).

Regulations

45 CFR 164.506

45 CFR 164.520(c)

2.2 Use and Disclosure for Payment Purposes

Policy

The Toledo-Lucas County Health Department uses protected patient information pursuant to its Notice of Privacy Practices and under the guidance of the HIPAA privacy regulations for purposes of [payment](#) purposes. The use and disclosure of information for payment purposes does not require specific authorization, but only the [minimum necessary](#) amount of information must be made available.

Procedure

- A. [Use](#) and [disclosure](#) of protected health information is permitted under this policy to conduct the following activities:
 - 1. Providing information to the patient's health plan to determine eligibility for benefits and coverage
 - 2. Submitting a claim for services to the patient's health plan
 - 3. Processing credit card transactions or transactions to obtain authorization for personal checks
 - 4. Providing information needed by the patient's health plan to conduct a medical review
- B. Before seeking payment for nonemergency treatment, a patient must be given the Notice of Privacy Practices and a written acknowledgment of receipt must be obtained. Obtaining the acknowledgment is the responsibility of the front desk staff.
- C. Procedures for obtaining an acknowledgment are described in [Section 3.1.3](#).
- D. Use and disclosure of protected health information for payment purposes is limited to the information that can be transmitted using the standards for electronic transactions. These restrictions apply whether the transaction is conducted electronically or using paper forms.

Regulations

45 CFR 164.502(b)(2)(vi)

45 CFR 164.506

45 CFR 164.520(c)

2.3 Use and Disclosure for Health Care Operations

Policy

The Toledo-Lucas County Health Department uses protected patient information pursuant to its Notice of Privacy Practices and under the guidance of the HIPAA privacy regulations for purposes of [health care operations](#). The use and disclosure of information for health care operations-related activity does not require specific authorization, but only the [minimum necessary](#) amount of information must be made available.

Procedure

- A. [Use](#) and [disclosure](#) of protected health information is permitted under this policy to conduct the following activities:
1. Quality assessment and improvement
 2. Professional credentialing
 3. Medical and utilization review
 4. Legal Services
 5. Auditing
 6. Business planning and market research
 7. Grievance procedures
 8. Due diligence analysis related to sales and acquisitions
 9. Creation of de-identified information and limited data sets
 10. Customer service
 11. Compilation of patient directories
 12. Compliance monitoring
- B. Before using or disclosing protected health information for any of the functions included in health care operations, the medical practice must give the patient its Notice of Privacy Practices.
- C. Obtaining an acknowledgement of receipt of the notice is the responsibility of the front desk staff.
- D. Procedures for obtaining an acknowledgment are established in [Section 3.1.3](#).

Regulations

45 CFR 164.506

2.4 Use and Disclosure Outside the Practice

- A. When a provider, who is not a member of the practice, contacts a staff member and requests information for the purposes of treating a patient previously treated at the Toledo-Lucas County Health Department, the staff member may provide information without restriction. It is not necessary for the patient to authorize the disclosure of protected health information that will be used for the purpose of treatment.
- B. When disclosing information to another provider for purposes of payment, staff members should use the following procedure:
 - 1. A patient may have requested and been granted restrictions on the use or disclosure of protected health information. Staff members should review the patient's records to determine if any restrictions have been placed on the use or disclosure of protected health information.
 - 2. Before disclosing information for treatment purposes, a medical practice staff member must verify the identity of the person making the request. In other words, the staff member must determine that the person making the request is, in fact, a health care professional who is requesting information for the purpose of treatment.
 - 3. If the professional requesting information is known to the practice, is a member of a group that is known to a staff member, or is affiliated with a facility that is known to the practice, a staff member may presume that the provider is who he or she claims to be. Otherwise, a staff member should obtain additional assurances sufficient to satisfy his or her professional judgment that the person requesting the information is a health care provider who will use the information for purposes of treatment.
 - 4. Protected health information should be sent only to the verified business address of the provider requesting it.
- C. When a staff member requires information on a patient's health condition from another provider, he or she may request the information without restriction. The patient need not authorize this request.
- D. The information requested must, however, be used for the purpose of evaluating the patient's medical condition or determining a course of treatment.
- E. A patient may have been granted a restriction on the information that is to be used or disclosed to other providers. In this situation, the restrictions must be honored.

Regulation

45 CFR 164.502(b)(2)

45 CFR 164.514(d)(4)

45 CFR 164.514(h)(1)

2.5 Use and Disclosure for Public Health Activities

Policy

Use and disclosure of patient information will be reported to the appropriate [Public Health Authority](#) as required by law. Patient authorization is not required, however, under certain circumstances the patient must be notified that the information has been disclosed.

Procedure

- A. The following information may be reported to the appropriate public health agency as required by law, whether or not the patient authorizes the disclosure:
 - 1. Information required to compile vital statistics (births and deaths)
 - 2. Information on communicable diseases pursuant to Ohio Administrative Code 3701-3
 - 3. Information on reportable injuries
- B. Staff may disclose protected health information to government agencies which are responsible for administering public health programs such as Medicare and Medicaid, and for licensing providers, conducting audits, and for other purposes related to the oversight of the health system.
- C. Staff members should refer requests for protected health information received from oversight agencies to the Privacy Officer.
- D. The Privacy Officer will review requests for protected health information and obtain legal opinion if he or she believes one is necessary before approving the disclosure of the requested information.

2.5.1 *Mandatory Reporting of Child Abuse*

- A. In accordance with Ohio Revised Code (ORC) 2151.421, the medical practice must report cases of suspected child abuse or neglect to Lucas County Children Services.
 - 1. Under this section, a child is defined as a person under eighteen years of age, or a mentally retarded, developmentally disabled, or physically impaired child under twenty-one years of age.
- B. Reports must be made by telephone or in person and shall be followed by a written report, if requested by the receiving agency or officer. The written report must include:
 - 1. The child's name, address and age;
 - 2. The names and addresses of the parents or the person or guardians, if known;
 - 3. The nature of the injuries, abuse, or neglect that is known or reasonably suspected; and
 - 4. Any other information that might be helpful.

2.5.2 *Mandatory Reporting of Abuse, Neglect, and Domestic Violence*

- A. Staff must report suspected abuse, neglect, or domestic violence to the proper agency, as required by law even if the patient does not authorize the disclosure. Only the types of information that are required by law should be disclosed. The following situations should be reported immediately:

1. Any known or suspected abuse, neglect, or exploitation of an adult, in accordance with ORC 5101.61, to the Lucas County Department of Job and Family Services at 419-213-8663.
 - i. Reports shall be made orally or in writing, except that oral reports should be followed by a written report if a written report is requested by the department. The written report should include:
 - The name, address, and approximate age of the adult;
 - The name and address of the individual responsible for the adult's care;
 - The nature and extent of the alleged abuse, neglect, or exploitation; and
 - The basis of the belief that abuse, neglect, or exploitation has occurred.
2. Any known or suspected abuse or neglect of a person with mental retardation or a developmental disability, in accordance with ORC 5123.61, to the Lucas County Board of Developmental Disabilities at 419-381-5206 (during business hours), or 419-380-5100 (after business hours). You may also call the Ohio Department of Developmental Disabilities hotline at 1-866-313-6733.
 - i. Reports shall be made by telephone or in person and shall be followed by a written report. The reports should contain the following:
 - The name, age, and address of the suspected victim;
 - The names and addresses of the person's custodian(s), if known; and
 - Any other information that would assist in the investigation of the report.

2.5.3 Non-mandatory Reporting of Abuse, Neglect, and Domestic Violence

- A. Staff may report cases of suspected abuse or neglect to local law enforcement without the agreement of the patient if the following criteria are met:
 1. It is believed that the report may prevent serious injury to the patient or others.
 2. The disclosure is permitted under federal or state law.
- B. Disclosure of information should be restricted to only information that can be disclosed legally.
- C. The patient must be informed of any disclosure of protected health information unless it is believed that informing the patient may lead to serious harm for the patient or another person or unless state law prohibits such notification.
- D. If it is not possible to inform the patient, the patient's personal representative must be informed of the disclosure unless it is believed that informing the representative may lead to serious harm for the patient or another person.

2.5.4 Disclosures to Schools Regarding Immunizations

- A. Staff may disclose information regarding immunizations about a patient that is a student or a prospective student at an educational institution, if those immunizations are required by the State or other law for admission.

B. Certain requirements must be met in order to provide this information to the educational institution, including:

1. A request must be made from the educational institution, parent, guardian, or patient
2. The information provided to the school is limited to proof of the immunizations required
3. The school must be required by State or other law to have proof of these immunizations on file prior to admission of this student
4. The parent, guardian, or the individual themselves (if they are of age or an emancipated minor) must agree to the disclosure and this must be documented by the practice

Regulation

45 CFR 164.512

2.6 Use and Disclosure for Specialized Government Functions

Policy

The Toledo-Lucas County Health Department may use and disclose protected health information without written patient authorization for specialized government functions as described in this section.

Procedure

A. Specialized government functions are:

1. Certain military and veterans activities, as required by the federal government
2. National security and intelligence activities
3. Protective services for the President of the United States and others as authorized by law
4. Certain medical suitability determinations
5. A correctional institution or other law enforcement custodial situations
6. Government programs providing and/or administering public benefits

B. The staff may:

1. Use and disclose information as appropriate to support military missions if appropriately directed by federal government agencies.
2. Disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities authorized by law.
3. Disclose protected health information requested by law enforcement agencies without obtaining the patient's authorization.

C. Staff members may report:

1. Any information requested by a subpoena, court order, or summons.
2. The name and address, date and place of birth, Social Security number, ABO blood type and Rh factor, type of injury, date and time of treatment or death, and a description of physical characteristics when requested by a law enforcement official. Staff may not report other information such as information related to DNA or DNA analysis, dental records, tissue typing, or the analysis of body fluids or tissues without a court order, subpoena, or summons.
3. Protected health information concerning the victim of a crime, but only with the agreement of the victim or when a law enforcement office indicates that the information is needed to investigate suspected criminal activity.
4. Protected health information that is evidence of criminal conduct on the premises of practice.
5. Protected health information concerning emergency treatment when the disclosure is necessary to alert law enforcement agencies to the commission of a crime, the location of the victim(s) of a crime, or the identity, description, or location of a suspected perpetrator of a crime.

D. Staff members should refer requests for protected health information received from law enforcement agencies to the Privacy Officer. The Privacy Officer will review requests for protected health information and

obtain a legal opinion if he or she believes one is necessary before approving the disclosure of the requested information.

- E. In regards to a judicial or legal action, staff members may disclose protected health information for use under the following circumstances:
 - 1. It has been requested in a court order or an order of an administrative tribunal.
 - 2. It has been requested by means of a subpoena, discovery request, or other legal process.

- F. Before responding to the request, efforts should be made to ensure that disclosure is limited to the minimum protected health information specifically requested and that one of the following assurances is obtained:
 - 1. The party seeking the protected health information has made a good-faith effort to provide a written notice to the subject of the request, has provided sufficient information to the subject of the request to permit the individual to object to the disclosure, and has resolved any objections that may have been raised.
 - 2. The party seeking the protected health information provides written documentation that is has entered into or otherwise obtained a qualified protective order that a) prevents the parties to the legal action from using or disclosing protected health information for any purpose not related to the litigation or legal proceeding for which the information was requested, and b) requires the return or destruction of the protected health information at the conclusion or the proceeding.

- G. Unless a request is referred by the Privacy Officer, staff members should refer requests for protected health information from law enforcement agencies to the Privacy Officer. The Privacy Officer will notify and seek legal guidance from legal counsel on how to respond to the request. Before responding, the Privacy Officer will obtain the assurances described in this policy.

Regulations

45 CFR 164.512(d)

45 CFR 164.512(e)

45 CFR 164.512(f)

45 CFR 164.512(k)

2.7 Use and Disclosure for Other Purposes

Policy

The Toledo-Lucas County Health Department will make protected health information available as appropriate under the HIPAA privacy regulations.

2.7.1 Disclosure of Protected Health Information After Death

- A. The protected health information of a deceased individual will be handled according to the policies and procedures applied to the protected health information of living patients.
- B. The death of a patient does not reduce the privacy protections that his or her protected health information will receive until 50 years after his or her death. At that point, health information is no longer considered protected health information unless specifically protected by a law other than HIPAA.

Regulation

45 CFR 164.502(f)

2.7.2 Disclosure to Disaster Relief Agencies

- A. Information on a patient's location, medical condition, or death may be disclosed to disaster relief organizations such as the Red Cross and other public or private organization.

Regulation

45 CFR 164.510(b)(4)

2.7.3 Disclosure to Coroners and Medical Examiners

- A. Staff may disclose protected health information without the patient's authorization to a coroner or medical examiner who requests the information for the following purposes:
 - 1. Identification of a deceased person
 - 2. Determination of the cause of death
 - 3. Other purposes specified in state or federal law
- B. The credentials of the coroner or medical examiner making the request should be verified. If the request is made in person, staff should ask to be shown an official identification. If the request is made by telephone, staff should ask that the request be submitted in writing and should obtain the official address to which information should be sent.
- C. Staff should confirm that the information is being requested by the coroner or medical examiner for use in establishing the identity of a deceased person or determining the cause of death.
- D. The requested information should only be sent to the office address of the coroner or medical examiner.

Regulation

45 CFR 164.512(g)(1)

2.7.4 Disclosure to Funeral Directors

- A. A staff member may disclose protected health information that a funeral director requests for the purpose of preparing a body for burial or cremation.
- B. Staff should attempt to obtain the permission of the patient or patient's representative before disclosing requested information, but permission is not required.
- C. Only the information that a funeral director is entitled to request under state laws should be disclosed.
- D. The funeral director should be asked to submit a request for the specific information that is required in writing. This request may be faxed, but should identify the funeral director by name and address.
- E. An attempt should be made to contact the patient's representative or a close family member (spouse, child, or other family member) or close personal friend who has been involved in the patient's treatment for permission to disclose the requested information.
- F. The information that has been requested should only be sent to the business address of the funeral director.

