Revised February 2014

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
HIPAA and HITECH
LARAMIE COUNTY COMMUNITY COLLEGE
DENTAL HYGIENE PRIVACY AND SECURITY POLICIES AND PROCEDURES

LARAMIE COUNTY COMMUNITY COLLEGE DENTAL HYGIENE
HIPAA & HITECH POLICIES AND PROCEDURES
TABLE OF CONTENTS

DEFINITIONS AND CONCEPTS OF HIPAA RELATED TERMS

(Terms are Listed Alphabetically and Underlined)
Throughout this document, the following terms are used:

Academic Dental Hygiene Practice (a.k.a., Dental Practice) – reference to the "academic dental hygiene practice" is meant to describe the dental hygiene clinical practice on campus that is a HIPAA covered entity and serves as a learning environment for our dental hygiene and dental assistant students. Dental practice may also be used in lieu of academic dental hygiene practice, with the intention of the description being one and the same.

Business Associate – Generally means an entity, or a person who is not a member of the dental practice's workforce, that performs a service for the dental practice involving patient information. Examples of business associates include a billing service, collection agency, accounting or law firm; consultant, health information organization, e-prescribing gateway, data transmission company that requires access to patient information on a routine basis; and a company that offers patients personal health records on behalf of the dental practice. A dental practice must have a business associate agreement in place with each of the dental practice's business associates. A business associate subcontractor that has access to patient information is treated as a downstream business associate. A business associate must have a business associate agreement in place with each of the business associate's subcontractors.
A health care provider, such as a dental laboratory, does not become a business associate when a dental practice discloses patient information to the health care provider for treatment purposes. However, a health care provider may be a business associate of a dental practice if the health care provider performs a service for the dental practice rather than providing treatment for a patient. For example, a dental practice would need a business associate agreement with a health care provider that accesses the dental practice's patient information for purposes of providing training to the dental practice's workforce. 45 CFR § 160.103.

Covered Entity –A covered entity means:

1. A health plan

2. A health care clearinghouse

3. A healthcare provider (such as a dental practice) that transmits any health information in electronic form in connection with a transaction covered by HIPAA 45 CFR § 160.103

Data Set – Means a semantically meaningful unit of information exchanged between two parties to a transaction 45 CFR § 162.103.

De-identified – In general, patient information is "de-identified" if 18 identifiers are removed, and the remaining information cannot be used alone or in combination with other information to identify the patient. HIPAA does not apply to properly de-identified information.

The **18 identifiers are**: names, street address other than town, city, state, and zip code, telephone numbers, fax numbers, email addresses, social security numbers, medical records numbers, vehicle identifiers and serial numbers, including license plates, device identifiers and serial numbers, full face photographs or comparable images, URL's, IP address numbers, Biometric identifiers (includes finger and voice prints).

Designated Record Set or Record – Means any item, collection, or grouping of information that includes patient information and is maintained, collected, used or disseminated by or for the dental practice. Several of patient rights under HIPAA apply only to patient information in a "designated record set".
Example, a patient has a right to:

- See information about the patient that the dental practice maintains in a designated record set, and/or get copies of information about the patient that the dental practice maintains in a designated record set

- Have the dental practice amend, when appropriate, information or a record about the patient in a designated record set

HIPAA – When reference is made to "HIPAA", it is an abbreviation for HIPAA Privacy, Security and Breach Notification Rules and stands for **Health Insurance Portability and Accountability Act**.

Limited Data Set – A limited data set is a limited set of identifiable patient information as defined in the Privacy Regulations issued under the Health Insurance Portability and Accountability Act. This limited data set of information may be disclosed to an outside party without a patient's authorization if certain conditions are met. First, the purpose of the disclosure may only be for research, public health, or health care operations. Second, the person receiving the information must sign a data use agreement with Laramie County Community College. This agreement has specific requirements which are discussed as follows:
A limited data set is information from which specific "identifiers" have been removed. Specifically, as it relates to the individual or his or her relatives, employers, or household members, **all of the following identifiers must be removed in order for health information to be in a state of limited data set. Those identifiers are:**

- Names
- Street addresses (other than town, city, state, and zip code)
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical records numbers (chart numbers)
- Health plan beneficiary numbers
- Account numbers
- Certificate license numbers
- Vehicle identifiers and serial numbers, including license plates
- Device identifiers and serial numbers
- Full face photographs or comparable images
- URL's
- IP address numbers
- Biometric identifiers (includes finger and voice prints)

The health information that may remain in the information disclosed includes:
- Dates such as DOB or DOD, appointment dates (however, see note below)
- City, state, five digit or more zip code
- Ages in years, months or days or hours

It is important to know that this information is still protected health information or PHI under HIPAA. It is not de-identified information and is still subject to the requirements of the Privacy Regulations.

Data Use Agreements
Because a limited data set is still PHI, the Privacy Regulations contemplate that the privacy of individuals will be protected by requiring covered entities (Laramie County Community College) to enter into data use agreements with recipients of limited data sets. The data use agreement must meet standards specified in the Privacy Regulations. A data agreement must:

- Establish the permitted uses and disclosures of the limited data set

- Identify who may use or receive the information
- Prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as permitted by law
- Require the recipient to use appropriate safeguards to prevent a use or disclosure that is not permitted by the agreement
- Require the recipient to report to the covered entity any unauthorized use or disclosure of which it becomes aware
- Require the recipient to ensure that any agents (including subcontractors) to whom it provides the information will agree to the same restrictions as provided in the agreement
- Prohibit the recipient from identifying the information or contacting the individuals

The limited data set provisions also require covered entities to take reasonable steps to cure any breach by a recipient of the data use agreement. That is, if Laramie County Community College determines that data provided to a recipient is being used in a manner not permitted by the agreement, it must work with the recipient to correct this problem. If these steps are unsuccessful, Laramie County Community College would have to discontinue disclosure of PHI to the recipient under the data use agreement and report the problem to the Department of Health and Human Services (HHS.gov).

(Creating the Limited Data Set)
A covered entity (Laramie County Community College) may use one of its own workforce to create the limited data set. The Department of Human Services also has indicated that a covered entity may allow a person requesting a limited data set to create it, as long as the person is acting as a business associate of the covered entity. A business associate is someone who is not part of the covered entity's workforce but who will use the covered entity's PHI to perform some task on behalf of the covered entity. Examples of business associates are Eagle Soft Software from the company Patterson Dental, ADA Commission on Accreditation for accreditation information, lawyers and firms that analyze patient data, etc. The covered entity (Laramie County Community College) must enter into a separate business associate agreement with the entity and the agreement must meet the requirements of the Privacy Regulations. Once the limited data set is created under the business associate agreement, all of the PHI, other than the PHI qualifying as the limited data set under the data user agreement must be returned to the covered entity. It is possible that someone will act as the covered entity's business associate to create the limited data set from a broader set of PHI. In such a case, the recipient will need to sign both a data use agreement and the business associate agreement.

Responsibility for Data Use Agreements

A. When Laramie County Community College (LCCC) is the provider of the data:

LCCC has drafted a data use agreement for use by those who wish to disclose limited data set to recipients.

B. When LCCC is the recipient of the data: If LCCC is the recipient of limited data set of PHI from a non-LCCC source, the recipient may be asked to sign the other party's Data Use Agreement. In this case, the recipient is responsible for reviewing the Data Use Agreement and determining if it complies in material terms with the Data Use Agreement template. If the other party's Data Use Agreement is significantly different from the LCCC Data Use Agreement template, or if there is any uncertainty, the LCCC General Counsel is to be consulted.

Tracking and Accounting
Disclosures of a limited data set are not subject to the HIPAA tracking/accounting requirements. The rationale appears to be that the marginal increase in privacy protections that such an accounting would provide is outweighed by its burdens. The Department of Health and Human Services has taken the position that the privacy of individuals regarding PHI disclosed in a limited data set can be adequately protected through a signed data use agreement.

Disclosure – Means releasing, transferring, providing access to, or divulging information in any manner outside the dental practice or other entity holding the information 45 CFR § 160.103
We do not sell personal health information or disclose it to companies that wish to sell a patient their products. We must have written permission (called an "authorization") to use and disclose a patient's health information, except for the uses and disclosures described below.

- **You and Your Personal Representative**. We may disclose your health information to you or your personal representative (an individual who has the legal right to act on your behalf).

- **Others Involved in Your Care**. We may share your health information with family members or friends who are directly involved in your medical care, or the payment of your medical care, when you are present and have given us verbal or written permission. We will not discuss your health information with your family or friends if you are not present, unless you have given us your permission or we believe it is in your best interest. Our health professionals will exercise their professional judgment in determining when friends and family members may receive health information (e.g., a family member picking up radiographic images, will require written permission).

- **Treatment**. We may use your health information or disclose it to third parties to aid with your medical treatment. We may disclose health information about you to doctors, nurses, pharmacists, technicians, dental hygiene or dental assistant students, or other persons who are involved in taking care of you.

- **Payment**. We may use your health information or disclose it to third parties, including the subscriber, in order to obtain payment for your dental treatment, to determine your eligibility for benefits, or to coordinate your benefits with other plans. For example, we may discuss your health information with your doctor to obtain a prior approval for a dental procedure or to determine whether our health plan will cover the treatment. Similarly, we may use or disclose your health information to others to assist with adjudication of health claims or to coordinate benefits with other health coverage you may have. Also, we may share information with a medical provider to determine whether a particular treatment is medically necessary, experimental, or investigational. We will send to the member an explanation of benefits indicating the amount the health plan has paid for medical services provided to the member, his or her covered spouse and other covered dependents.

- **Health Care Operations**. We may use your health information and disclose it to third parties who help us with the day-to-day management of our health care services, providers, and pharmacies. These uses and disclosures are allowed under HIPAA's definition of Treatment, Payment, and Operations (TPO) and ensure that you receive quality care. For example, we may use your health information to conduct quality assessment and improvement activities, review the performance of our clinic, conduct and arrange for accreditation review, legal services, and auditing activities, business planning and development, and other general dental care delivery and health plan administration activities. However, we will not use your genetic information for any underwriting or eligibility purposes.

- **Appointment Reminders and Health Related Benefits and Services**. We may use and disclose your health information to remind you about appointments for dental care in our offices.

- **Marketing**. We do not use protected health information for marketing.

- **As Required By Law**. We will disclose your health information to third parties when required to do so by federal, state or local law. For example, we may share your health information when required to do so by state workers' compensation law, the Department of Health and Human Services, or state regulatory officials.

- **To Avert A Serious Threat To Health Or Safety**. We may use and disclose your health information to third parties when it is necessary to prevent a serious threat to your health and safety or to the health and safety of the public or another person. Any disclosure, however, would only be to someone able to assist in preventing the potential harm.

- **Lawsuits and Disputes**. If you are involved in a lawsuit or a dispute, we may disclose your health information in response to a court or administrative order. We may also disclose your health information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only after we make efforts to inform you of the request or to obtain an order protecting the requested information. If you are a party to a lawsuit in a Wyoming court case, a court order or your authorization must be provided to release your health records (in addition to a subpoena).

- **Public Policy Matters**. We may use or disclose your health information in certain limited instances for matters involving the public welfare, such as:

- For public health risks (e.g., prevention or control of disease, reporting births and deaths, reporting abuse and neglect) or for research purposes when there are sufficient privacy protections in place.

- To a health oversight agency for activities authorized by law (e.g. audits, investigations, inspections, and licensure necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

- To law enforcement officials (in response to a court order, subpoena, warrant, summons or similar process or to report certain kinds of crimes) and to national security officials under certain limited circumstances.

- To a funeral director, coroner, or medical examiner to permit them to carry out their duties

- To facilitate organ donation and specified research purposes, so long as certain safety measures are in place to protect your privacy.

- **Employers and Plan Sponsors**. In order for you to be enrolled in a health plan, we may share limited information with your employer or other organizations that help pay for your dental health coverage. However, if your employer or another organization that helps pay for your health coverage asks for specific health information, we will not share your health information unless they first obtain your written authorization.

- **Business Associates**. We hire third parties to provide us with various services that are necessary for our dental clinic to function. Before we share your health information with these companies, we will have a written contract with them in which they promise to protect the privacy of your health information.

- **Other Uses and Disclosures of PHI**. We have no plans to use or disclose your health information for purposes other than those provided for above or as otherwise permitted or required by law. If you provide us an authorization to use or disclose your health information to third parties, you may revoke the authorization, in writing, at any time. If you revoke your authorization, we will no longer use or

disclose your health information for the reasons covered by your written authorization. Please remember that we are unable to take back any disclosures we have already made with your authorization.

- **Health Care Operations** – This is a "broad" category of dental practice activities such as business management and general administrative activities of the dental practice (for example, HIPAA compliance, customer service, resolving internal grievances, the sale of the practice to another covered entity (or to an entity that will become a covered entity following the sale) and due diligence related to the sale, and de-identifying PHI). Other examples include business planning and development (such as cost management and planning related analyses), conducting quality assessment and improvement activities, certain patient safety activities, case management and care coordination, reviewing the competence or qualifications of health care professionals and student practitioners, conducting training programs in which health care students, trainees, or practitioners learn under supervision, training of non-health care professionals, licensing and credentialing activities, arranging for legal services, and auditing (including fraud and abuse detection and compliance programs). To determine whether an activity is a health care operation, consult the full definition in 45 CFR § 160.103.

- **Minimum Necessary** – When a dental practice uses or discloses patient information or requests patient information from a health care provider, health plan, clearinghouse, or business associate, the dental practice must make reasonable efforts to limit the patient information to the minimum amount necessary.

Exceptions: Minimum necessary does NOT apply in the following situations:

- Disclosing patient information to a health care provider for treatment purposes
- Requesting patient information from a health care provider for treatment purposes
- Disclosing a patient's information to the patient or personal representative
- When a patient has signed an authorization form for the use or disclosure
- Disclosures to the U.S. Department of Health and Human Services (HHS)
- Uses and disclosures required by law
- Uses and disclosures required in order to comply with the Privacy Rule
- A dental practice may not access, use, disclose or request a patient's entire dental record unless the entire dental record is needed to accomplish the purpose of the use, disclosure, or request, or unless one of the above exceptions applies.

Office of Civil Rights – a.k.a., OCR 10

Payment – Generally means the dental practice's activities to obtain reimbursement or compensation for service performed or products provided and a provider's activities to collect. Examples of "payment" activities include things like determination of eligibility or coverage, coordination of benefits, determination of cost sharing amounts, billing, claims management, collection activities, review of medical necessity, coverage, appropriateness of care or justification of charges, utilization review, including precertification and preauthorization, concurrent and retrospective review of services, and disclosure of limited information to consumer reporting agencies relating to collection of premiums or reimbursement (names and addresses, date of birth, Social Security number payment history, account number, and name/address of health care provider and/or health plan). 45 CFR § 164.501.

Protected Health Information or PHI –Protected health information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media and includes information transmitted or maintained in any other form or medium. The abbreviation "PHI" in this manual is intended to mean "protected health information" ("PHI"). Most patient information is PHI, including dental records, health histories, billing records, radiographs, full-face photographs, and even "demographic" information such as patient names, addresses, phone numbers, email addresses, genders, etc.