Regulation

45 CFR 164.512(g)(2)

2.7.5 Disclosure for Cadaveric Organ Donation

- A. Following the death of a patient, a medical practice may disclose protected health information to an organ procurement organization such as an eye bank or tissue bank without the patient's prior consent or authorization, and without obtaining authorization of the patient's representative.
- B. Staff may not disclose this information if a patient or the patient's representative has indicated that he or she does not want to donate organs or tissue, or if the patient has imposed a restriction on the disclosure of protected health information for this purpose.

Regulation

45 CFR 164.512(h)

2.7.6 Disclosure for Purposes of Research

- A. Use and disclosure of information for purposes of research is allowable under the rule with authorization from the patient. In some instances, it is also allowable without specific signed authorization.
- B. A staff member may provide a researcher with protected health information in the following instances:
 - 1. With a signed authorization from the patient (sometimes found within the informed consent form for the research study)
 - 2. With a HIPAA waiver from the applicable institution review board or privacy board
 - 3. When a data use agreement is in place with the researcher and there is a limited data set provided to the researcher, as described in the data use agreement

4. If the information has been de-identified

Regulation

45 CFR 164.512(i)

2.7.7 Disclosure to Avert a Threat to Health or Safety

- A. Staff members may disclose protected health information without the patient's authorization if, in his or her professional judgment, such disclosure is necessary to reduce a serious and imminent threat to the health and safety of a person or the public.
- B. Information may be disclosed only to a person who is able, in the judgment of the staff member, to prevent or lessen the threat.
- C. If the patient has threatened to harm or injure another person or persons, that threat may be disclosed to the person(s) identified by the patient as the target(s).
- D. If the patient has admitted that he or she has participated in a violent crime, that admission may be disclosed to law enforcement agencies.
 1. Staff members may not disclose information related to participation in a violent crime if that information is learned in the course of treatment, counseling, or therapy for a propensity to engage in the criminal conduct, or if the patient has disclosed criminal activity while requesting referral for treatment, counseling, or therapy of such a propensity.
- E. If the staff member has reason to believe, based on all circumstances, that the patient has escaped from a correctional facility or lawful custody, the staff member may disclose that belief to law enforcement agencies.

Regulation

45 CFR 164.512(j)

2.8 Communications and Media Relations

Policy

To ensure that all employees and associates who engage in communications and media relations activities on behalf of the organization do so in a manner compliant with the HIPAA privacy regulations.

2.8.1 *Internal Uses of Protected Health Information*

A. Interviews and Articles

1. When writing articles or stories that are printed in publications circulated within the Toledo Lucas County Health Department, staff members may contact the individual or a health care provider to access the individual, to obtain a signed consent from the individual allowing the Toledo Lucas County Health Department to interview him or her and to obtain information for the article or story.

B. Patient Satisfaction Surveys

1. Quality assessment and improvement activities are considered health care operations under the privacy regulations.
2. To conduct patient satisfaction surveys, which are quality assessment and improvement activities, the Toledo Lucas County Health Department must state in its notice that it may use protected health information for health care operations.
3. If the department uses a vendor to conduct patient satisfaction surveys on behalf of the agency, there must be a business associate agreement in place.

Regulations

45 CFR 164.506

45 CFR 164.512

2.8.2 *External Disclosures of Protected Health Information*

A. Media Inquiries

1. Facility directories may contain the following information about an individual:
 - i. Name
 - ii. Location in the facility
 - iii. Condition of the individual in non-specific terms such as Good, Fair, Critical
 - iv. Religious affiliation
2. Individuals must be given the opportunity to restrict or prohibit the use of protected health information for facility directories and inform the individual that the agency may disclose this information to the media.
3. If the individual is incapacitated or deceased, or there is an emergency treatment situation, the department may use or disclose some or all of the protected health information in the facility directory if such use or disclosure is consistent with a prior expressed preference, or if such use and

disclosure is considered in the best interest of the individual. The agency must inform the individual of the use or disclosure when it is practical to do so.

4. When media does not know an individual's name, but gives other identifying information such as location or address of an accident, the agency may disclose non-patient specific information, such as age and gender, in addition to the condition of the individual.
5. If media requests information about an individual by name, subject to that individual's objection, the agency may release the information contained in the facility directory.

B. Media Requests for Interviews and/or Articles

1. Physicians, other health care providers and/or media relations personnel who provide protected health information about individuals to be included in an article or story must obtain the individual's written authorization before making such a disclosure.

C. Photographs, Videotapes, or Other Images

1. An individual's written authorization must be obtained before photographing or videotaping that individual for medical education, staff education, or publicity purposes.
2. If the individual's written authorization specifically allows the reuse of the information described above, the information may be reused in accordance with the authorization.
3. If the authorization does not specifically allow for the reuse of information, the information may not be reused.

Regulations

45 CFR 164.506

45 CFR 164.510(a)

45 CFR 164.512

2.9 Marketing and Fundraising

Policy

The Toledo Lucas County Health Department may not inappropriately use protected patient information for marketing or fundraising and will provide all patients an ability to opt out of all marketing and fundraising communications.

2.9.1 Use and Disclosure for Marketing

- A. The following types of marketing communications do not require authorization:
1. Communication to members of health plans that describe the medical practice, its members, and the services that are available from the practice, unless financial remuneration is provided to the practice for the communication.
 2. Communications to a patient as part of the patient's treatment that are specific to the medical condition of the patient, unless financial remuneration is provided to the practice for the communication.
 3. Communications from the patient's health plan during treatment for the purpose of altering the patient to the availability of alternative treatments, therapies, health care providers, or treatment settings, unless financial remuneration is provided to the practice for the communication.
 4. Face-to-face communications between staff members and patients during a patient visit.
 5. Promotional gifts of nominal value such as pens, note pads, or coffee mugs.
- B. Patients must specifically authorize the use of protected health information collected or maintained by the medical practice for a communication that is sent to the individual describing a product or service offered by an organization other than the medical practice.
1. Examples include mailings by pharmaceutical companies, retail pharmacies, health clubs, and suppliers of unrelated medical services such as durable medical equipment.
- C. Any communications that involve direct or indirect remuneration to the provider require authorization from the patient, even if they are describing a health-related product or service provided by the organization itself.

Regulations

45 CFR 164.501

45 CFR 164.514(e)(1)

2.9.2 Use and Disclosure for Fundraising

- A. The following information may be used to support the efforts to raise funds that directly benefit the medical practice without the patient's authorization:
1. Demographic information (i.e., date of birth, sex, marital status, address)
 2. The dates on which the patient received health care services from the medical practice

3. Department in which the service was provided
 4. The treating physician
 5. Information about patient outcome
 6. Health insurance status
- B. Other protected health information may not be used in fundraising activities without the patient's authorization. That is, the patient's authorization is required for the use of any protected health information except those items found in the list above.
- C. Fundraising appeals sent to individuals must include the following paragraph describing how the individual may opt out of further fundraising communications:
1. To be removed from future fundraising appeals, please call [###-###-#### ext.###] and ask to be removed from our fundraising mailing list, or check off the box asking to be removed from our fundraising mailing list on the reply card and return it to the office by dropping it in a mailbox.
- D. Protected health information may not be used to support fundraising on behalf of other organizations (that is, for raising funds that do not benefit the practice directly), without the patient's authorization.

Regulation

45 CFR 164.514(f)(1)

2.10 Personal Representatives

Policy

To ensure the Toledo Lucas County Health Department recognizes personal representatives as required by the HIPAA privacy regulations. A [personal representative](#) may act on behalf of the patient for the purposes of authorizing use and disclosure of protected health information, or receiving information that otherwise would be sent to the patient.

2.10.1 Designation of a Personal Representative

- A. A personal representative may be the spouse, adult child, or other member of the patient's family. A personal representative also may be a close personal friend, or any individual with power of attorney or other legally recognized authority to make medical decisions on behalf of the patient if he or she is incapacitated or otherwise unable to make decisions.
- B. A patient may designate a personal representative in writing. However, a person who is identified in the patient record as having medical power of attorney or other legal authority to act on behalf of the patient will be recognized as a personal representative.
- C. A parent or legal guardian of an unemancipated minor (generally a child under the age of 18) will be recognized as a personal representative of the child.
 - 1. A staff member should ask the patient to identify an individual or individuals who may act as the patient's personal representative on the acknowledgment form.
 - 2. If a patient becomes incapacitated, a person accompanying the patient will be recognized as the patient's personal representative if he or she can present evidence of having legal power of attorney or other legally binding authority to make medical decisions on behalf of the patient.
 - 3. The parent or legal guardian of an unemancipated minor will be recognized as the personal representative of a child, subject to restrictions contained in [Section 2.11](#).

2.10.2 Authority of Personal Representative

- A. If a patient is incapacitated, a personal representative may sign any form (such as authorization, revocation of authorization, and request for access to information), the uses of which are described in these policies.
- B. A personal representative may receive protected health information concerning the patient necessary to carry out the representative's legal duties to the patient (for example, providing an informed consent to treatment, or for enforcing an advance directive concerning life support).

2.10.3 Refusal to Recognize Personal Representative

- A. A medical practice staff member may refuse to disclose information to a person identified as a patient's personal representative if the staff member believes that disclosing such information may endanger the patient.
 - 1. A medical practice staff member who believes that disclosing information to a personal representative may endanger the patient should notify the Privacy Officer.

2. Requests from the personal representative for information concerning the patient should be referred to the Privacy Officer.

Regulation

45 CFR 164.502(g)

2.11 Parental Access to Protected Health Information Concerning Children

Policy

To ensure the Toledo Lucas County Health Department properly recognizes a parent or guardian as a child's personal representative. This policy also establishes restrictions to that authority as required by the HIPAA privacy regulations.

Procedure

- A. A parent, guardian, or other person recognized by state law as acting in loco parentis on behalf of a patient who is an unemancipated minor will be recognized as the patient's personal representative. In this policy, "parent" refers to a parent, guardian, or other person acting in loco parentis.
- B. A parent may act as a personal representative unless state or other law permits the minor to request that information not be shared with the parent.
- C. Generally, a medical practice will require a parent or legal guardian's signature on any authorization forms for a minor patient unless the patient requests that his or her parents not be notified.
 - 1. The Privacy Officer should review any minor's request for confidentiality pertaining to the use or disclosure of protected health information that relates to the parent or guardian, to determine whether the request complies with state and federal laws.

Regulation

45 CFR 164.502(g)(3)

2.12 Disclosure of Information to Family Members

Policy

Protected health information concerning a patient may be disclosed to a family member, other relative, or close personal friend of the individual who requires the information to assist in the patient's care and treatment.

Procedure

- A. If the patient is able to do so, he or she must agree to the sharing of this information before it occurs. Patients should generally be asked whether the information may be shared with family members. However, permission can be assumed if the patient has an opportunity to object to disclosure of information to family members and does not do so.
- B. If the patient is incapacitated, staff members may exercise their professional judgment in determining when it is in the patient's best interest to disclose protected health information to the family member.
- C. The information that may be disclosed to a family member, relative or close personal friend is limited to information directly relevant to the family member's involvement in the patient's care.
- D. If possible, disclosure of information to others should occur when the patient is present, or after the patient has agreed to the disclosure.
- E. If the patient is present or available for consultation concerning the disclosure, he or she should be given an opportunity to object to the disclosure. If the patient objects to the disclosure, the information should not be disclosed.
- F. If the patient is not present or available for consultation, or is incapable of agreeing or objecting to the disclosure, the attending physician should exercise his or her best professional judgment to determine whether the disclosure is in the best interest of the patient.
- G. If the patient agrees to the disclosure or the disclosure is determined to be in the best interest of the patient, only that information that is directly relevant to the family member's involvement in the patient's care should be disclosure.

Regulations

45 CFR 164.502(g)(2)

45 CFR 164.510(b)(1)(i)

2.13 Minimum Necessary Standard

Policy

The Toledo-Lucas County Health Department staff routinely uses protected health information about patients to carry out their duties. Staff may also need to disclose protected health information about patients to persons outside the agency or to request protected health information from these persons. The Toledo-Lucas County Health Department staff must limit their uses, disclosures, and requests of protected health information to the minimum amount of information necessary to accomplish the purpose of the use, disclosure, or request.

Procedure

A. This policy does not apply to the following types of uses, disclosures, and requests:

1. [Section 2.1 Use and Disclosure of Protected Health Information for Treatment Purposes](#)
2. [Section 2.4 Use and Disclosure Outside the Practice](#) (for treatment purposes)
3. [Section 2.5 Use and Disclosure for Public Health Activities](#)
 - i. Using or disclosing protected health information required by law
4. [Section 2.6 Use and Disclosure for Specialized Government Functions](#)
5. [Section 2.10 Personal Representatives](#)
6. [Section 3.2 Authorization of Use and Disclosure](#)
 - i. Using or disclosing patient information pursuant to a patient's written authorization permitting such use or disclosure
7. [Section 11.1 Use of Standard Transactions](#)
 - i. Using or disclosing protected health information in order to complete standardized electronic transactions, as required by HIPAA.
8. Using or disclosing protected health information as required for compliance with the HIPAA privacy regulations.

B. Routine Uses, Disclosures, and Requests

1. All individuals shall have access to the information required to carry out their responsibilities.
2. The agency shall have a process in place to designate the amount of access employees in each functional area should have based on the flow of protected health information within the organization and what information is required in order to carry out certain responsibilities, including procedures for establishing and monitoring access.
3. Supervisors in each functional area are responsible for establishing guidelines for access to protected health information, which will be made available to the Privacy Officer upon request.
4. Such guidelines will be reviewed periodically.
5. The Security Officer is responsible for establishing guidelines for access to [electronic protected health information](#).

6. Employees are required to maintain the confidentiality of all protected health information whether electronic, oral or written, to which he or she may be exposed either during the course of his or her duties or as a result of [incidental disclosure](#).
 - i. The duty of privacy protection continues during non-working hours and after the employee is no longer associated with the Toledo-Lucas County Health Department.
7. Employees are required to be trained on all applicable access guidelines and restrictions consistent with the minimum necessary standard.
8. Employees should contact the Privacy Officer if there is a question regarding the amount of access that is appropriate for the performance of certain functions.