Patient – The HIPAA rules refer to "individuals." For a dental practice, this usually means the patient and that term is used in this manual. HIPAA protects information about both current and former patients, and that in some cases other people, such as a patient's legal representative, or the parents or guardians of minor children, have rights under HIPAA.

Use – We have no plans to use or disclose health information for purposes other than those provided by law. If a patient provides an authorization to use or disclose health information to third parties, that authorization may be revoked, in writing, at any time. If authorization is revoked, Laramie County Community College will no longer use or disclose the patient's health information for the reasons covered by the written authorization. Laramie County Community College is unable to take back any disclosures already made with a patient's authorization.

Workforce Employee – The LCCC dental hygiene clinic workforce employee means employees, volunteers, students, trainees, and other persons whose conduct, in the performance of work for a dental practice, is under the direct control of the dental practice, whether or not they are paid by the dental practice. A business associate's workforce means the business associate's employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the business associate, is under the direct control of the business associate, whether or not they are paid by the business associate. 45 CFR § 160.103. 11

2013 FINAL RULE

INTRODUCTION

On January 25, 2013, the federal government published changes to the HIPAA rules that require covered dental practices (such as the Laramie County Community College Dental Hygiene Clinic, a.k.a. dental practice) to update compliance programs.

Effective and Compliance Dates

The changes are effective March 26, 2013, but dental practices have until September 23, 2013 to come into compliance.

All business associate agreements entered into on or after January 25, 2013 must be compliant with the new requirements by September 23, 2013, but a transition period until September 22, 2014 applies to certain agreements that were in place on January 25, 2013

The increased civil money penalties have been in effect since 2009, and apply to HIPAA violations occurring on or after February 18, 2009.

HISTORY

Purpose of the Law

Congress passed the HIPAA law in 1996 to require national standards for electronic health care transactions and code sets. Since Congress recognized that advances in electronic technology could erode the privacy of health information, Congress added provisions to the law requiring Federal privacy protections for patient health information. These provisions led the government to adopt the HIPAA Security and Privacy Rules. The rules have been strengthened over time. For example, the 2009 HITECH ACT required the Breach Notification Rule and other enhancements to HIPAA that were intended to enhance public confidence in the privacy of patient information as health care providers increased their use of electronic health record (EHR's). Many of the HITECH enhancements are embodied in new regulations issued on January 25, 2013 ("the Final Rule").

Compliance Dates

Dental practices were required to comply with the Privacy Rule beginning in 2003. Security Rule compliance began in 2005. In 2009, the Breach Notification Rule came along, and the government increased penalties for HIPAA violations and strengthened HIPAA enforcement.

State Law

A dental practice's HIPAA program must comply with both HIPAA and applicable state law. If a state is not contrary to HIPAA, a dental practice must comply with both HIPAA and the state law. If a state law is contrary to HIPAA, a dental practice must comply with the state law if the state law is "more stringent" than HIPAA. In general, state law is more stringent than HIPAA if the state law relates to the privacy of patient information and provides greater privacy protection for patient information or greater rights to patients with respect to that information.

For example, HIPAA requires a dental practice to act within 30 days if a patient asks to see or get copies of certain patient information. If state law requires a dental practice to act on such a request in a shorter time frame, it would be more stringent than HIPAA.

Enforcement

Federal government enforcement of HIPAA used to be complaint driven. For example, if a patient complained to the federal government that a dental practice was not complying with HIPAA, the government could investigate and could impose penalties or corrective action. While this is still the case, the federal government now has expanded enforcement responsibilities and has the authority to conduct HIPAA audits that are not generated by a patient complaint or other information indicating possible noncompliance. The federal government may also investigate breaches that are reported to the US Department of Health and Human Services (HHS) in accordance with the Breach Notification Rule. The Office for Civil Rights, an agency of HHS, is responsible for federal HIPAA enforcement.

In addition to federal enforcement, the HITECH Act of 2009 gave state attorneys general the authority to bring civil actions on behalf of state residents for violations of the HIPAA privacy and Security Rules. State attorneys general have the authority to obtain damages on behalf of state residents and to enjoin further violations of the HIPAA Privacy and Security Rules. More information can be found at www.hhs.gov/ocr/privacy/hipaa.

Penalties

In the beginning, civil money penalties for a dental practice that did not comply with HIPAA were limited to $100 or less per violation, up to an annual cap of $25,000 for all violations of the same HIPAA requirement or prohibition. Today, there are tiered penalty amounts for increasing levels of culpability, up to an annual cap of $1.5 million for all violations of the same HIPAA requirement or prohibition. If a violation was due to willful neglect and was not corrected within 30 days, there is a minimum penalty of $50,000 per violation.
Applies to: All covered entity dental practices of which Laramie County Community College Dental Hygiene Clinic is a covered entity. Effective date: The increased penalties apply to HIPAA violations occurring on or after February 18, 2009

Background:

OCR has the right to impose civil money penalties on dental practices that violate HIPAA. Some HIPAA violations carry criminal penalties, including fines and imprisonment. OCR also has the authority to require a dental practice to take corrective action, including instigating a formal (and costly) Corrective Action Plan if OCR finds the dental practice noncompliant.
The new rule has tiered penalty amounts for increasing levels of culpability, up to an annual cap of $1.5 million for all violations of the same HIPAA requirements or prohibition. If a violation was due to willful neglect and was not corrected within 30 days, there is a minimum penalty of $50,000 per violation.

Violation Category	**Penalty Range Per Violation**	**Maximum Penalty for All Such Violations of Identical Provisions in a Calendar Year**
Did not know	$100 - $50,000	$1.5 million
Reasonable cause	$1,000 - $50,000	$1.5 million
Willful neglect, timely corrected	$10,000 - $50,000	$1.5 million
Willful neglect, not timely corrected	$50,000	$1.5 million

How violations are counted.

If a HIPAA violation continues for a number of days, (for example, if appropriate safeguards are lacking for a number of days), the number of identical violations may be counted on a **PER DAY BASIS**. OCR considers the number of affected individuals and HIPAA requirements violated. For instance, usually with a breach of unsecured patient information there will be both (1) an impermissible use or disclosure and (2) a safeguards violation, and OCR may calculate a separate civil money penalty for each. As such, a dental practice may be liable for multiple violations of multiple requirements, up to a cap of $1.5 million for **EACH** requirement.

Aggravating and mitigating factors.

HIPAA contains a list of aggravating and mitigating factors that can affect the amount of civil money penalty. The new rule requires the government to consider the factors when determining the amount of a penalty for a HIPAA violation.
The OCR will determine the amount of a penalty on a case-by-case basis, depending on the nature and extent of the violation and the nature and extent of the resulting harm, as well as other aggravating and mitigating factors listed in 45 CFR 160.408. Examples of the factors include:

- The number of individuals affected
- Whether the violation caused physical, financial, or reputational harm or hindered a patient's ability to obtain health care
- The dental practice's history of prior compliance or non-compliance

- The financial condition of the dental practice
- Whether the imposition of civil money penalty would jeopardize the dental practice's ability to continue to provide health care.
- The size of the dental practice

LARAMIE COUNTY COMMUNITY COLLEGE DENTAL HYGIENE
POLICY STATEMENT

THE LARAMIE COUNTY COMMUNITY COLLEGE DENTAL HYGIENE CLINIC IS DEFINED AS A HEALTH PROVIDER AND A COVERED ENTITY BY HIPAA. WE CONDUCT CERTAIN FINANCIAL, ADMINISTRATIVE, EDUCATIONAL, AS WELL AS DENTAL RADIOGRAPHIC IMAGES (DENTAL X-RAYS) TRANSACTIONS ELECTRONICALLY, AND POSSESS INDIVIDUAL IDENTIFABLE HEALTH INFORMATION. WE WILL COMPLY WITH ALL OF THE REQUIREMENTS OF THE HIPAA PRIVACY RULE 2013.

LARAMIE COUNTY COMMUNITY COLLEGE DENTAL HYGIENE CLINIC OR PARTIES EMPLOYED OR INVOLVED IN ACADEMIA RELATED TO DENTAL HYGIENE PATIENT CARE AND THE DENTAL HYGIENE CLINIC WILL NOT DISCLOSE PROTECTED HEALTH INFORMATION TO NON-HEALTH CARE ENTITIES WITHOUT A SIGNED PATIENT AUTHORIZATION OR OTHER HIPAA PERMISSION FORMS. LARAMIE COUNTY COMMUNITY COLLEGE DENTAL HYGIENE CLINIC WILL INSTITUTE APPROPRIATE SAFEGUARDS TO PREVENT IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION.

Confidentiality of PHI

A. Coverage

Laramie County Community College Dental Hygiene (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

August 2014

C. Purpose

To define the Organization's Confidentiality Policy and the use of confidential communications.

D. Policy

All Organization workforce members who have access to or disclose sensitive or confidential patient information (also referred to as *protected health information (PHI)* or *electronic protected health information (ePHI)* by Health and Human Services and in HIPAA law) have a responsibility to maintain at all times the confidentiality of this information.

Examples of sensitive or confidential information include, but are not limited to the following types of information:

1. Patient demographics or financial information
2. Medical Records, diagnostic or clinical records in general
3. Employee
4. Payroll
5. Billing
6. Contract
7. Medical Staff

Access to, or disclosure of PHI/ePHI must be controlled and monitored by the Organization at all times.

Organization in General

The policy of the Organization is to maintain patient confidentiality when using Protected Health Information (PHI/ePHI) in any form, including, but not limited to the following:

1. Verbal communications
2. Hard copy records (charts)
3. Electronic records
4. Printouts pertaining to the patient
5. Notes maintained by faculty, staff, or students providing care to the patient
6. White boards
7. Patient sign-in sheets
8. Message logs

9. Inquiries or information from payers
10. Faxed patient information
11. Diagnostic testing/results, radiographs
12. Printed patient information
13. Electronic copies of patient information
14. Data Exchanged copies of patient information
15. E-mails, letters or other individual (patient) communications / disclosures of PHI

The Organization applies HIPAA-based security measures (i.e. password protection and encryption) to prevent unauthorized users from accessing patient and other information in computerized data systems.

In addition, the Organization does the following to protect patient confidentiality:

1. Restricts the amount of information released in response to calls about current patients.
2. Responds to and follows all proper individual (patient) requests for confidential communications; Confidential communications can be facilitated through a number of different mechanisms. This Organization's workforce will work with the individual (patient) to create a confidential atmosphere for communications of their PHI according to their guidelines as to the method, format and receiving parties of these communications.
3. Incorporates into its Policies and Procedures, existing laws and additional protections for highly sensitive information, such as treatment records.
4. Provides training on privacy and security policies and practices to all workforce members annually.
5. Applies appropriate sanctions when violations of this policy occur.

Departmental Responsibilities

Each organizational unit within the Organization is responsible for enforcement of policies, standards, and practices set forth by the Organization to maintain patient confidentiality.

Management responsibilities shall include, but are not limited to the following:

1. Secure storage of patient information.
2. Procedures for release of patient information to third party payers, providers, etc.)
3. Procedures for disposal of hard copy records and electronic records.
4. Secure transmission and storage of electronic records.
5. Protection of confidential information from access, use, or dissemination by unauthorized persons.
6. Use of confidential communications as agreed to by the Organization from an individual (patient) request.
7. Monitoring that access to PHI is secured, controlled, documented and closely managed and in accordance with written policies and procedures.
8. Auditing for inappropriate access and use of PHI by individuals and workforce members.

Individual Responsibilities

All Organization workforce members and vendors are responsible for adhering to this and related information security policies and standards and for safeguarding all confidential patient information. These responsibilities shall include, but are not limited to, the following:

1. Avoid access, retrieval, or use of any information on a current or former patient unless authorized for legitimate job related duties (i.e. assisting in care/treatment, providing a consultation, or approved educational research or business purposes) within the Organizational unit.
2. Limit the access, use, and disclosure of protected health information to the minimum amount

necessary to accomplish the intended purpose.

3. Interact with individuals (patients) to determine the best methods and formats for confidentially communicating with them, especially upon, but not necessarily as a result of their specific request.
4. Dictate patient notes and discuss patient care only in private areas (i.e. not in hallways, elevators, cafeteria lines).
5. Protect personal User ID and password used to access the Organization's data *Systems* from disclosure to others.
6. Take special care to protect information (e.g. in hard copy charts, printouts or on computer screens) from being viewed by unauthorized persons.
7. Use secure methods for authorized storage, transmission, disclosure and disposal of confidential PHI.

Employees are responsible for reporting to the HIPAA Privacy and Security Officer Dental Hygiene Director; 307-778-1386 any known or suspected internal /external violation of Organization privacy policies or any wrongful use or disclosure of PHI.

E. Definitions

Breach of PHI:
Section 13400 HITECH
(1)(A) Breach – (is the) unauthorized acquisition, access, use, or disclosure of' PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
(B) Exceptions – Breach does not include

(i) any unintentional acquisition, access or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if

(I) such acquisition was made under good faith and within the course and normal scope of employment or professional relationship…with CE or BA

(II) such information is not further acquired, accessed or used

(ii) any inadvertent disclosure for an individual who is otherwise authorized to access PHI at a facility operated by a CE or BA…

(iii) any such information received as a result of such disclosure is not further acquired, accessed, etc.

Electronic Health Record: An EHR (electronic health record) is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Personal Health Record: A PHR (personal health record) is managed, shared, and controlled by or primarily for the individual

F. Related Polices:

- 21s - HIPAA Violation and Breach
- 26s - Sanctions, Enforcement and Discipline
- 6s - Appropriate Access of PHI by Workforce
- 11s - Disclosure of PHI

LARAMIE COUNTY COMMUNITY COLLEGE DENTAL HYGIENE PROGRAM
PRIVACY AND SECURITY POLICIES AND PROCEDURES
FOR HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT)

I. PRIVACY OFFICER 45 CFR 164.530 (a) & 45 CFR 164.524 (e) (2)

POLICY:
Our dental practice's Privacy Officer shall be responsible for developing and implementing our HIPAA privacy and breach notification policies and procedures, receiving complaints about our privacy and breach notification practices, providing further information about our Notice of Privacy Practices, and receiving and processing requests for access, amendment, and accountings of disclosure.
(See Privacy Officer Job Description in Appendix)

PROCEDURE:
Staff Duties – Our Privacy Officer is responsible for developing privacy and breach notification policies and procedures and putting them into action. Examples of these policies and procedures include how to protect patient privacy, how you are permitted to use, disclose and request information about patients, and how to respond to requests from patients and others concerning dental records and other information.

Privacy Officer Duties – The Privacy Officer is responsible for developing and implementing privacy and breach notification policies and procedures and updating them as appropriate. The policies and procedures will apply to patient information in oral, written and electronic form. Your duties include, but are not limited to, the responsibilities in the Privacy Officer job description (see Appendix).

II. PRIVACY POLICIES AND PROCEDURES (45 CFR 164.530 (i)

POLICY:
Our dental practice will develop and implement policies to comply with the HIPAA Privacy and Breach Notification Rule, as well as applicable state laws. We will revise our policies and procedures promptly as appropriate when there is a change in the law or in our privacy practices.