C. Non-Routine Uses of Protected Health Information

1. Staff are instructed to notify the Privacy Officer if they believe they need to use protected health information in a way that is not addressed in this policy.
2. The Privacy Officer should follow ethical and industry guidelines regarding the use of patient information for treatment purposes when making this decision, and should balance the agency's desire to provide quality care and to obtain reimbursement for that care with the patient's interest in privacy.
3. If there is insufficient time to consult with the Privacy Officer without jeopardizing patient care, the staff member should consider these factors and notify the Privacy Officer as soon as possible afterwards.

D. Non-Routine Disclosures of and Requests for Protected Health Information

1. Employees are instructed to notify the Privacy Officer if they believe they need to disclose or request protected health information in a way that is not addressed in this policy.
2. The Privacy Officer should then determine what information may be disclosed or requested according to the following:
 - i. Disclosures in Response to Requests From Selected Persons – when the persons or organizations who have entered into a Business Associate Agreement with the agency are making a request, the Privacy Officer or designee may reasonably rely on such a request as requesting the minimum protected health information necessary for the disclosure
 - ii. A listing of all business associates will be kept in the office of the Privacy Officer, including:
 - Billing companies
 - Collection agencies
 - Staffing agencies
 - Cleaning services
 - Copying services
 - Companies who provide professional services to the agency

- iii. When one of the following persons or organizations are making a request, the Privacy Officer or designee may allow disclosure of the protected health information without second-guessing the request or limiting the amount of information released:
- A health care provider that is required to comply with federal privacy regulations
 - A health plan or health care clearinghouse that converts health information to and from standard and non-standard formats
 - A researcher with appropriate documentation from the Institutional Review Board (IRB) that meets the requirements of [Section 2.7.6](#).
 - A public official or agency requesting protected health information for public policy purposes, if the public official or agency represents that the request is the minimum necessary for the stated purpose of the disclosure.
- iv. If the Privacy Officer or designee strongly believes that a request by one of the foregoing persons or organizations seeks more than the minimum information necessary, he or she should attempt to reach a compromise that meets the concerns and needs of both parties.
- v. Disclosures in Response to All Other Requests – if the request is made by any other person or organization, the Privacy Officer or designee should decide how much information to disclose using the following criteria:
- What is the purpose of the disclosure?
 - What type of information does the recipient need to accomplish the purpose of disclosure?
 - Where is this information located? (i.e. x-ray, medical record, electronic database)
 - Is other information attached to this information? If so, is the attached information also needed to accomplish the purpose of disclosure? If the attached information is not needed, a copy of the record should be made and the extraneous information should be redacted.
- vi. Requests for Protected Health Information From Others – when deciding what information may be requested from another person or organization outside the agency, the Privacy Officer should consider the following:
- What is the purpose of the request?
 - What type of information does the agency need to accomplish this purpose?
 - What other information is likely to be attached to the information the agency is requesting? If that information is not needed, the Privacy Officer or designee should specify in the request that this information does not need to be disclosed.

- Can the request be phrased more narrowly to target only the information needed by the agency to accomplish this purpose?

3. If there is insufficient time to consult with the Privacy Officer without jeopardizing patient care, the staff member should consider the factors described above and notify the Privacy Officer as soon as possible afterwards.
4. Many disclosures to persons outside the Toledo-Lucas County Health Department or requests for information from persons outside the agency will require a written authorization from the patient whose information is involved. This policy only discusses how much information may be disclosed or requested and does not discuss when such authorizations are required.

E. Using, Disclosing, or Requesting the Entire Medical Record

1. Staff are instructed to contact the Privacy Officer or designee if they believe that the entire medical record should be used, disclosed, or requested in a way that is not addressed as “routine” and is not excepted from this policy.
2. The Privacy Officer or designee will determine whether there is a specific justification for using, disclosing, or requesting the entire medical record.
3. The specific justification for using, disclosing, or requesting the entire medical record should be documented in the patient’s medical record.
4. If there is insufficient time to consult with the Privacy Officer without jeopardizing patient care, the staff member should consider the factors described above and notify the Privacy Officer as soon as possible afterwards.

F. Violations

1. Suspected violations should be promptly reported to the Privacy Officer, and procedures should be followed as described in [Section 1.5](#).
2. If appropriate, the Privacy Officer will follow procedures outlined in [Section 1.7](#) and [Section 1.8](#).
3. Any attempt to retaliate against a person for reporting a violation will itself be considered a violation of [Section 1.9](#).

Section 3 – Notice and Authorization

3.1 Notice of Privacy Practices

Policy

The Toledo Lucas County Health Department is required to provide a Notice of Privacy Practices to all patients or any persons requesting a copy. All individuals have the right to receive adequate notice of the uses and disclosures of protected health information that may be made by an organization, and of the individual's rights and the agency's responsibility with respect to protected health information.

Procedure

- A. The Privacy Officer is responsible for developing the Notice of Privacy Practices.
- B. The Notice of Privacy Practices must be written in plain language that most patients of average intelligence and education will be able to understand.

3.1.1 *Required Contents of Notice of Privacy Practices*

- A. The following language must appear exactly as it is shown here and must be prominently displayed at the top of the notice:

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED
AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

- B. Uses and Disclosures
 - 1. This section of the notice must describe and give examples of the uses and disclosures for purposes of treatment, payment, and healthcare operations covered by the notice.
 - 2. It must identify the legally mandated disclosures that may be made without the patient's authorization.
 - 3. It must indicate that any other use or disclosure of protected health information requires written authorization by the patient, and that an authorization may be revoked by the patient.
- C. Additional Uses of Information
 - 1. The uses and disclosures listed in this section must be specified if the medical practice intends to use protected health information for any other the listed activities. This section can be merged with the previous section.
 - 2. This section identifies any use of protected health information in the preparation of appointment reminders, in offering information about treatment and other health-related benefits or services, or to conduct fundraising for the practice.
- D. Individual Rights
 - 1. This section of the notice must identify the rights of the patient under the federal privacy rule. These must include:
 - i. The right to request restrictions

- ii. The right to receive confidential communication
- iii. The right to inspect and copy protected health information
- iv. The right to amend protected health information
- v. The right to receive an accounting of disclosures
- vi. The right to receive a printed copy of the notice itself

E. Toledo Lucas County Health Department's Duties

- 1. This section describes the duties of the organization, specifically with respect to maintaining the privacy of protected health information, giving the Notice of Privacy Practices to patients, and abiding by the terms of that notice.

F. Right to Revise Privacy Practices

- 1. The notice must clearly state that the medical practice reserves the right to modify its privacy practices and that should it do so, the revised notice will be made available to patients upon their request.

G. Complaints

- 1. This section must outline the procedure for submitting complaints concerning the medical practice's privacy practices, or to report suspected violations of privacy rights.
- 2. It also must indicate that the organization will not retaliate against the patient for submitting a complaint or reporting a suspected violation.

H. Contact Person

- 1. This section of the notice must contain the name, or title, and telephone number of the Privacy Officer

I. Effective Date

- 1. This section must give the effective date of the Notice of Privacy Practices. The effective date may not be earlier than the date on which the notice is printed and made available for distribution.
- 2. In the case of revisions to the notice, the effective date of the revised notice may not be earlier than the printing and release date of the revised notice. In other words, the policies described in the notice cannot go into effect before patients have been informed of the policies.

3.1.2 Providing the Notice of Privacy Practices to Patients

- A. The notice must be given to all patients at the time of their first visit to the organization. The notice must also be given to any patient who requests one at any time.
- B. All patients will be given a copy of the notice during their first contact, whether in person in the office, via telephone consultation, or through other electronic means such as email.
- C. A copy of the notice will be posted in waiting areas.

- D. The notice will be posted on the department's website.
- E. An individual who receives a copy of the notice electronically (by email) also may request a printed copy.

3.1.3 Acknowledgement of the Notice of Privacy Practices

- A. All patients must be asked to sign an acknowledgement that they have received a copy of the Notice of Privacy Practices.
- B. If the patient cannot sign the acknowledgement, his or her personal representative may sign the acknowledgement.
- C. If the patient cannot sign the acknowledgement and his or her personal representative is not available, or if the patient refuses to sign the acknowledgement, the staff member who requests the acknowledgement must document the attempt to obtain an acknowledgement and briefly summarize the reason it was not obtained.
- D. When a patient requires emergency treatment, providing the notice and obtaining an acknowledgement should be delayed until the patient's condition has been stabilized.
- E. Copies of all signed acknowledgements should be included in the patient's medical record or filed with the Privacy Officer.

Regulation

45 CFR 164.520

3.2 Authorization of Use or Disclosure

Policy

Protected health information, in certain situations, will be used and disclosed only pursuant to a written, signed patient authorization, as designated by the HIPAA privacy standards or other pertinent state laws.

Procedure

- A. *Use* refers to the use of the information by the member of the staff of the agency. *Disclosure* refers to the disclosure of information to a person or organization separate from the agency.
- B. Examples of uses and disclosures for which authorization would be required include:
 - 1. Providing camp physicals or medical examinations required for participation in athletic activities
 - 2. Providing mailing lists to other organizations for marketing campaigns
 - 3. Participation in medical research and clinical trials
- C. The authorization obtained from a patient must be written in plain language.

3.2.1 Required Contents of Authorization for Use or Disclosure

- A. Information to be Used or Disclosed
 - 1. This section must list the information that will be used or disclosed to others. The descriptions should specify the nature of the information covered by the authorization. The medical practice should not rely instead on a blanket statement that covers any and all information that may be collected or received by the practice.
- B. Persons Authorized to Use or Disclose Information
 - 1. This section must identify specific medical practice staff who will use or disclose the information. The authorization may specify a class of staff members who are authorized to use or disclose the information (i.e. members of an identifiable research team).
- C. Persons to Whom Information May Be Disclosed
 - 1. This section must specifically identify the person or persons to whom the information will be disclosed. The authorization may designate a class of individuals such as the principle investigator or a research project at a specific university.
- D. Purpose of Requested Use or Disclosure
 - 1. This section must describe the purposes for which the information will be used or disclosed. When an individual initiates the authorization, for example, for a school or camp physical, this section may simply state "at the request of the individual."
- E. Expiration Date of Authorization

1. This section must specify a date after which the information described in the first section may no longer be used or disclosed. When information is to be used for research, the expiration section may simply state “none” or “end of research study.”

F. Right to Terminate or Revoke Authorization

1. This section must specifically describe the right of the patient to revoke the authorization, any restrictions on the ability of the patient to revoke the authorization, and the procedures for revoking the authorization.

G. Potential for Re-disclosure

1. This section must include a statement explaining that information used or disclosed under the authorization may be re-disclosed by the individual or organization receiving it and that re-disclosed information may not be protected by the federal privacy rules.

H. Impact on Treatment

1. This section must clearly describe the effect of refusing to authorize the requested use and disclosure of protected health information.
2. If the authorization is not for research-related treatment, a statement must appear explaining that the patient may not be denied treatment if he or she does not authorize the requested use and disclosure of protected health information.
3. If the authorization is for research-related treatment, a statement may be included indicating that authorization is required to receive the research-related services. This statement is not required, however, unless authorizing use or disclosure is a precondition for receiving treatment.

I. Remuneration

1. This section must describe whether the use or disclosure will result in remuneration, directly or indirectly, for the medical practice or staff member. This section is required only for authorization of uses and disclosures related to marketing. It is not required for research-related authorizations.

J. Signature

1. The patient or a person representative must sign and date the authorization. If a personal representative signs the authorization, he or she must describe the source of his or her authority to sign on the patient’s behalf, for example, legal power of attorney.

3.2.2 *Obtaining Authorization for Use or Disclosure*

- A. When a staff member knows in advance of collecting or creating protected health information that the information will be used or disclosed for a purpose not covered by the notice, the staff member should seek the patient’s authorization at the time the information is collected.
- B. It is not necessary, however, to obtain the patient’s authorization before the information is created. Authorization can be obtained at any time after it is created but before the information is used or disclosed for a purpose not covered by the notice.

- C. The staff member who uses or discloses the information is responsible for obtaining the patient's authorization. The patient or the patient's representative must be given a copy of the signed authorization.
- D. The staff member requesting the authorization should obtain an authorization form and complete the sections describing the information to be used or disclosed, the purposes of the use or disclosure, the persons who will use or disclose the information, and the persons to whom the information will be disclosed.
- E. The staff member or a person designated by the staff member should review the authorization request with the patient.
- F. The patient may request restrictions on the use and disclosure of protected health information. The staff member requesting the authorization should consider these requests and may, at his or her discretion, accept or reject them. Accepted restrictions should be clearly noted on the authorization form.
- G. The patient should sign and date the authorization form and the signed and dated authorization form should be placed in the patient's record. The patient must be given a copy of the signed and dated authorization form.

3.2.3 Refusal to Sign an Authorization for Use or Disclosure

- A. A patient who refuses to authorize specific use or disclosure may not be refused treatment except under the following circumstances:
 - 1. The treatment is available only to participants in a research study. A patient who does not authorize use of information for research may be refused treatment that is available only to participants in the research study.
 - 2. The services to be provided have no purpose other than responding to a request for information from another entity (for example, from a parent requesting a physical for a child who wants to participate in sports programs).
- B. When a patient refuses to sign an authorization, it should be determined whether the request involves information included in either of the two categories listed above.
- C. If the authorization is for use and disclosure of information for purposes of research-related treatment, the patient should be told that the treatment is available only to participants in a study and that the participants must authorize use and disclosure of their information in the study.
- D. If the authorization involves a request for information from another organization, the patient should be told that the services will not be provided unless disclosure is authorized.
- E. If the patient continues to refuse to sign the authorization, the persons requiring the authorization should be notified of the patient's refusal.