PROCEDURE:

Staff Duties – Our dental practice has privacy and breach notification policies and procedures. The policies and procedures will be updated from time-to-time. All workforce, volunteer and student members must comply with the policies and procedures when they do their job.

Privacy Officer Duties –The dental hygiene director is responsible for developing, implementing and documenting our privacy and breach notification policies and procedures and for updating them as necessary – for example, if our privacy practices change, if the HIPAA rules change, or if there is a change in state law.
Provide all members of our workforce with a paper or electronic copy of the privacy, security and breach notification policies and procedures, and any revisions, and keep a current copy readily accessible to all workforce members.

When there is a change in the law or in our privacy practices, revise the policies and procedures (and if necessary, the Notice of Privacy Practices) as appropriate prior to the effective date of change.
(See Sample of the Acknowledgment of Receipt of HIPAA Policies and Procedures in Appendix)

III. NOTICE OF PRIVACY PRACTICES OR NPP 45 CFR 164.520, 45 CFR 164.530 (i), & 45 CFR 164.502 (i)

POLICY:
Our practice will provide a notice of our privacy practices to our patients, and to anyone else who requests a copy. Our Notice and the way we provide it will comply with HIPAA and applicable state law. Our practice will revise the Notice as appropriate, and will provide the revised Notice as required by HIPAA. Our practice will not use or disclose patient information in a manner that is inconsistent with our Notice, HIPAA, or state law.

PROCEDURE:
Staff Duties – Our Notice of Privacy practices describes how our dental practice may use and disclose patient information. Ask the Privacy Official if you have any questions about the Notice. Do NOT use or disclose patient information in violation of our Notice.
Provide our Notice to each new patient at his or her first appointment, and ask the patient to sign the Acknowledgement of Receipt form for patients. (See Appendix for sample of Acknowledgment of Receipt form for Patients). If a patient refuses to sign the acknowledgment of receipt, note on the form that you tried to get the acknowledgment, and the reason that you could not do so. If the patient has a personal representative, such as the parent or guardian of a minor, provide the Notice to the personal representative and ask the personal representative to sign the acknowledgment form.
Retain each completed acknowledgment form for six (6) years from the date it was created or the date that it was last in effect, whichever is later. If we don't have an acknowledgment form for a patient, then at that patient's next appointment give the patient a copy of the Notice and ask the patient to sign the acknowledgment.
We have a supply of Notices at the reception desk for people who ask for a copy to take with them. Give a copy to anyone who asks for one. However, inmates do not have a right to a Notice of Privacy Practices. An inmate is defined as a person who is incarcerated in or otherwise confined to a correctional institution.

Privacy Officer Duties – This person is responsible for developing our Notice of Privacy (and/or working with appropriate IT staff, administrators, lawyers, consultants on campus) and for revising our Notice when appropriate – for example, if our privacy practices change, if the HIPAA rules change, or a change in the state law.

Providing the Notice – the Privacy Officer is responsible for training students, volunteers and workforce members to provide the Notice, for posting a copy of the Notice in a clear and prominent place in the dental practice, for making sure there is a supply of Notices at the reception desk for people who ask for a copy to take with them, and for posting the Notice prominently and making it available electronically on our practice's website.

Revising the Notice – The Privacy Officer is responsible for the following:
1. Whenever our privacy practices change, or there is a change in the law or the HIPAA Rules that requires a change to the Notice, determine whether our dental practice must revise the Notice. If so, revise the Notice as appropriate.

2. If our Notice is revised, then on or after the effective date of the revision, our practice will:
- Provide the new Notice to new patients on their first appointment and ask them to sign the acknowledgment.
- Have a supply of copies of the new Notice available in the dental office and give a copy to anyone who asks for a copy to take with them.
- Post the new Notice in a clear and prominent location in the dental office.
- Post the new Notice on our website, and make the new Notice available electronically through the website
- Retain at least one copy of both the old and the new Notices for at least six (6) years from the date when the document was created, or the date when the document last was in effect, whichever is later.

Complying with our Notice. Train workforce members to comply with our Notice.
(See Notices of Privacy Practices in Appendix)

IV. DESIGNATED RECORD SETS 45 CFR 164.501, 45 CFR 164.524, & 45 CFR 164.526

POLICY:
Our Privacy Officer will create and retain a written list of our dental practice's "designated record sets", and will update the list whenever it is appropriate.
(See Designated Record Set for LCCC Dental Hygiene Clinic in Appendix).

PROCEDURE:
Privacy Officer Duties – The Privacy Officer will create a list of every set of records in our dental practice that meets the HIPAA definition of a "designated record set". The list must include

1. All dental records and billing records about patients maintained by or for our dental practice.

2. Every group of records maintained by or for our dental practice that is used, in whole or in part, by or for our dental practice to make decisions about patients.

Note: a "record" means any item, collection, or grouping of information that includes patient information and is maintained, collected, used, or disseminated by or for our dental practice. Our designated record sets that are maintained off-site and/or by a business associate must be included on the list.

Whenever our dental practice changes its recordkeeping system in a way that changes our list of designated record sets create a revised list of designated record sets. Retain each list for at least six (6) years from the date when it was created, or from the date when it was last in effect, whichever is later.

V. MINIMUM NECESSARY 45 CFR 164.502 (b) & 45 CFR 164.514 (d)

POLICY:
Our dental practice will use, disclose and request the minimum amount of patient information that is necessary for the intended purpose of the use, disclosure or request.

PROCEDURE:
Staff Duties – Do not access patient information that you are not authorized to access and is not necessary to do your job. Accessing the patient information out of curiosity or for other impermissible purposes is prohibited, and will result in disciplinary action. When making a routine disclosure or request, follow our dental practice's written minimum necessary limits. Before our dental practice makes a non-routine disclosure or requests, we must assess the minimum necessary patient information for the purpose. Always limit uses, disclosures and requests for patient information to the minimum amount necessary for the purpose.

Privacy Officer Duties – Develop the following documents and keep them up to date:
The minimum necessary patient information that our workforce members are authorized to access to do their jobs
(See Workforce Access to Patient Information List in Appendix)

Action Items Needing to Be Done to Accomplish Minimum Necessary:

- Workforce members within the dental practice have been identified by category, patient information needed to do their jobs, and any conditions that apply to their access.
- Routine Disclosures and Requests will be managed by the form called Routine Disclosures and Requests and can be found in the Appendix. This form is to be used whenever our practice makes a routine disclosure of patient information to a third party, or for use when our dental practice makes a routine request for patient information from a third party. The form is self-explanatory regarding the required information.
- Occasionally, the dental practice may want to disclose or request patient information in a non-routine situation. Our dental practice will assess non-routine disclosures and requests to determine the minimum amount of information that is necessary for the purpose. This determination will most likely involve the Clinic Coordinator, Clinic Manager and the Privacy Officer.

(See Routine Disclosures and Requests Form in Appendix)

Minimum Necessary when Responding to Requests for Patient Information
In most cases the dental practice will determine the minimum necessary information to disclose when responding to an appropriate request for patient information, and may not rely on the person requesting the information to determine the minimum necessary amount. However, in the following situations, the dental practice **may** rely on the person making the request to determine the minimum necessary amount, when it is reasonable to do so under the circumstances:

- The dental practice is making a permitted disclosure to a public official and the public official tells the dental practice that the information requested is the minimum necessary for the stated purpose.
- A health care provider, health plan, or health care clearinghouse that is a HIPAA covered entity is asking for the patient information.
- A professional who is a member of the dental practice's workforce, or who is a business associate of the dental practice, requests patient information in order to provide professional services to the dental practice, and the professional tells the dental practice that the information requested is the minimum necessary for the state purpose.