3.2.4 Revoking Authorization for Use or Disclosure

- A. A patient may revoke an authorization. The revocation must be in writing and must be attached to the related authorization.

- B. A patient who indicates that he or she wants to revoke an authorization should be given an authorization revocation form.
- C. The staff member who sought the original authorization, if he or she is available, or another staff member should explain to the patient that revoking the authorization will not affect any use or disclosure of information that has already occurred.
- D. The patient should sign and date the revocation form. The revocation form should be appended to the authorization and included in the patient's records.

Regulation

45 CFR 164.508

3.3 Patient Requests

Policy

The Toledo Lucas County Health Department recognizes the patient's right to request confidential communications in certain instances, as well as to request restrictions on specific uses and disclosures of protected health information.

Procedure

- A. Patients may request two types of privacy protections:
 - 1. Confidential communications
 - 2. Restrictions on the use and disclosure of protected health information

3.3.1 Patient Requests for Confidential Communications

- A. Staff members must accommodate a patient's request for confidential communication if the following criteria are met:
 - 1. The patient provides an alternative address or telephone number at which he or she may be contacted.
 - 2. The request can be accommodated without limiting the ability of the agency to submit claims to the patient's health plan.
- B. If the request for confidential communication will prevent the practice from submitting claims to the patient's health plan, the request will be accommodated only if the patient identifies another method of paying for services provided by the medical practice.
- C. Requests for confidential communication must be made in writing. The staff members may provide the patient with a confidential communication request form, or the patient may simply submit a written request.
- D. The staff member may not require the patient to explain why he or she wants to receive confidential communications, although the staff member is permitted to request an explanation. The patient may refuse to provide any explanation or justification for his or her request.
- E. When a patient requests confidential communication of protected health information (for example, the results of a diagnostic test), the staff members to whom the request is made should tell the patient that the request must be made in writing and explain the conditions that must be met before the requests will be granted.
 - 1. The patient should be given a confidential communication request form by the staff member to whom the request is made or by a staff member he or she identifies.
 - 2. The patient should be informed that the request will be accommodated if the patient provides an alternative means of making confidential communications.
 - i. For example, the patient should provide a telephone number at which messages to contact the provider can be left. No method of contacting the patient that prevents the staff

member from identifying both the patient and the medical practice will be considered acceptable.

3. The requests for confidential communication should be documented in writing.

3.3.2 Patient Requests for Restrictions on Use and Disclosure

- A. A patient may request restrictions on the use and disclosure of protected health information for treatment, payment, and health care operations as described in the notice of privacy practices. A patient also may request restrictions on the use and disclosure of protected health information covered by an authorization form.
- B. The medical practice should consider these patient requests but is not required to accept them. The practice generally accepts a request for a restriction on the uses and disclosures that are described in the notice of privacy practices or outlined in an authorization only if the following criteria are met:
 1. The request will not impede treatment, payment, or day-to-day functioning of the agency.
 2. The restrictions will not interfere with the purpose for which an authorization is being sought.
 3. The patient has valid reasons for requesting restrictions, in the judgment of the patient's physician.
- C. One instance in which the practice will be required to accept the requested restriction is when a patient has requested restriction on a release of information to a third-party payer for a service he or she has already paid in full out of pocket. In that instance, the provider must accept the individual's request for restriction, unless it is otherwise prohibited by law.
- D. Once the medical practice accepts requested restrictions, they must be honored unless doing so would interfere with emergency treatment.
- E. All restrictions to which the practice agrees must be documented in writing.
- F. A restriction on the disclosure of information that a patient requests and that the practice agrees to does not prevent the practice from disclosing information that is mandated by law, which does not ever require the patient's authorization.
 1. A patient may request a restriction on the use or disclosure of information at the time he or she signs an acknowledgement of receiving the Notice of Privacy Practices or an authorization form.
 2. The request should be reviewed by the Privacy Officer or designated staff member to determine whether the requested restriction would impede the use of information for treatment, payment, or health care operations.
 3. The Privacy Officer, or the designated staff member, should ask the patient to explain why he or she is seeking the restriction.
 4. The restriction should be agreed to if, in the judgment of the Privacy Officer, it will meet the requirements set out in this policy.
 5. If the request is agreed to, it should be documented and must be attached to the authorization form to which it applies.

3.3.3 Termination of Restrictions on Use and Disclosure

- A. The practice may terminate a restriction on the use and disclosure of protected health information to which it has agreed.
- B. A staff member who wishes to terminate a restriction should contact the Privacy Officer and discuss the need for termination. The termination request should be approved if the continuation of the restriction would substantially impede treatment, payment, or the day-to-day operation of the practice.
- C. The staff member should contact the patient to discuss the need for the termination and the patient must be given the opportunity to agree or disagree with the termination.
 - 1. If the patient agrees to the termination, he or she should sign a statement to that effect. If the patient is not available to sign a written statement, his or her oral agreement should be noted, signed, and dated by the staff member who discussed the termination with the patient.
 - i. Information collected prior to the date of the termination may be used or disclosed as though the restriction had never been accepted.
 - 2. If the patient does not agree to termination, only information collected after the date of the termination may be used or disclosed without considering the restriction. The restriction will continue to apply to information collected prior to the date of termination.
- D. The termination of restrictions should be attached to the authorization form in which the restriction appears.

Regulation

45 CFR 164.522

Section 4 – Patient’s Rights

4.1 Access to Protected Health Information

Policy

Patients have the right to receive access to their protected health information under the HIPAA privacy regulations. It is the policy of the Toledo Lucas County Health Department to ensure that these rights are met.

Procedure

- A. A patient or a patient's representative may, subject to approval, inspect and obtain a copy of patient information maintained in medical records or other information systems of the Toledo Lucas County Health Department.
- B. A patient must submit a request to inspect or copy protected health information.
- C. The request will be reviewed
- D. If the request is denied, the patient will be informed
- E. If the request is approved, the patient will be given access to the requested information.

Regulation

45 CFR 164.524(1)

4.1.1 Requests for Access to Protected Health Information

- A. When a patient or the patient's representative requests access to information, he or she should be told that all requests to inspect or copy protected health information must be submitted in writing. The patient should be referred to the Privacy Officer.
- B. The Privacy Officer will give the patient or the patient's representative a copy of a request form and explain the agency's policies on allowing patients to inspect their information.
- C. Upon receipt of a request form, the Privacy Officer will review the request as explained in the next section.
- D. This policy does not address or prevent a physician from sharing the results of laboratory or other diagnostic tests with a patient or patient's representative, or from discussing the results of medical procedures.
 - 1. These communications related to treatment may be made orally or in writing at the discretion of the patient's physician.
- E. This policy does not address or prevent other staff members from discussing or disclosing to the patient, orally or in writing, information related to the current status of claims that have been submitted to the patient's health plan.

Regulations

45 CFR 164.520(c)(iv)(c)

45 CFR 164.524(b)(1)

4.1.2 Review of Requests for Access to Protected Health Information

- A. The request for access to personal health information will be sent promptly to the Privacy Officer. A copy of the request will be filed in the patient's records.
- B. The Privacy Officer will consider the restrictions on access listed below when determining whether to approve or deny the request to inspect or copy protected health information.
- C. A decision to grant the patient or patient's personal representative permission to inspect or copy the requested information will be made within 30 days of the date the request is submitted.
- D. If the protected health information is maintained in electronic form and the patient would like to view the information or receive a copy of it in electronic form, he or she must make that request specifically on the request form.
- E. Restrictions on Access
 - 1. Psychotherapy notes will not be made available to the patient unless approved by the treating therapist or successor.
 - 2. Information compiled in anticipation of, or for use in, legal proceedings will not be made available to the patient or the patient's legal representative unless required by law or court order.
 - 3. Information that, by law, may not be disclosed to the patient will not be made available to the patient or the patient's representative.
 - 4. Information will not be made available if the patient's physician believes that it is likely to endanger the life or physical safety of the patient.
 - 5. Information will not be made available if the patient's physician believes that access to the information is reasonably likely to cause substantial harm to a person other than the patient who is referenced in the patient's records.
 - 6. Information will not be made available to a personal representative of the patient if the patient's physician believes that access to the information by the personal representative is reasonable likely to cause harm to the patient or another person.
- F. The Privacy Officer will review the request to inspect or copy protected health information and will contact the patient's physician to determine if there are any reasons to restrict the patient's or patient representative's access to the information.
- G. If the request is disapproved, wholly or in part, the patient will be notified using the procedures outlined in the next section.
- H. If the request is approved, the patient will be notified and arrangements made for the patient to inspect or copy the requested information using procedures describe in [Section 4.1.4](#).

Regulations

45 CFR 164.524(a)

4.1.3 Denial of Requests to Access Protected Health Information

- A. When a patient's request to inspect or copy protected health information is denied, wholly or in part, the patient will be contacted and given an opportunity to request a review of that decision.
- B. Communication of Denial of Requests for Access
 - 1. A written explanation of the denial of a patient's request to inspect or copy protected health information will be prepared using the appropriate form.
 - 2. If an alternative, such as summary of the requested information, could satisfy the patient's request at least in part, the communication should describe that alternative.
 - 3. A patient or the patient's representative whose request to inspect or copy protected health information is denied may request a review of that decision by a licensed health professional who was not involved in the decision to deny the request.
- C. Review of Decision to Deny Access
 - 1. If the Privacy Officer receives a copy of a denial notice indicating the patient is requesting a review of the denial, he or she should forward the request to a licensed health professional who was not involved in the original denial and ask him or her to review the decision.
 - 2. The review should normally be completed within 30 days. The Privacy Officer will follow up with the reviewing physician if the review is not complete within 30 days.
 - 3. The Privacy Officer should communicate the result of the review to the patient using the reviewer form.
- D. Inspection of Records
 - 1. Although requested information is generally made available to the patient within 30 days of the date the request is made, that time period can be extended to 60 days if the records in question must be retrieved from off-site storage.

Regulations

45 CFR 164.524(d)

45 CFR 164.524(b)(2)

4.1.4 Approval of Requests to Access Protected Health Information

- A. Approval of a patient's request to inspect or copy protected health information should be communicated to the patient or the patient's representative using the request approval form.
- B. The form should specify the date and time that the records will be available for access.
 - 1. The Privacy Officer will determine the earliest date at which the requested information can be made available.
- C. The Privacy Officer or designated staff person will prepare the approval form and send it to the patient.

D. Arrangements for Inspection

1. Arrangements should be made to provide access to protected health information at a place and time convenient for the patient.
2. The patient must inspect the records on the premises of the medical practice.
3. If this is not satisfactory to the patient, he or she should be given the option of having copies made and sent to an address that he or she specifies.
4. The patient may be charged the cost of preparing and mailing the copies or the supplies and labor to put together the electronic version for mailing.

Regulations

45 CFR 164.524(c)

45 CFR 164.524(d)

4.2 Amendment of Protected Health Information

Policy

To ensure that the rights of patients to request that amendments be made to their protected health information under HIPAA privacy regulations are met.

Procedure

- A. A patient may request amendment of the information maintained by the Toledo Lucas County Health Department contained only in the designated record sets listed below. The patient must follow the procedures outlined in Section 4.2.1 when requesting amendment of information maintained by the agency.
- B. [Designated Record Set](#)
 - 1. The patient's medical records
 - 2. The patient's billing records
 - 3. Other records that contain protected health information used to direct treatment

Regulation

45 CFR 164.526(a)

4.2.1 Requests for Amendment of Information

- A. Requests to amend protected health information must be submitted in writing. Patients should use the patient information amendment form.
- B. Patients who indicate their belief that the information in their records is incorrect should be given a patient information amendment form.
- C. Patients should be referred to the Privacy Officer to resolve questions about the form.

Regulation

45 CFR 164.526(b)

4.2.2 Review of Requests for Amendment of Information

- A. Patient information amendment forms should be forwarded to the Privacy Officer.
- B. The Privacy Officer should contact the patient's physician or a staff member he or she designates and request a review of the requested amendments.
- C. The physician or designated staff member should indicate which of the requested amendments should not be made because the information on the patient's record is accurate and complete or meets other requirements for denying a request that are listed in the next section.
- D. The physician or designated staff member should then return the form to the Privacy Officer.
- E. The Privacy Officer should review the form after it is returned by the patient's physician and identify any information that should be amended.

- F. The Privacy Officer should initiate the procedures for amending PHI specified in [Section 4.2.4](#).
- G. Action must be completed on any request for amendment within 60 days of receiving the request.
- H. If action cannot be completed within 60 days, the medical practice must notify the patient of the delay, including reasons for the delay, and complete the review within 90 days of the date the request was originally received on.
- I. After completing the review, the Privacy Officer will complete the patient information amendment form by indicating the disposition of each requested amendment.
- J. A copy of the completed patient information amendment form will be sent to the patient along with any explanatory comments that the Privacy Officer believes to be necessary.
- K. The patient will be asked to submit the names and addresses of any organizations or individuals that he or she has reason to believe have received the uncorrected information for the purpose of notifying them of the amendment, if granted.

Regulation

45 CFR 164.526(b)(2)

4.2.3 Denial of Requests for Amendment of Protected Health Information

- A. The Privacy Officer may deny a patient's request to amend records if the following criteria are met. If the information to be amended:
 - 1. Was not created by the agency (received from outside entity)
 - 2. Is accurate and complete
 - 3. Does not exist in the specified records
 - 4. Is not available for inspection by patient or patient's representative (see [Section 4.1](#))
- B. When a request to amend protected health information is denied, the patient will be informed in writing of the decision. The notice sent to the patient must advise him or her of the following:
 - 1. The patient may submit a statement of disagreement that will become part of his or her records and will, in the future, be disclosed to any person or organization that receives the identified information.
 - 2. If the patient does not submit a statement of disagreement, he or she may ask the medical practice to include the request for amendment and the denial in any future disclosure of the identified information to any person or organization to receive it.
 - 3. The patient may file a complaint with the provider concerning the request for amendment. A description of how the patient can file this complaint must be included in the notice.
 - 4. The letter must identify the name, mailing address, and telephone number of the Privacy Officer.
- C. Statement of Disagreement

1. If the patient disagrees in writing when notified that a request for amendment of protected health information has been denied, the Privacy Officer will review it and will append it to or otherwise link it to the patient's record. This will ensure that it will accompany the original information when it is used or disclosed in the future.
2. The Privacy Officer may prepare an accurate summary of the patient's statement of disagreement if he or she believes that a summary will adequately provide a clear understanding of the disputed information.

D. Rebuttal of Disagreement

1. If a patient disagrees in writing when notified that the request for amendment of protected health information has been denied, the Privacy Officer will review the statement and determine whether a formal rebuttal or response, as provided in federal regulations, is necessary.
2. The Privacy Officer will consult as necessary with the patient's physician or other medical practice staff members to make this determination. If determined necessary, the Privacy Officer will prepare and append it to the patient's records.
3. Both the patient's statement of disagreement and the rebuttal statement will be noted in the patient's records.
4. The statement of disagreement and the rebuttal either will be included in the patient's records, or will be linked to those records to permit them to be included with the original information when it is used or disclosed in the future.
5. A copy of the rebuttal statement will be sent to the patient.

Regulations

45 CFR 164.526(5)

45 CFR 164.526(d)

4.2.4 Approval of Requests for Amendment of Protected Health Information

A. When a request for amendment of patient information is approved, the Privacy Officer will:

1. Initiate procedures for the amendment of internal records
2. Initiate the procedures for notifying other parties that the information has been amended

B. Amendment of Internal Records

1. When a patient's request for amendment of protected health information is approved, either of the following procedures should be followed:
 - i. The records containing the affected information are updated
 - ii. The amended information is linked to the original information
2. The Privacy Officer will refer the request for amendment to the medical practice staff member responsible for maintaining the affected record and will identify the records that need to be amended.

3. Those records should either be amended or be linked to the amended information (that is, contained in a new or corrected record where it will be available if the affected information is used or disclosed in the future).

C. Notifying Other Parties of Amended Information

1. When a patient's protected health information is amended in response to a patient, other organizations to which the information being amended has been disclosed will be notified of the amendment.
2. Organizations to be notified include:
 - i. Business associates, health plans, and other providers the Privacy Officer can identify as having received the information.
 - ii. Persons and organizations the patient can identify as having received the information that requires amendment, but only to the extent that the Privacy Officer can confirm that these persons or organizations previously received the information.
3. The medical practice is not required to confirm that the organization or other entities notified of the amendment have updated their records.

D. Receipt of Notification of Amendment

1. When notified by another medical practice, health plan, or other covered entity that protected health information received earlier has been amended, the medical practice will follow the procedures in place for handling its own amended information.

Regulations

45 CFR 164.526(c)

45 CFR 164.526(e)

4.3 Accounting for Disclosures of Protected Health Information

Policy

To ensure patients' rights to request an accounting of specific types of uses and disclosures of their protected health information made under the HIPAA privacy regulations are met.

Procedure

- A. The Privacy Officer will create a system for documenting all disclosures of protected health information for which an individual may request an accounting.
- B. When a staff member discloses protected health information, the staff member will document the disclosure. This documentation will be necessary if the patient were later to request an accounting of disclosures.
- C. Disclosures of protected health information that medical practice is required to report to a patient include:
 - 1. Any disclosures, other than a disclosure for purposes of treatment, payment, or healthcare operations, will be documented by completing a disclosure accounting form.
 - 2. The disclosure accounting form will be forwarded to the Privacy Officer who will update the files and databases that are used to prepare accountings of disclosures.
- D. Disclosures of protected health information that a medical practice is not required to report to a patient include:
 - 1. Any disclosures for the purpose of treatment, payment, or healthcare operations
 - 2. Any disclosures specifically authorized by the individual
 - 3. Any disclosure to the patient himself or herself
 - 4. Any disclosure for use in a facility directory
 - 5. Any disclosure to national security or intelligence agencies required by law
 - 6. Any disclosure to correctional institutions or law enforcement agencies required by law
 - 7. Any disclosure that is part of a limited data set
 - 8. Any disclosure that occurred prior to April 14, 2003

4.3.1 Requests for an Accounting of Disclosures of Protected Health Information

- A. To receive an accounting of disclosures of protected health information, a patient must submit a written request to the Privacy Officer.
- B. A patient who indicates to any staff member that he or she would like to receive an accounting of disclosures should be told to contact the Privacy Officer.
- C. The Privacy Officer will provide the patient with a disclosure of accounting form and review the types of disclosures that will be reported in the accounting.
- D. The Privacy Officer will determine whether the ability of the patient to obtain an accounting of disclosures has been suspended in response to a request from a law enforcement or health oversight agency. If the patient's right to an accounting has not been suspended, the Privacy Officer will start preparing an account.

1. Requests from law enforcement agencies should be submitted in writing. The written statement should indicate that providing an accounting is likely to impede on the agency's activities and should specify a time period during which the patient's right will be suspended.
2. Suspensions that last more than 30 days must be supported in writing and the request must be made in writing. If a written request is not submitted, the individual's right may not be suspended for more than 30 days.
 - i. Communication from a law enforcement or health oversight agency requesting the suspension should be directed to the Privacy Officer.
 - ii. The Privacy Officer will verify the credentials of the government official that makes a verbal request and document the identity of the official or agency.
 - iii. The Privacy Officer will place the patient's name on a list of persons whose right to an accounting has been suspended pursuant to an official request.
- E. If a patient requests more than one accounting during any 12-month period, they will not be charged for the first accounting, but will be informed that the agency may charge a fee for the second accounting. If the patient agrees to pay the fee, the second accounting will be provided.

4.3.2 Information Provided in an Accounting of Disclosures of Protected Health Information

- A. The information that will be provided in an accounting disclosure includes:
 1. The date of the disclosure
 2. The name of the entity or person who received the protected health information
 3. A brief description of the purpose of disclosure or a copy of authorization for disclosure
- B. Disclosures for business associates for purposes of treatment, payment, and healthcare operations should not be included in the accounting.
- C. Copies of accountings of disclosed information prepared for patients should be kept for six years.

Regulation

45 CFR 164.528

Section 5 – Business Associates

5.1 Business Associates

Policy

The Toledo-Lucas County Health Department protects the confidentiality and integrity of health information of its patients. This section defines the guidelines and procedures that must be followed for business associates who come into contact with protected health information.

Procedure

- A. A [business associate](#) is defined as any person or organization that performs or helps perform any function or activity that involves the use or disclosure of protected health information.
- B. In short, any person (other than an employee or other member of the practice staff) or organization that receives, transmits, or uses protected health information from the Toledo Lucas County Health Department is a business associate.
- C. A business associate may receive protected health information from the medical practice, create protected health information for the medical practice, or transmit data on behalf of the medical practice.
- D. Protected health information may be disclosed to business associates only if the Toledo-Lucas County Health Department receives satisfactory assurances that the business associate will safeguard the privacy of the protected health information that is creates or receives.

5.1.1 Business Associate Agreements

- A. Written contracts or agreements must be negotiated between a medical practice and any business associate that will handle protected health information it receives from or creates for the practice.
- B. This contract or agreement must include satisfactory assurances that:
 - 1. Identify the uses and disclosures of protected health information permitted under contract
 - 2. Permit the business associate to use or disclose information only as permitted under the privacy standards
 - 3. Restrict use and disclosure of the protected health information the business associate creates or receives to those that are not specified in the contract
 - 4. Call on the business associate to fully comply with the provisions of the HIPAA privacy and security regulations, not limited by specific references in the contract with the department
 - 5. Provide for reporting to the Toledo Lucas County Health Department any use or disclosure of protected health information not provided for under the business associate's contract
 - 6. Require the business associate to apply the same restrictions and conditions on use and disclosure of protected health information to the agents and [subcontractors](#) to whom it forwards the protected health information
 - 7. Make protected health information available to patients as provided in [Section 4.1](#).

8. Amend any protected health information that it receives when asked to do so by the department
9. Make available to the department the information it needs to account for uses and disclosures of protected health information as provided in [Section 4.3](#).
10. Make internal practices, books, and records related to the use and disclosure of protected health information available to HHS for purposes of determining compliance with the privacy standards
11. Return, if feasible, all protected health information to the department upon termination of the contract, and destroy any copies of such information. When return and/or destruction of protected health information is not feasible, the business associate will extend contractual protections to the use and disclosure of information for the purposes that make its return or destruction not feasible.
12. Notify the Toledo-Lucas County Health Department in the event of unauthorized disclosure of unsecured PHI
13. Provide for termination of the contract if the business associate violates any contractual provisions
14. Comply with the privacy rule to the extent the business associate is carrying out the organization's obligations under the privacy rule
15. Business associates must enter into business associate agreements with their subcontractors that impose the same obligations that apply to the business associates themselves.

5.1.2 Contractual Breaches by Business Associates

- A. If a staff member becomes aware of activities or practices by the business associate that violate the agency's contractual obligations, the activities or practices must be reported to the Privacy Officer.
- B. Investigation and Correction of Contractual Breaches
 1. When the Privacy Officer is notified that a business associate has violated a contractual provision related to the privacy of protected health information, he or she must implement the procedure to correct the violation.
 2. The Privacy Officer will contact the business associate and determine whether a contractual provision has been violated.
 3. If a contract provision has been violated, the Privacy Officer will identify steps to be taken by the business associate that will enable it to comply with its contractual obligations.
 4. The Privacy Officer will review corrective action steps with the business associate and determine whether those steps or other measures suggested by the business associate will correct the violation.
 - i. If an agreement can be reached, the corrective measures will be summarized in writing and sent to the business associate.
 5. The Privacy Officer will monitor the implementation of the corrective action measures by periodically contacting the business associate.

- i. The Privacy Officer may discontinue monitoring the contract after receiving adequate assurances that the corrective measures have been implemented and that the contract provisions will be complied with in the future.
6. If it is not possible to develop an acceptable corrective action plan, the Privacy Officer should implement the procedures established in the next section to terminate the contract.

5.1.3 Termination of Business Associate Contracts

- A. When the Privacy Officer is not able to correct violations of contractual obligations by a business associate, he or she should implement the following procedure:
 1. Identify an alternative source for the services provided by the business associate
 2. Refer the matter to the department's legal counsel with a request that formal action be taken to terminate the contract
 3. Have the department's legal counsel notify the business associate that action will be taken to terminate the contract if the violation of contract provisions is not immediately corrected
 4. Monitor the status of the contract and arrange for replacing the business associate when the contract is formally terminated.
- B. If the contract cannot be terminated, the contract violation should be reported by legal counsel to HHS as required by federal regulations.

Regulation

45 CFR 164.504

Section 6 – Security

6.1 Designation of Security Official

Policy

Compliance with federal [security](#) standards is the responsibility of the security official. It is the policy of the Toledo-Lucas County Health Department to appoint a Security Officer to fulfill these requirements.

Procedure

- A. The Information Technology Manager will serve as the organization's Security Officer.
- B. The Security Officer is responsible for:
 - 1. Establishing the provider's security program and overseeing its implementation
 - 2. Ensuring compliance with federal and state security regulations and standards
 - 3. Reviewing all purchases or acquisitions of information technology for consistency with the provider's security policies and standards
 - 4. Investigating security incidents (i.e., known or suspected violations of security policies and procedures and breaches in security measures of the security of the provider's PHI)
 - 5. Reviewing information system activity to ensure compliance with the provider's security policies and procedures
 - 6. Developing and implementing a security training and awareness program for the provider's employees and staff
 - 7. Reviewing and approving the security provisions of contracts with business associates
 - 8. Delegating specific tasks such as review of business associates contracts, while remaining responsible for compliance with the provider's security policy and standards
 - 9. Reviewing annually compliance with security requirements, policies, and standards
- C. The Security Officer may assign any of these responsibilities to other staff members or contractors but continues to be responsible for making sure these responsibilities are carried out.

6.2 Security Management Process

Policy

The Toledo-Lucas County Health Department has established a comprehensive security management process to ensure the availability, integrity, and confidentiality of patient information and other sensitive information.

Procedure

- A. The goal of this program includes preventing, detecting, containing, and correcting threats to the security of sensitive information
- B. These goals will be met by following through with activities established by:
 - 1. [Section 6.3 Risk Analysis](#)
 - 2. [Section 6.4 Risk Management](#)
 - 3. [Section 6.5 Sanction Policy](#)
 - 4. [Section 6.6 Information System Activity Review](#)

6.3 Risk Analysis

Policy

The Security Officer conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI the covered entity holds.

Procedure

- A. A comprehensive analysis of security threats is conducted at least once every three years. It is reviewed annually and updated as needed.
- B. The risk analysis comprehensively describes the information system, including the following components:
 1. The computer hardware and software that make up the provider's information system
 2. The categories and qualifications of staff members who use the system
 3. The functions and activities supported by the information system
 4. The data and information the information system collects, processes, and stores
 5. The physical environment that houses the information system components
 6. On-site and off-site storage of information
 7. The organizations to which information is transmitted
 8. The data and information transmitted to other organizations
 9. The internal and external connections between the provider's information system and the information systems of other organizations
- C. The risk analysis identifies threats to the security of the provider's PHI, including natural, human, and environmental threats. It also identifies the nature of each threat or vulnerability and how each may damage information security.
- D. The analysis indicates the preventative measures that the agency has implemented, or planning to implement, to limit the damage that might be caused by each threat or vulnerability and evaluates the likelihood that each security threat or vulnerability might occur.
- E. The risk analysis describes the nature and extent of the damage each threat might cause to the integrity, availability, and confidentiality of the provider's information resources.
- F. It also identifies high-priority threats that are the focus of risk management efforts and recommends controls or actions to lessen the risk associated with high-priority threats.
- G. The Security Officer reviews and approves the risk analysis, whose results are shared with other members of the provider's management team and presented to the governing body of the Toledo-Lucas County Health Department.