VI. VERIFICATION OF IDENTITY 45 CFR 164.514 (h)

POLICY:
Our dental practice will not disclose patient information to persons who do not have the authority to access the information.

PROCEDURE:
Staff Duties – If a person asks you for information about a patient, and you know the person and know that the person has the authority to get the information such as date of birth, address, or approximate date of last appointment. If you are unsure, direct the request to the Privacy Official.
In all other cases, if a person asks for patient information and you do not know the person, or you are not sure that the person has the authority to access the information requested, direct the request to the Privacy Official who will verify the person's identity and authority to get the patient information requested.

Privacy Officer Duties – If a person asks for information about a patient, and we do not know the person and/or we are not sure that the person has the authority to access the information they asked for, the Privacy Official is responsible for verifying the person's identity and authority to get the patient information they request. Determination will be made as follows:

- Is the disclosure required or permitted?
- Did the patient sign an authorization form before our dental practice makes the disclosure?
- The minimum necessary information is provided, where applicable?
- Ask for the person's photo ID and any other appropriate documentation and do the following:
    - If a person we don't know comes to the dental office and asks for information about a patient, check the If the person claims to be a patient asking for his or her own information, ask for the date of birth, address, approximate date of last appointment, or some other information to verify identity. If the person wants to see or get copies of his or her own information, or a personal representative wants to see or get copies of the patient's information, refer to the section in this manual about **Patient Rights and Requests.** If the person says that he or she is a family member or friend of the patient, ask to see a photo ID and refer to the section in this manual about friends or family members. If the person says that he or she is a patient's personal representative, ask to see a photo ID and exercise professional judgment to verify that the person is acting on behalf of the patient. Where appropriate, require the person to provide documentation, such as proof of legal guardianship or a Power of Attorney (they will usually have these documents with them).
    - LCCC wishes to disclose patient information for research purposes and the documentations and representations required in section 45 CFR 164.512 (i) of the Privacy Rule are in place.
    - If the person is a public official, ask to see his or her identification badge or other credentials. If the request is in writing, review the government letterhead, insignia, address, and credentials.
    - If confronted with any of the following situations, check the special rules for verifying identity in 45 164.515 (h) and consult legal counsel as appropriate:
    - If a public official asks for patient information
    - If the dental office receives an administrative request, subpoena, or summons, civil or authorized investigative demand, or similar process
    - If the dental office receives a request for patient information for research purposes.

NOTE: If all procedures have been followed for verification and you do not believe that our dental practice should provide patient information to the person asking for it, politely tell the person that we are unable to release the information. The person may submit a request in writing and provide more information about his or her identity and authority to get the information. Require all persons, other than patients we know, personally and their family members and friends, as is needed to complete the Verification of Identity Form.
This form is to be scanned into the patient record and maintained for six (6) years from the date the document was created, or six (6) years from the date the document was last in effect, whichever is later.
(See Verification of Identity Form in Appendix)

VII. REQUIRED DISCLOSURES 45 CFR 164.502 (a) (2)

POLICY:
Our dental practice will disclose patient information when required by HIPAA. The Standard is detailed below:
The Standard: Disclosures by **whistleblowers** and workforce member **crime victims**.

1. Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers or the public; and
The disclosure is to:

A. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

B. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.

2. Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

The protected health information disclosed is about the suspected perpetrator of the criminal act; and
The protected health information disclosed is limited to the information listed in 164.412 (f)(2)(i).

PROCEDURE:
Staff Duties – Refer all of the following requests to the Privacy Officer:

- If a patient, or a patient's personal representative, asks to see or get copies of the patient's information
- If a patient, or a patient's personal representative, asks for an accounting of disclosures
- If HHS asks for patient information

Privacy Officer Duties – HIPAA requires a dental practice to disclose patient information in response to an appropriate request from a patient or personal representative to see or get copies or for an accounting of disclosures. Disclosure is also required when patient information is requested by HHS in connection with a HIPAA investigation, compliance review, or audit. In these situations, patient authorization is not required, and the minimum necessary requirement does not apply. However, certain steps in Request for Access and Accounting of Disclosures must be followed.
See the ADA Practical Guide to HIPAA Compliance Privacy and Security in Appendix

VIII. PERMITTED USES AND DISCLOSURES, Reference Listed Below

POLICY:
Our dental practice will not use or disclose patient information without written authorization unless the use or disclosure is required or permitted under HIPAA.

PROCEDURE:
Staff Duties – Do not use or disclose patient information, except for routine purposes that you are authorized and trained to make, unless you have the prior approval of the Privacy Officer.

Privacy Officer Duties – Will be responsible for determining whether a proposed use or disclosure of patient information requires the patient to sign an authorization form, or whether the use or disclosure is permitted by HIPAA.
Policies and procedures will continue to be developed for handling these situations that are likely to arise in our dental practice. Officer will train staff and put the policies and procedures into action.
References to these rules can be found in:
45 CFR 164.502(a) (i)
45 CFR 164.502 (g)
45 CFR 164 510 (b)(5)
45 CFR 164.502 (f)
45 CFR 501 (definition of “treatment”)
45 CFR 164.502 (a)(1)(ii)
45 FR 164.501 (definition of “payment”)
45 FR 164.506
45 FR 164.501 (definition of “health care operations”)
45 FR 164.506
45 CFR 164.502 (a)(1)(iii)
45 CFR 164.510
45 CFR 164.502 (e)
45 CFR 164.502 (j)
45 CFR 164.512 (f)(2)
45 CFR 164.502 (d) (de-identification)
45 CFR 164.514 (e)(limited data sets)
45 CFR 164.514(f)
45 CFR 164.14 (e)(f)
45 CFR 164.502 (d)
See Decision Tree: Decedent PHI in Appendix

IX. PATIENT AUTHORIZATION FORMS 45 CFR 164.508

POLICY:
Our dental practice will not use or disclose patient information without having the patient sign an appropriate authorization form unless the Privacy Rule permits or requires the use or disclosure.

PROCEDURE:
Staff Duties – Consult the Privacy Officer before using or disclosing patient information unless the use or disclosure is routine and you are authorized to make the use or disclosure.

Privacy Officer Duties – The privacy officer will train workforce members to recognize routine uses and disclosures that they are authorized to make and that are required or permitted by HIPAA, including uses and disclosures for purposes of treatment, payment and healthcare operations

If the dental practice wishes to make a use or disclosure of patient information that is not permitted or required by HIPAA, the patient must first sign an authorization form. Do the following 4 things when a signed authorization form is required:
1. Determine whether the dental practice's standard authorization form is sufficient, or whether additional information should be included on the form (for example, authorizations for subsidized marketing communication or for the sale of patient information require additional information on the form). Properly fill in all of the appropriate blanks on the form.

2. Verify identification if you do not personally know the person who will sign the authorization form, or if you are not sure the person is authorized to sign it (for example, if you are not sure that the person is a personal representative of a patient). Do not permit an unauthorized person to sign an authorization form.

3. Give the authorization form to the patient and let the patient read it and ask questions. Answer any questions the patient may have about the form. If the patient understands and agrees with the form, have the patient sign the form and return to you.