6.4 Risk Management

Policy

The Security Officer implements a comprehensive risk-management program based on the results of the risk analysis. The risk-management program includes the security measures identified by the risk analysis. These security measures aim to reduce the risks and vulnerabilities to a reasonable and appropriate level.

Procedure

- A. The Security Officer develops comprehensive risk-management plan at least every three years. The Security Officer reviews the risk-management plan and updates it as needed every 12 months.
- B. The risk-management plan summarizes the results of the risk analysis, including the major security threats the risk-management plan addresses and the measures that will be implemented to mitigate or keep risks at an acceptable level.
- C. The risk-management plan identifies the specific actions that will be taken to implement the security measures the risk analysis identified, including a timetable for implementation of each measure.
- D. The risk-management plan clearly describes the magnitude of the risks that will be accepted if the plan is adopted.
- E. The plan must include documentation that the accepted risks are reasonable based on the lack of availability of cost-effective risk reduction measures.
- F. Risks are considered reasonable if they:
 1. Cannot be reduced;
 2. Can be reduced only by adopting measures that would severely impair the ability of the information system to perform its intended functions; or
 3. Can be reduced only by implementing measures whose cost substantially exceeds the anticipated costs of any security failures that would be prevented.
- G. The risk-management plan is reviewed with and approved by the Toledo-Lucas County Board of Health annually.

6.5 Sanction Policy

Policy

Employees and other members of the Toledo-Lucas County Health Department workforce are subject to sanctions for violating the provider's security policies and procedures.

Procedure

A. Violations of security measures and the penalties associated with them include the following:

1. Minor Security Breaches

i. This category of breaches consists of minor or unrepeated violations of security policies

- Example: a staff member briefly leaves her workstation unattended without logging off to prevent injury to a patient or another staff member or due to sudden illness.
- Sanction – A minor infraction will result in brief counseling and, if necessary, additional security training

2. Significant Security Breaches

i. This category includes any documented violation of the security of PHI that could easily have been avoided had the staff member exercised due care

- Example: A staff member attaches a note to his workstation monitor that gives his user ID and password.
- Sanction: A pattern of repeated, significant violations of security policies may be grounds for temporarily suspending an employee and may lead to termination

3. Severe Security Breaches

i. This category includes any deliberate violation of security policies and procedures or confidentiality requirements that are not justified by considerations of employee or patient health and safety or were not necessary or unavoidable during the emergency situation.

- Example: a staff member makes a copy of PHI and gives it to a vendor without obtaining required authorizations.
- Sanction: A deliberate violation of security policies will result in the immediate suspension of the employee or other workforce member and the termination of all access to protected health information and information resources.

6.6 Information System Activity Review

Policy

The Security Officer periodically reviews records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Procedure

- A. The Security Officer reviews all security incident reports and ensures that any breaches in security have been corrected.
- B. The Security Officer regularly reviews records of system activity to identify any patterns of activity that suggest the Toledo-Lucas County Health Department's security policies and procedures have been breached, either by members of its workforce or by individuals or organizations that are not business associates of the practice.
- C. The Security Officer determines whether the security has been violated and takes appropriate corrective action, including changes in security policies and procedures.
- D. The Security Officer maintains records of all reviews of security incidents and system activity, and reports any findings to other members of the agency's management.

6.7 Workforce Security

Policy

The Security Officer develops and implements policies allowing only those workforce members who have the appropriate qualifications and job responsibilities to use the provider's PHI and information systems.

6.7.1 Authorization

Policy

All employees and other members of the provider's workforce must be specifically authorized to use the information resources or to access PHI. If they are not specifically authorized, they must be under the direct supervision of an appropriately authorized staff member when working with PHI or on components of the provider's information system and working only for a temporary period, such as when repairing a system.

Procedure

- A. Generally, staff members are authorized to use only the PHI needed to perform their professional and job responsibilities
- B. The job descriptions of every staff member should specify the access to information resources and PHI that is authorized. Following are the categories of access authorization:
 1. Clinical Authorization
 - i. Physicians, nurses, and other health professionals may access any information contained in a patient's records (other than information that has been restricted by the patient's physician) for the purpose of treating the patient, including consulting with other professionals concerning the patient's treatment.
 2. Clerical Authorization
 - i. Clerical staff responsible for preparing and submitting claims and processing payment information may access any information contained in the patient's records needed to meet requirements for submission and adjudication of a claim for services.
 3. Administrative Authorization
 - i. Members of the provider's management may access any information contained in patient records when required for the purpose of supervising staff or complying with licensing and other regulatory requirements.
 4. IT Management Authorization
 - i. Staff members responsible for managing the provider's information resources may access information needed to configure security features of computer hardware and software. Examples include establishing user passwords and setting permissions to access data or configure hardware and software.
 - ii. A staff member who requires access to information that he or she is not authorized to access should request the assistance of an appropriately authorized staff member.

- iii. Maintenance and housekeeping staff who may have physical access to PHI should be supervised closely enough to reasonably ensure that the security policies of the medical practice are not violated.
- iv. Staff members who are authorized to access PHI must complete security and privacy training and must review the limitations on their access to information and information resources.

6.7.2 Clearance

Policy

Staff members will be authorized to access PHI and to use information resources if they meet the minimum professional or technical qualifications for the position they occupy and they have not been disciplined for serious infractions of security in previous jobs. Staff members who have been disciplined for infractions of security policies and procedures may be granted restricted access until their trustworthiness has been established to the satisfaction of the Security Officer.

Procedure

- A. When verifying credentials and checking references, the staff member responsible for hiring should determine that the candidate has not been sanctioned or disciplined for infractions of security policies or standards in the past.
- B. Any restrictions on access to information resources should be communicated to the Security Officer so the necessary technical restrictions in access privileges can be implemented.

6.7.3 Termination Procedures

Policy

A staff member's authorization to use information resources and to access PHI ends upon termination of employment.

Procedure

- A. Staff members must turn in keys or key cards that give access to computer equipment or facilities upon termination of their relationship with the Toledo-Lucas County Health Department.
- B. The Security Officer should be notified of the effective date of any employee termination or of the date on which a staff member's authorization to use the provider's information resources will be terminated.
- C. The staff member's user account on the provider's information system will be disabled or deleted upon termination of the relationship with the agency.
- D. The staff member will surrender any protected information, including information contained on storage media (i.e. a CD-ROM or removable disk, data storage key, etc.) that may be in the staff member's possession at the time the relationship with the agency ends.
- E. The employee should be escorted out of the building, and the employee's access authorization terminated immediately when the employee's supervisor feels these actions are appropriate to safeguard the security

of the provider's PHI and information system. The Security Officer should be notified and steps taken to safeguard security such as rekeying the locks.

6.8 Information Access Management

Policy

The Security Officer is responsible for developing and implementing procedures to authorize staff members' use of the provider's information resources. This includes establishing access to PHI, based on the staff member's job responsibilities and qualifications. Authorization is limited to the information that individual needs to fulfill his or her job responsibilities.

6.8.1 Access Authorization

Policy

Staff members receive authorization to access PHI and to use the Toledo-Lucas County Health Department's workstations, conduct transactions, and run software applications based on their job responsibilities and qualifications. Authorization enables staff members to use the provider's information resources. Staff members should not access information for other staff members lacking appropriate authorization.

Procedure

- A. Only authorized staff members are allowed to use workstations (computer terminals, personal computers, and other devices) that can access PHI.
- B. A unique user ID and password are required to use the Toledo-Lucas County Health Department's information system.

6.8.2 Access Establishment and Modification

Policy

The Toledo-Lucas County Health Department will establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process based on their access needs at the time.

Procedure

- A. The Toledo-Lucas County Health Department grants individual users the right to access PHI and related information resources consistent with its access policies and procedures.
- B. When a staff member's access authorization needs to be changed, a formal request should be submitted to the Security Officer, who then reviews the request and authorizes the revised access privileges if the request meets the provider's authorization requirements.
- C. The ability of staff members and other users to use workstations or computer programs to conduct specific transactions or to perform various functions, tasks, or procedures is determined by each individual's access authorization.
- D. These tasks include installing new software, backing up data, and maintaining and configuring computer hardware and software.

6.9 Security Awareness and Training

Policy

The Security Officer is responsible for developing and implementing a security awareness and training program for all members of the provider's workforce, including professional staff, practice partners, and management.

Procedure

A. The security program must cover:

1. The definition of security (availability, integrity, confidentiality)
2. Threats to security (natural, human, and environmental)
3. Methods of safeguarding security
4. Security features of the provider's information system and applications
5. Use of major applications
6. Policies on installation and configuration of software
7. Controls on access to information
8. Correct use of antivirus software
9. Controls on access to information
10. Contingency plans and disaster procedure
11. Workstation policies
12. Good security practices (workstation use policies)
13. Security incident reporting procedures
14. Use ID and password policies

B. All staff members, including management and professional staff, are required to complete security training before they can use the provider's information systems or are permitted to access PHI.

C. New staff members receive security training as part of their orientation.

D. Contractors and consultants receive training and/or information on the agency's security policies and procedures.

6.10 Security Reminders

Policy

The Toledo-Lucas County Health Department publishes periodic notices and security updates to maintain awareness of security procedures and sound security practices. Notices are prepared whenever significant new security threats are identified, whenever security features of computer hardware and software are revised or updated, and whenever the Security Officer believes that a security incident warrants calling the attention of staff members to security policies and procedures.

Procedure

- A. The Security Officer is responsible for preparing, distributing, and posting security notices and periodic updates.
- B. The Security Officer is responsible for announcing the availability of security updates and changes to security policies and procedures at staff meetings.

6.11 Protection from Malicious Software

Policy

Anti-virus software is installed on all computer workstations and servers to protect the Toledo-Lucas County Health Department and its information from attack by malicious software such as computer viruses and other external threats.

Procedure

- A. The Security Officer is responsible for ensuring that antivirus software has been installed on all workstations and on network servers. The Security Officer also ensures that antivirus software is regularly updated.
- B. Staff members must not disable antivirus software and must immediately take action to report virus infections and remove viruses from affected machines when the antivirus software identifies an infection.
- C. The Security Officer maintains a log of virus infections and detections that includes a record of successful eradication of viruses and cleaning of affected files and computer applications.
- D. The Security Officer confirms that the viruses have been successfully removed from the affected machines.
- E. Staff members with access to the internet should not open email messages and email attachments from unknown senders.

6.12 Log-in Monitoring

Policy

Log-in procedures limit the number of unsuccessful long-in attempts to five, after which a user must contact the information system administrator to have his or her password reset.

Procedure

- A. The Security Officer reviews log-in monitoring records and investigates patterns that suggest security breaches or attempted penetration of security measures by unauthorized users.
- B. Operating systems are configured to monitor log-in attempts. The Security Officer maintains a record of any investigations of suspected efforts to penetrate the security measures by unauthorized users.

6.13 Password Management

Policy

All passwords in use at the Toledo-Lucas County Health Department should conform to a specific set of guidelines as set forth in this policy. This will help to keep passwords safe and secure across the enterprise.

Procedure

- A. All users must select a password conforming to the following guidelines:
 - 1. Passwords should be between six and 10 characters
 - 2. Passwords should not be the name of a pet, spouse, child, or parent
 - 3. Passwords should be a word or sequence of letters and numbers that cannot easily be guessed
 - 4. Password should never be written down
 - 5. Passwords should never be given to other staff members
 - 6. A new password should be selected every six months, and previous passwords should not be used
- B. The Security Officer reviews password policies when a user first receives his or her user ID.
- C. The Security Officer monitors password usage and identifies any patterns that suggest password policies and guidelines are not being followed.
- D. The Security Officer requires staff members who frequently lose or forget their passwords to complete retraining on the correct use of passwords.

6.14 Security Incident Procedures

Policy

Security incidents are to be reported promptly to the Security Officer. Incidents should be reported by the staff members responsible for the incident or staff members who identify the incident.

Procedure

- A. The Security Officer or an assigned delegate investigates security incidents and determines:
 1. Whether a breach of security has occurred
 2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused.
- B. The Security Officer ensures that actions needed to repair any damage caused or potentially caused by a security incident are taken.
- C. The Security Officer documents the report of a security incident, the findings of the investigation, and any actions taken in response to those findings.

6.15 Contingency Plan

Policy

It is the policy of the Toledo-Lucas County Health Department that policies and procedures are in place to protect the security of PHI during an emergency caused by fire, vandalism, system failure, natural disaster, or other contingencies. Security includes the availability, integrity, and confidentiality of the information.

Procedure

- A. Every three years, the Toledo-Lucas County Health Department develops a comprehensive contingency plan based on a thorough examination of the impact of natural, human, and environmental risks on the agency's ability to secure its information and information resources.
- B. The contingency plan identifies the major natural and man-made disasters that could adversely affect the availability, integrity, and confidentiality of PHI maintained in electronic form. The plan identifies the actions that will be taken to compensate for disasters that affect the availability, integrity, and confidentiality of PHI.
- C. The contingency plan assigns specific responsibilities to members of the staff. These responsibilities specifically address failures in normal security safeguards that are likely to occur during an emergency. The Security Officer reviews, tests, and updates the contingency plan annually.
- D. Other elements of contingency planning are found in [Section 6.16](#) – [Section 6.21](#).

6.16 Data Back-up Plan

Policy

The Security Officer develops a comprehensive plan to back up PHI and critical applications, or implements fault-tolerant systems that reduce the likelihood that equipment failure or disasters will adversely affect the integrity and availability of PHI.

Procedure

- A. Detailed back-up procedures are documented in the Toledo-Lucas County Health Department's contingency plan.
- B. These procedures create an exact copy of PHI at a given point in time.
- C. The detailed back-up procedures specify an interval for the creation of back-up data sets.
- D. Back-up copies of PHI are to be stored in a secure but accessible location as specified by the contingency plan.

6.17 Disaster Recovery Plan

Policy

The Toledo-Lucas County Health Department maintains back-up data sets that can be used to recreate data lost as a result of machine failure or other disaster.