4. Confirm that the authorization is properly completed and signed, and make sure that the following information is in the form:

- A description of the patient information to be used or disclosed
- The name of the person(s) authorized to make the disclosure
- The name of person(s) to whom the dental practice may disclose the information
- The purpose for the use or disclosure (if the patient initiated the authorization you may write "at the request of the individual" in this space)
- An expiration date or an expiration event that relates to the patient or to the purpose of the disclosure
- Signature and date of signature of the patient or the patient's personal representative. If the authorization is signed by a patient's personal representative, the form must have a description of the representative's authority to act for the patient

Defective authorization. An authorization is defective and is not valid if:

- It has expired
- The required information has not been filled out completely
- Our practice knows that the authorization has been revoked
- Our practice knows that material information in the authorization is false

5. Give the patient a copy of the completed, signed authorization form. Scan and retain the authorization form for at least six (6) years from the date of its creation, or from the date when it was last in effect, whichever is later.
(See AUTHORIZATION FORM FOR USE OR DISCLOSURE OF PATIENT INFORMATION - CORE ELEMENTS in Appendix)

X. SUBSIDIZED MARKETING COMMUNICATIONS 45 CFR 164.501 (definition of "marketing") & 45 CFR 164.508 (a) (3)

POLICY:
Prior to making a marketing communication, our dental practice will obtain any required written authorization, as needed. **Laramie County Community College Dental Hygiene Clinic does not market**.
PROCEDURE:
Staff Duties – Unless approved, do not:

- Use or disclose patient information for making a communication that encourages someone to buy or use a product or service
- Encourage patients to buy or use a product or service, or
- Accept payment from anyone for making a communication that encourages someone to buy or use a product or service.

XI. SALE OF PATIENT INFORMATION 45 CFR 164.502 (a) (5) (ii) & 45 CFR 164.508 (a) (4)

POLICY:
Our dental practice will NOT "sell" patient information (as defined by HIPAA). It is not our practice to "sell" patient information to any vendor, clearinghouse, etc.
PROCEDURE:

Staff Duties – The DH staff and are prohibited from exchanging any information about our patients for money or anything else of value. "Information about our patients" includes patient lists, schedules, names and addresses, and any other information about our patients. "Anything of value" includes money, things, opportunities, information, or anything else that has even a small amount of value.

Privacy Officer Duties – Will train staff to NOT "sell" or disclose any patient information in exchange for anything of value, or permits a business associate to do so. The Privacy Officer will follow the HIPAA rule and train staff according to 45CFR 164.502(a)(5)(ii).

Authorization forms (Use or Disclosure of Patient Information) will NOT be needed for this policy because Laramie County Community College Dental Hygiene Clinic does NOT permit the sale of any patient information.

XII. MITIGATES HARM (45 CFR 164.530 (f)

POLICY:
If our dental practice or one of our business associates uses or discloses patient information in violation of its privacy policies and procedures or in violation of the Privacy Rule, our Laramie County Community College General Counsel may decide to litigate, to the extent practicable, any harmful effect known to us.

PROCEDURE:
Staff Duties – Immediately tell the Privacy Officer about any improper use or disclosure of patient information by our dental practice or by one of our business associates. If you are aware of any harmful effects of the improper use or disclosure, or any ways to lessen those harmful effects, tell the Privacy Official immediately.

Privacy Officer Duties – When it has been discovered that our dental practice or one of our business associates has used or disclosed patient information in violation of its policies and procedures, or in violation of the Privacy Rule:

- Determine whether our dental practice is aware of any harmful effects of the use or disclosure
- If so, determine whether our dental practice is reasonably capable of doing anything capable to lessen the harmful effects
- Consults with LCCC Administration and General Counsel for guidance when handling harmful effects
- Comply with the Breach Notification Rule and, if appropriate, log the use or disclosure in case the patient asks for an accounting of disclosures.
- Remember that if our dental practice knows that a business associate is doing something that violates the business associate agreement, you must:
- Determine whether it is a "material" breach of the agreement (for example, it is likely a material breach if a business associate that does not provide the dental practice timely notice of a breach of unsecured patient information).
- If the breach is material, our dental practice must plan and take reasonable steps to end the violation
- And, if those steps are not successful, terminate the agreement with the business associate, if it is "feasible" to do so (for example, it may not be "feasible" to end an agreement with a business associate at that time if there is not another person or company that could take over the business associate's responsibilities).

XIII. BUSINESS ASSOCIATES 45 CFR 160.103, 45 CFR 164.502 (e), 45 CFR 164.504 (e), 45 CFR 164.308 (b) & 45 CFR 164.314 (a)

POLICY:
Our dental practice will manage our relationships with business associates in compliance with HIPAA, and will not permit a business associate to access patient information unless a compliant business associate agreement is in place.

PROCEDURE:
Staff Duties – Do not permit outside persons or entities, such as contractors, vendors and consultants, to access patient information unless the person or entity is not a HIPAA "business associate", or an appropriate business associate agreement is in place. In general, you may provide patient information to another health care provider for treatment purposes (for example, a specialist, dental lab, or pharmacy).

Notify the Privacy Officer **IMMEDIATELY** if you have reason to suspect that a business associate agreement is required but not in place, or that a business associate may be in violation of HIPAA.

Privacy Officer Duties – Will consult with LCCC Contract Department and develop a Business Associate Agreement form from the current template and update the form as appropriate. In addition, the Privacy Officer will ensure that a compliant business associate agreement is in place for every business associate.
If our dental practice becomes aware that a business associate is in violation of HIPAA, then our practice must:

- Take reasonable steps to end the violation, and if that is not successful,
- Determine whether it is feasible to terminate the business associate agreement
- If feasible, terminate the agreement

b. If not feasible, develop a project plan for bringing noncompliant business associate into compliance, or replacing the business associate as soon as is reasonably feasible

- Take reasonable steps to mitigate (lessen) any harm caused by the violation as recommended by LCCC General Counsel

(See template of Business Associate Agreement provided by LCCC Contract Department in Appendix,)

XIV. PATIENT RIGHTS AND REQUESTS 45 CFR 164.524

POLICY:
Our dental practice will provide patients, and their personal representatives as appropriate, access to patient information in a designated record set as required by HIPAA.

PROCEDURE:
Staff Duties – If anyone asks to see or get a copy of patient information, politely tell the person that all requests must be in writing and must be viewed by the Privacy Official. Give the person a copy of our Request for Access form, ask them to fill it out and give it to the Privacy Official.

Privacy Officer Duties – **Review** requests for access. Promptly review all completed Request for Access forms to determine whether the request should be granted or denied in compliance with HIPAA. Access (or written denial of access) must be provided within 30 days of the date that our dental practice received the written request for access, unless our dental practice has properly extended the period for up to 30 additional days.
Verify the identity of the person making the request where appropriate.

If our dental practice believes there are permissible grounds to deny access, determine whether the grounds are appropriate and, if so, prepare and send the Denial of Request for Access form. It is prudent to consider a legal opinion when denying a request for access. If the grounds for denial are reviewable and the patient or personal representative requests a review, provide an appropriate review of the denial in compliance with HIPAA.

If our dental practice will **grant a request to see records**, arrange for a time and place in the dental office for the person to see the records within the appropriate time frame (within 30 days of the date that the dental practice received the request, or within the extension time period if properly extended).

If our dental practice will grant a **request for copies of records**, provide the copies within the appropriate time frame (within 30 days of the date that the dental practice received the request, or within the extension time period if properly extended).

Fee Schedule. If our dental practice decides to charge for copies (depending on the size of the document), .05 per copy may be charged for copying. The patient may have to assume the cost of mailing the copies. This may also include the cost of preparing summaries and explanation of patient information. The fee schedule must comply with both HIPAA and applicable state laws. For electronic copies, the patient may have to assume the cost of CD-ROMs and/or USB drives.

Electronic Copies. **If a patient requests an electronic copy of a record that our dental practice maintains in an electronic designated record set, our dental practice must provide an electronic copy.** Our dental practice is not required to provide the exact kind of electronic copy that the patient asks for if we cannot readily do so. If the patient does not agree to the kind of electronic copy that our dental practice can readily produce, offer the patient the information in hard copy.