Procedure

- A. Staff members who believe that a system failure or other disaster has resulted in the loss of information should report the possible failure to the Security Officer or on-duty staff member responsible for operating the information system.
- B. Technical staff members responsible for preparing back-up data sets test the back-up copies to ensure that they:
 - 1. Contain an exact copy of the information they back up
 - 2. Can be restored when needed
- C. The Security Officer determines when a back-up data set should be used to recreate or restore lost data. Procedures for restoring data are documented in the contingency plan.
- D. Staff members are notified of any data that are lost following restoration of the back-up data set.
 - 1. For example: a machine failure destroys information created since the last back-up. Staff members should be notified that these data have been lost. Back-up copies should be made available to users within one working day of being requested.

6.18 Emergency-mode Operation Plan

Policy

The Toledo-Lucas County Health Department has established procedures to safeguard the security of PHI during emergencies that impair normal security safeguards. The staff members responsible for creating and implementing these procedures are specified in greater detail in the agency's contingency plan.

Procedure

- A. The Security Officer develops detailed emergency-mode operating procedures as part of the comprehensive contingency plan.
- B. These procedures safeguard the provider's information resources and PHI during emergencies that disrupt normal security measures.
- C. During an emergency that disrupts power supplies, the Toledo-Lucas County Health Department's information systems are shut down.
- D. Power interruptions and other disasters that disrupt even these essential services are sufficient reason to close the provider's office until essential services have been restored.
- E. Patients requiring emergency treatment will receive stabilizing treatment and be transferred to a facility where adequate care can be provided.
- F. During power disruptions, staff members maintain paper records of information that would ordinarily be recorded electronically.
- G. After restoration of power, electronic databases are updated from these paper records. When an emergency condition exposes components of the provider's information system to theft or unauthorized removal, the Security Officer or a designated staff member is present to prevent loss of information or essential system components.
- H. A complete inventory of any damage to information system components is conducted after the emergency condition resolves.

6.19 Testing and Revision Procedures

Policy

Contingency plans are to be reviewed with staff members and tested, evaluated, and revised as necessary at least once every 12 months.

Procedure

- A. The Security Officer reviews contingency plans with all staff members to ensure that those responsible for implementing the plans are appropriately trained.
- B. New staff members responsible for implementing contingency procedures are thoroughly trained in these procedures.
- C. Back-up data sets are tested to verify that they contain exact copies of the information that they back up and that the back-up data can be successfully restored.
- D. Emergency power supplies are inspected and tested monthly or more frequently to confirm their ability to provide power for the time period specified in the provider's contingency plan.
- E. Fire alarms and fire-suppression equipment are inspected and tested every six months, or according to a schedule required by life-safety codes, to confirm that they will operate as intended and be available when needed.

6.20 Applications and Data Criticality Analysis

Policy

As part of the development of a comprehensive contingency plan, the Security Officer assesses the relative criticality of specific applications and data. Arrangements are made to ensure that critical applications and equipment are replaced within one work day in the event of failure. Critical data are backed up as provided in the back-up plan.

Procedure

- A. Every three years, the Security Officer analyzes all applications, computer hardware, and provider data to identify those applications, hardware components, and data sets that are critical to the organization's successful operations.
- B. The Security Officer reviews the criticality analysis and updates it as needed every year.
- C. The criterion for identifying critical components is whether rendering a component unusable or unavailable would significantly disrupt the Toledo-Lucas County Health Department's ongoing operations.
- D. To determine criticality, the Security Officer assesses the options for replacing the affected components.
- E. The analysis must identify components that must be quickly replaced or restored to operating condition during an emergency. It must also identify the longest potential period of time those critical components can be unavailable and the most cost-effective method of restoring function within the critical time period.

6.21 Evaluation

Policy

The Security Officer conducts comprehensive evaluations of the technical and nontechnical components of the Toledo-Lucas County Health Department's information systems to document compliance with federal and state security standards and to identify areas of noncompliance. Based on evaluations, the Security Officer develops and implements action plans to bring the provider to compliance with federal and state security regulations and standards.

Procedure

- A. The Security Officer prepares the evaluation using all necessary internal and external resources.
- B. The Security Officer prepares a comprehensive report documenting the findings of the evaluation and compliance action plan.
- C. The evaluation report is presented to the organization's management for approval.

6.22 Business Associate Contracts

Policy

A business associate that creates, receives, maintains, or transmits electronic PHI for the provider must provide satisfactory assurances that it will appropriately safeguard the information. These assurances must be included in a written contract or other arrangement with the business associate.

Procedure

- A. Written contracts or agreements must be established with all the business associates before the exchange or creation of PHI with or by the associate.
- B. All written contracts or agreements must contain the assurances identified in the Toledo-Lucas County Health Department's policies for business associate agreements, including the required termination provisions.

Section 7 – Physical Safeguards

7.1 Facility Access Controls

Policy

The Security Officer develops and implements policies and procedures that allow only authorized staff members and contractors to physically access the provider's electronic information systems. The areas of the practice's facilities in which components of its information systems are housed are physically secure and deny access to all but properly authorized staff members.

7.1.1 Contingency Operations

Policy

Only staff responsible for implementing specific aspects of contingency plans, including maintaining essential services during emergencies and monitoring unsecured areas housing components of the Toledo-Lucas County Health Department's information system, are permitted access to facilities during an emergency.

Procedure

- A. All staff members responsible for implementing contingency plans have keys, passwords, and other information or devices needed to gain access to information system components during emergencies.

7.1.2 Facility Security Plan

Policy

All computer equipment and devices that are used to access, transmit, or store PHI are protected from unauthorized physical access, tampering, and theft.

Procedure

- A. Network servers and storage devices are housed in a secure location that visitors to the practice cannot access. The equipment closet, office, or room in which such equipment is located is locked at all times.
- B. Back-up copies of PHI are stored in a secure location.
- C. Back-up media stored on-site are kept in locked cabinets.
- D. Back-up media stored off-site are stored so as to prevent physical access by anyone lacking proper authorization.
- E. Technology advancements and increased availability of technologies to the public will be periodically assessed to determine whether they pose a threat to security.

7.1.3 Access Control and Validation Procedures

Policy

All components of the Toledo-Lucas County Health Department's information system are housed in secure locations. Visitors to the department's office are accompanied by a staff member when in a position to access the provider's information resources. Consultants and contractors responsible for installing, maintaining, or testing computer equipment and software are authorized to access the agency's information systems as if they were staff members authorized to perform similar tasks or functions.

Procedure

- A. Components of the Toledo-Lucas County Health Department's information system other than workstations are located in secure, locked areas or cabinets.
- B. Only staff members authorized to use or service that equipment have keys to secure areas.
- C. All visitors to the department are to register with the receptionist and sign the visitor log, which includes:
 - 1. The name of the visitor
 - 2. The company or government entity represented by the visitor
 - 3. The purpose of the visit
 - 4. The time of arrival
 - 5. The person being visited
 - 6. The time the visitor leaved the facility
- D. Visitors to the provider are not left alone except in public waiting areas.
- E. Visitors should not be left alone in areas such as physician offices in which they may be able to access the provider's information system. Contractors and maintenance personnel who are not staff members sign the visitor's log but need not be accompanied by a staff member at all times when performing work covered by a business associate agreement.
- F. Contractors and maintenance personnel are given a unique user ID and password so that the practice can monitor their access to the agency's information resources.
 - 1. Before a user ID is activated, the Security Officer reviews with the contractor the provider's security policies and procedures and the provisions of the business associate agreement related to security.

7.1.4 Maintenance Records

Policy

All repairs and modifications to the physical components of the Toledo-Lucas County Health Department's facilities that are related to security (i.e. hardware, walls, doors, and locks) are documented in the agency's risk-assessment plan.

Procedure

- A. The Security Officer must approve in advance any modifications to the physical facilities housing the components of the agency's information system.
- B. The Security Officer will make needed changes to the risk-assessment and risk-management plan that reflect these changes in physical facilities.

7.2 Workstation Security

Policy

All staff and associates of the Toledo-Lucas County Health Department must follow all workstation use guidelines to maintain a secure workstation at all times.

Procedure

A. Guidelines on workstation use at Toledo-Lucas County Health Department are as follows:

1. All Workstations
 - i. All users must log off all workstations rather than leaving them unattended. This includes workstations in private offices.
 - ii. Screens should be positioned within the workstations so that they are visible only to the persons who use them.
2. Workstations in Private Offices
 - i. These workstations may be used to access all patient information, including both clinical information and billing information and to perform administrative functions related to computer security.
 - ii. Staff members should not access patient information when visitors, including patients, can view the information displayed on the screen.
3. Workstations in Common Non-Public Areas
 - i. A workstation at a nursing station is an example of this type of workstation.
 - ii. These workstations may be used to access all patient information, including both clinical information and billing information.
 - iii. Staff members should not access patient information when patients and other visitors to the practice can view the information displayed on the screen.
 - iv. These workstations should not be used to perform administrative functions related to security, such as adjusting settings to enable access to programs or data.
4. System Management Workstations
 - i. A workstation in an office housing a network server or storage is an example of this type of workstation.
 - ii. These workstations may be used to access all patient information, including both clinical information and billing information. However, patient information should be accessed from these workstations only when necessary to perform maintenance on, or to troubleshoot the information system.

7.3 Device and Media Controls

Policy

The Toledo-Lucas County Health Department will properly manage changes to storage media and equipment that create, maintain, or transmit protected health information.

7.3.1 Disposal

Policy

All [electronic media](#) – such as fixed and removable disk drives, rewritable CD-ROMs, and back-up tapes that are used to store PHI or information enabling security features of the provider’s information systems – are “sanitized” using the following procedures.

Procedure

- A. Before sale or disposal, all computer hardware is examined and certified as containing no PHI or information enabling security features of the department’s information system, including information that would enable a user to access the practice’s information system.
- B. All storage devices and media are to be given to the Security Officer for disposal. Only an authorized staff member may dispose of storage devices and media.
- C. Before disposal, the storage media are sanitized either by means of degaussing, triple overwriting, or physically dismantling and destroying the storage media.
- D. All CD-ROMs, including rewritable CD-ROMs, are rendered unreadable by abrading the data storage surface before disposal.
- E. All software and data are removed from all computer equipment prior to sale or disposal of the equipment. Disk drives are sanitized by degaussing or triple overwriting.
- F. Logs are maintained of all computer equipment and storage media that have been disposed of.
- G. These logs include the date on which storage media were sanitized and a description of the sanitizing method used.

7.3.2 Media Re-Use

- A. All storage media, including removable disks, rewritable CD-ROMs, and back-up tapes, are “sanitized” before re-use, either by means of degaussing or triple overwriting.

7.3.3 Accountability

Policy

A record is maintained of any movements of any movements of computer equipment within the organization and all removal of equipment and storage media from the Toledo-Lucas County Health Department. This policy applies to the transfer of storage media to off-site storage locations. This policy does not apply to routine shifting of equipment during ordinary operation or maintenance.

Procedure

- A. The Security Officer maintains an inventory of all computer hardware installed in the organization. The log includes:
 - 1. A description of the equipment
 - 2. The equipment serial number
 - 3. The date on which the equipment was installed
 - 4. The location of the equipment
 - 5. The name of the person responsible for installation

- B. Log entries are made in the inventory of computer hardware for all equipment that is removed from the department's facilities. The log entry includes:
 - 1. The date on which the equipment was removed
 - 2. The destination of the equipment
 - 3. The reason for removal, such as repair or disposal
 - 4. The person responsible for preparing equipment for removal and any sanitizing of storage devices

- C. When storage media are transferred to off-site storage facilities, a record is made of the date and time the media were removed from the facility and the date and time the media arrived at and were processed by the storage facility.

7.3.4 Data Backup and Storage

Policy

Before computer equipment is relocated within or removed from the Toledo-Lucas County Health Department's facilities, a back-up data set of any information contained on storage devices that are integral parts of a piece of computer equipment.

Procedure

- A. The staff members responsible for maintaining the computer equipment ensure that a complete back-up data set of any information contained on the equipment is made before the equipment is removed from or relocated with the agency's facilities.

Section 8 – Technical Safeguards

8.1 Access Control

Policy

The Security Officer ensures that the provider's information systems implement technical measures that permit access to the provider's information resources only by those persons who have appropriate authorization.

8.1.1 Unique User Identification

Policy

Every staff member authorized to use the provider's information systems is given a unique user name and selects a password known only to the staff member. Staff members must use their user name and password when using the information system and accessing PHI.

8.1.2 Emergency Access

Policy

The Toledo-Lucas County Health Department's computer equipment is configured to allow only staff members with appropriate authorization to access information stored on the computer and to configure software installed on the equipment.

Procedure

- A. Staff members who implement contingency plans must have authorization that enables them to repair equipment and implement emergency procedures.
- B. If user accounts must be deleted or disabled to repair equipment failures or restore functions during an emergency, the affected users are notified and new user names and passwords are established.
- C. The Security Officer maintains written record of so-called "administrator" user account names and passwords in a secure, locked file. An administrator user account has full authorization to configure equipment and software.

8.1.3 Automatic Logoff

- A. All workstations at the agency are configured to log users off after 10 minutes of inactivity to maintain secure access to the workstation. After being logged off, a user must re-enter his or her name and password to resume uninterrupted activity.
- B. Users may not disable this automatic logoff feature.

8.1.4 Encryption and Decryption

Policy

When the Security Officer deems it necessary, information transmitted outside the agency is [encrypted](#) to prevent use by unauthorized individuals.

Procedure

- A. Data should be encrypted when transmitted over a network that might be accessible by unauthorized individuals.
- B. Information that can be used to alter or defeat the agency's security measures also should be encrypted.
- C. The Security Officer determines the technical methods for implementing encryption and decryption.

8.2 Audit Controls

Policy

The Security Officer implements technical measures to create a record of information system activity, including user logon/logoff and startup/shutdown of technical security measures.

Procedure

- A. The Security Officer periodically reviews records of system activity to identify security problems and to evaluate compliance with security policies and procedures.

8.3 Integrity

Policy

The Security Officer implements procedures and technical measures to guard electronic health information from improper alteration or destruction. Staff members must follow these procedures and may not take any action to evade the technical measures.

Procedure

- A. The technical measures the Security Officer implements should permit PHI to be modified only by staff members with appropriate authorization.
- B. Applications used to create and modify PHI should support tracking of changed to records, including the identity of the staff member making the change, the nature of the change being made, and the date on which the change occurred.

8.4 Person or Entity Authentication

Policy

All users within the Toledo-Lucas County Health Department's information system must follow the various guidelines for person or entity authentication to maintain security and integrity of the system at all times.

Procedure

- A. All users must use their passwords when logging on to the provider's information system. Passwords should not be written down or disclosed to other members of the staff, friends, family, or anyone else.
- B. A staff member may not use another staff member's user name and password to access the provider's information system. Staff members may not give their passwords to other staff members.
- C. Passwords should comply with the guidelines in [Section 6.13](#).
- D. Users must change their passwords once they become known to others.
- E. Users should change their passwords at least once every year, but not so frequently that they are likely to be forgotten.

8.5 Transmission Security

Policy

The Security Officer implements technical measures to guard against unauthorized access to PHI that is being transmitted over an electronic communications network.

8.5.1 Integrity Controls

- A. Applications that transmit information electronically must include technical capabilities to ensure that the information received by the recipient is the information that was transmitted by the sender.

8.5.2 Encryption

- A. The Security Officer identifies any circumstances under which information transmitted by the practice must be encrypted to prevent its use by unauthorized recipients.
- B. The Security Officer ensures that staff members who transmit information are familiar with the encryption requirements and the use of encryption software.
- C. Staff who transmit information must encrypt it when directed to do so by the Security Officer.

8.6 Business Associate Contracts/Agreements

Policy

Contracts between the Toledo-Lucas County Health Department and business associates will provide for compliance with the HIPAA security regulations by the business associate and any agents.

Procedure

- A. Business Associate agreements must include the following provisions or provisions with an equivalent effect:
 1. Implementation of Security Safeguards
 - i. The business associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that is creates, receives, maintains, or transmits on behalf of the covered entity. These safeguards shall be equivalent or identical to the administrative, physical, and technical safeguards the covered entity is required to implement under the federal security and privacy regulations.
 2. Extension to Agents and Subcontractors
 - i. If the business associate uses an agent or subcontractor to perform any of the work covered under an agreement with the Toledo-Lucas County Health Department and such work involves the creation or use of PHI, the business associate enters into a written contract or agreement with the subcontractor or agent that includes the same safeguards required by the agreement between the agency and the contractor.
 3. Reporting
 - i. The business associate must be required to report to the provider any security incident of which it becomes aware.
 4. Contract Termination
 - i. The Toledo-Lucas County Health Department may terminate the contract with the business associate if the provider determines that the associate has violated a material term of the contract, including any provisions related to the security and privacy of PHI.

Section 9 – Breach Notification

9.1 Discovery of Breach

Policy

As soon as a breach of unsecured protected health information is discovered, it is the policy of the Toledo-Lucas County Health Department to take action. That action may vary based on the situation. But it will not be delayed for any reason.

Procedure

- A. The Privacy Officer designated official by the Privacy Officer will take action upon discovery of a breach.
- B. The action taken may involve investigating, conducting a risk assessment and, if appropriate, beginning notification procedures following the risk assessment.
- C. Under HIPAA breach notification regulations, a breach of PHI is to be treated as having been “discovered” on the first day the incident is made known to the organization, or, by exercising a reasonable amount of diligence would have been known to the organization.
- D. This also includes breaches the organization’s business associates make.

9.2 Breach Discovery

Policy

Any and all legitimate potential breaches of unsecured protected health information will be investigated by this organization.

Procedure

- A. The organization will name the Privacy Officer or designated official by the Privacy Officer to act as the investigator of the breach, unless there is a conflict of interest in the situation.
- B. This person is responsible for the entire process, from the initial investigation through the notification of the individuals and appropriate entities.

9.3 Risk Assessment

Policy

An inappropriate acquisition, use, disclosure, or access of information not likely to compromise protected health information is not actually considered a breach. To determine if an actual breach has occurred, a risk assessment must be performed.

Procedure

- A. When a potential breach has occurred, a risk assessment will be performed to determine if the protected health information has been compromised. The following questions must be answered during this risk assessment:
 - 1. What was the extent and nature of the information involved in the case?
 - 2. Who is the unauthorized person who received access to the information during the breach?
 - 3. Was the PHI actually acquired or viewed by the unauthorized person?
 - 4. Has the risk to the PHI been mitigated
- B. If there was a low probability of compromise, there is no breach. This must be documented in the investigation records.
- C. If a compromise was likely, the investigation will continue at that point.

9.4 Notification

Policy

If the organization determines that a breach has occurred, the Toledo-Lucas County Health Department will notify the individuals involved in the breach, as well as the Department of Health and Human Services, in the appropriate manner based on the breach. The media will also be informed if appropriate, based on the situation. This notification will be made in a timely manner, unless there is a delay due to law enforcement reasons.

Procedure

- A. Notice will be provided via first class mail to the individual at his or her last known address, or via email if he or she previously agreed to receive electronic communication from the organization.
- B. If the patient refused to receive both mail and electronic communications from the provider, the organization must call the patient and request that he or she pick up the written notice.
- C. If it is clear that the notice has not reached the individual or if there is no contact information available, a substitute notice may be used.
 - 1. If there are fewer than 10 individuals for whom there is incorrect or insufficient contact information, a substitute notice may be provided via telephone, an alternative written notice, or other appropriate means.
 - 2. If there are 10 or more individuals for whom there is incorrect or insufficient contact information, a substitute notice may be in the form of a posting on the main page of the practice website for 90 days, or printed in the local newspaper or via broadcast media. The notice must include a toll-free phone number that potential involved patients can call to determine if they were involved in the breach.
- D. Media Notice
 - 1. If a breach involved 500 or more patients, a notice must be provided in the form of a press release to the media.
 - 2. If the breach is widespread across a large area, such as state or a section of the country, a large prominent media outlet with a widespread circulation across that market area would be appropriate.
 - 3. If the breach is limited to individuals in a single city, a press release to the news media with circulation within just that city is appropriate.
- E. HHS Notice
 - 1. For breaches of 500 or more individuals, the organization will notify HHS as soon as it notifies the individuals.
 - 2. For breaches of fewer than 500, breaches will be maintained in a log and will be submitted no later than 60 days after the end of the calendar year in which the breaches were discovered.
- F. Timeliness of Notice

1. Once the Toledo-Lucas County Health Department determines that a notification must be made, it proceeds without unreasonable delay, and no later than 60 days after the discovery of the breach.
2. The only appropriate delay would be when law enforcement prohibits the organization from releasing the information about the breach.

9.5 Breach Information Log

Policy

It is the policy of the Toledo-Lucas County Health Department to maintain a detailed log of every breach of unsecured PHI to be reported to the Department of Health and Human Services at the end of the calendar year.

Procedure

A. A log must be maintained that contains the following detailed information:

1. A description of what exactly happened, the circumstances surrounding the breach
2. The date of the breach
3. The date of the discovery
4. The number of patients involved
5. A description of all types of unsecured PHI involved in the breach
6. The results of any risk assessment performed
7. A description of what types of notifications were made
8. Details of steps taken to resolve the situation and make corrective action/mitigation

Section 10 – Unique Identifiers

10.1 Patient Identifiers

Policy

As patients change third-party payers on a regular basis, it is important their identifying information is verified on a regular basis. It is the policy of the Lucas-County Health Department that we will verify patient insurance identifiers on at least an annual basis.

Procedure

- A. We will verify the insurance information of each patient annually, including patient ID number
 1. The patient will be asked to verify identifying information via a visual check of the patient information form kept in the chart.
 2. The patient will be asked to present an insurance card
 3. A copy of the insurance card will be kept with the patient's other billing information
 4. The patient will be asked about any possible secondary insurance or other pertinent identifying information the practice needs.
- B. These reviews will occur starting each January, and completed reviews will be noted in the chart and in the master patient index online to avoid requesting the same information from the patient twice.

10.2 Provider Identifiers

Policy

It is the policy of the Toledo-Lucas County Health Department to require that staff identified as health care providers and organization clinics identified as covered entities obtain a national provider identifier (NPI).

Procedure

- A. The Toledo-Lucas County Health Department will verify that all providers it employs have the appropriate national provider identifier (NPI) number.
- B. Any provider who does not yet have an NPI number will apply for one through the enumerator site at <https://nnpes.cms.hhs.gov/NPPES/Welcome.do>
- C. If changes need to be made to the information on a provider's NPI record, such as address, phone number, affiliation, etc. the Toledo-Lucas County Health Department will contact the enumerator to provide that information.

Section 11 – Transaction and Code Sets

11.1 Use of Standard Transactions

Policy

All of the following [transactions](#), when conducted electronically, will be in compliance with the federal standards for electronic transactions:

- A. Claim submission
- B. Claim status request
- C. Remittance advice and electronic fund transfer
- D. Coordination of benefits determination
- E. Eligibility and enrollment determination
- F. Referral authorization
- G. Health plan enrollment
- H. Health plan premium payment

11.1.1 Claim Submission and Coordination of Benefits

ASC X12N 837 – Health Care Claim: Institutional, Version 5010 (ASCX12N/005010X223), Effective 01/01/2012

ASC X12N 837 – Health Care Claim: Professional, Version 5010 (ASCX12N/005010X222), Effective 01/01/2012

ASC X12N 837 – Health Care Claim: Dental, Version 5010 (ASCX12N/005010X224), Effective 01/01/2012

NCPDP Telecommunications Standard Implementation Guide, Version D, Release 0 (version D.0),
Effective 01/01/2012

NCPDP Batch Standard Implementation Guide, Version 1, Release 2 (version 1.2), Effective 01/01/2012

Regulations

45 CFR 162.1102

45 CFR 162.1802

11.1.2 Claims Status Inquiries

ASC X12 276/277 – Health Care Claim Status Request and Response, Version 5010 (ASC X12N/005010X212)
Effective 01/01/2012

Regulation

45 CFR 162.1402

11.1.3 Remittance Advice and Electronic Funds Transfer

ASC X12N 835 – Health Care Claim Payment/Advice, Version 5010 (ASCX12N/005010X221),
Effective 01/01/2012

NACHA Corporate Credit of Deposit Entry with Addenda Record (CCD+), Effective 01/01/2014

NCPDP Telecommunication Standard Implementation Guide, Version D, Release 0 (version D.0),
Effective 01/01/2012

NCPDP Batch Standard Implementation Guide, Version 1, Release 2 (version 1.2), Effective 01/01/2012

Regulation

45 CFR 162.1602

11.1.4 Referral Authorization

ASC X12N 278 – Health Care Services Review – Request for Review and Response, Version 5010 (ASCX12N/005010X297), Effective 01/01/2012

Regulation

45 CFR 162.1302

11.1.5 Eligibility Transactions

ASC X12N 270/271 – Health Care Eligibility Benefit Inquiry and Response, Version 5010 (ASCX12N/005010X279), Effective 01/01/2012

NCPDP Telecommunications Standard Implementation Guide, Version D, Release 0 (version D.0), Effective 01/01/2012

NCPDP Batch Standard Implementation Guide, Version 1, Release 2 (version 1.2), Effective 01/01/2012

Regulation

45 CFR 162.1202

11.1.6 Health Plan Enrollment

ASC X12 834 – Benefit Enrollment and Maintenance, Version 5010 (ASCX12N/005010X220), Effective 01/01/2012

Regulation

45 CFR 162.1502

11.1.7 Premium Payment

ASC X12N 820 – Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 5010 (ASCX12N/005010X218), Effective 01/01/2012

Regulation

45 CFR 162.1702

11.2 Testing and Certification of Compliance with Federal Transaction Standards

Policy

Staff members responsible for selecting, installing, operating, and maintaining information systems used to conduct electronic transactions will certify, or obtain certification from vendors, that the systems are able to conduct transactions electronically that comply with the federal standards.

11.3 Trading Partner Agreements

Policy

All contracts or agreements with trading partners will include provisions that comply with federal regulation for trading partner agreements. These provisions:

- A. Describe duties and obligations of both parties to the agreement, including any responsibilities for safeguarding the security and privacy of the information the two parties exchange
- B. Require electronic transactions to be conducted in compliance with the federal standards for electronic transactions
- C. Prohibit any addition or modification of the data elements to a standard transaction
- D. Prohibit any use of codes that are not specified in a federal standard transaction code set
- E. May specify processing instructions for completing transactions between provider and a third-party payer such as specific codes that, if present, will result in the rejection of the transaction

Regulation

45 CFR 162.915

11.4 Updating Code Sets and Practices

Policy

Staff members responsible for coding claims will use only codes contained in the federal transaction code sets. Staff will update code sets when new code sets are issued.

Regulation

45 CFR 162.1000

11.4.1 Diagnosis Coding

Diagnoses must be coded using the International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM diagnosis codes).

11.4.2 Physician Services Coding

Physician services and surgical procedures must be coded using *Physician's Current Procedural Terminology* (CPT).

11.4.3 Dental Services Coding

Dental services must be coded using the American Dental Association's *Code on Dental Procedures and Nomenclature* (CDT).

11.4.4 Other Health-related Services Coding

Most other health-related services must be coded using the Healthcare Common Procedure Coding System (HCPCS Level II).

11.4.5 Drug Coding

- A.** Drugs must be coded using National Drug Codes (NDC). In some instances, drugs are coded using HCPCS Level II codes in the physician office setting for appropriate billing to third party payers.

Record of Change

(Required for all policies)

Date of Change	Changes Made By	Changes Made/Notes	Approved By
7/20/2018	BP	Updated reference from "Supervisor of Clinics" to "Privacy Officer" where applicable. Added page numbers. Added Record of Change.	Reference Update