Do NOT use outside electronic media in our system. Instead, we will have a supply of blank USB drives on hand to use to provide copies of patient information.
A patient has the right to ask for the electronic copy through email. If the patient prefers an **unencrypted email**, our dental practice must send the information in an unencrypted email. Our Request for Access form includes a notice that there is risk that the information in an unencrypted email could be read by a third party. Use reasonable safeguards to make sure that our dental practice correctly enters the email.
(See Request for Access form in Appendix)

AMENDMENT 45 CFR 164.526 (XIV CONTINUED)
POLICY:
A patient, and a personal representative, as appropriate, has the right to ask our dental practice to amend information about the patient in a designated record set if they believe that the information is not correct. As stated in our Notice of Privacy Practices (NPP), the request must be in writing and must give the reason for the amendment. If we deny the request, we will put our reason for denying the request in writing. If we agree to make the amendment, we will amend the record and tell the patient. If another HIPAA covered entity (such as a dental plan or a specialist) tells our practice that they made amendments to information about a patient, we will make the amendment to information in our designated record set, as appropriate.

PROCEDURE:
Staff Duties – If a patient (or patient's personal representative) asks to amend any information in our dental practice's records, politely tell them that the request must be in writing and give them a copy of the Request for Amendment form. Ask the patient to complete the form and give it to the Privacy Official. Only the privacy Official may receive and process requests for amendments. Immediately report a request to the Privacy Official.

Privacy Officer Duties - The Privacy Officer is responsible for receiving and processing all requests to amend the patient records.
Requests to amend patient records must be made in writing using our Request for Amendment form. The request must include a reason for the amendment. Make sure our Notice of Privacy Practices states that requests to amend records must be in writing and must state the reason for the request.
Review each requested amendment and determine whether the request should be approved or denied.
If our dental practice approves the amendment, append the amendment to the record, tell the patient that the amendment is approved, ask the patient who needs to be told about the amendment, ask the patient to agree that the dental practice may tell these persons about the amendment, and make a reasonable effort to send notice of the amendment within a reasonable time to the persons identified by the patient and to any other persons that we know have the information that we amended and may have relied on it (or may rely on it in the future) in a way that could harm the patient or put the patient at a disadvantage.
If our dental practice denies the amendment, send a written denial to the patient that contains the information required by HIPAA. If the patient gives us a statement of denial, determine whether our dental practice should write a rebuttal (and if so, consult with LCCC General Counsel to assist with the rebuttal).

Future disclosures of the information. If the patient gives us a statement of denial, ensure that every time our dental practice discloses the information in question, we include the request for amendment, our denial, the statement of disagreement, and our rebuttal (if any) or an accurate summary of these documents.

If the patient does not give us a statement of denial, but the patient asks for our dental practice to include the request for amendment and our denial whenever our dental practices discloses the information in question, ensure that copies of these documents (or an accurate summary) is included in all such disclosures.
If the dental practice is making an electronic standard transaction that does not permit the additional material to be included, transmit the material separately.
Documentation. Document all requests for amendment and log all requests for amendment and their disposition. Retain the documentation for at least six (6) years from the date of its creation, or from the date last in effect, whichever is later.
(See Request for Amendment form, Denial of Request to Amend form, Amendment Request Log in Appendix,)

ACCOUNTING OF DISCLOSURES 45 CFR 164.528 (XIV CONTINUED)
POLICY:
Upon request, our dental practice will provide a patient with an appropriate accounting of disclosures.

PROCEDURE:
Staff Duties – Every patient has the right to ask our dental practice for an "accounting of disclosures" of the patient's information.
Immediately report to the Privacy Officer any disclosures of patient information that are not for purposes of treatment, payment or healthcare operations. Tell the Privacy Officer the date of the disclosure, who received the patient information, the information that was disclosed, and the purpose of the disclosure.
The Privacy Officer is responsible for receiving and processing all requests for an accounting of disclosures. If a patient asks you for an accounting of disclosures, politely tell them that our Privacy Official handles these requests, give them a copy of your request form, and ask them to complete the form. Give it to the Privacy Official.

Privacy Officer – Use the Log of Disclosures of Patient Information form to record all disclosures of patient information that would need to be included if a patient asks for an accounting of disclosures. Since an accounting of disclosures must include disclosures made up to six (6) years before the request, make sure the information about each of disclosures in the log is retained for at least six (6) years from the date of the disclosure.
If a patient asks for an accounting of disclosures, have the patient complete the Patient Request for Accounting of Disclosures form.

Within 60 **days** of the date that our dental practice receives the request:

- Provide the accounting of disclosures, or

- If our dental practice cannot provide the accounting within 60 day period, send the patient a letter extending the period for up to 30 days. The letter must state the reasons for the delay and the date on which we will provide the accounting. We are only entitled to one 30 day extension. Provide the accounting to the patient at the end of the extension period.

- Maintain documentation of every request for an accounting of disclosures, every accounting of disclosures that our dental practice provides, and your designation as the person responsible for receiving and processing requests for accountings of disclosures for at least six (6) years from the date of the document's creation or the date when the document was last in effect, whichever is later.

Every patient is entitled to one free accounting of disclosures in any 12 month period. Determine whether our dental practice will charge a fee for requesting additional accountings of disclosures in a 12 month period, or whether all accountings of disclosure will be provided for free. If a fee will be charged, determine the permissible, reasonable cost-based fee for providing an accounting of disclosures. If a patient or personal representative requests an additional accounting of disclosures within a 12 month period, inform them of the fee and permit them to cancel or change the request in order to avoid or reduce the fee.
(See Log of Disclosures of Patient Information form and Request for Accounting of Disclosures in Appendix, pages 122 & 123)

CONFIDENTIAL COMMUNICATIONS 45 CFR 164.522 (b) (XIV CONTINUED)
POLICY:
Our practice will accommodate reasonable requests by patients to receive communications from our practice by an alternative means or at an alternative location.

PROCEDURE:

Staff Duties – If a patient asks our dental practice to contact him or her in a different way or at a different location, ask the patient to fill out our Confidential Communications form. Do not ask the patient to explain why he or she is making the request.

When our practice has agreed to a request for confidential communications, **FLAG** the patient's record. Within Eagle Soft it will be done in the ALERT as "Confidential Communication".

If you are communicating with a patient whose record is flagged, make sure to abide by the Confidential Communications request. The signed Confidential Communication form is to be scanned into the Smart Docs in the patient's chart.

Privacy Officer – Train staff to use the Confidential Communications form when appropriate. Develop the system to flag a patient's chart with this request and to continue to update the flagging protocol as changes are made to the dental chart.

The flag should not indicate to anyone other than our workforce that the patient has requested confidential communications.

Retain the completed forms for at least six (6) years from the date they were completed or the date when they were last in effect, whichever is later.
(See Confidential Communications form in Appendix,)

RESTRICTED DISCLOSURE 45 CFR 164.522 (a) (XIV CONTINUED)
POLICY:
Our practice allows patients to request restricted use or disclosure of their patient information. As of September 23, 2013, HIPAA requires our dental practice to agree to a request not to disclose information to a health plan about a health care item or service for payment and health care operations purposes when our dental practice has been paid for in full for the item or service by the patient or by a third party, unless the disclosure is required by law. Our dental practice is not required to agree to any other kind of request for restriction, but if we do we must abide by the restriction until it is terminated.

PROCEDURE:
Staff Duties – If a patient asks you not to use or disclose his or her information in a certain way, politely tell them that only our Privacy Officer can respond to requests for restrictions and ask them to contact our Privacy Officer.

Privacy Officer – You are responsible for responding to all requests to restrict the use or disclosure of patient information. Requests for restrictions will need to be in writing using the REQUEST FOR RESTRICTED USE OR DISCLOSURE form. All requests for restrictions need to be documented. Retain all completed documentation for at least six (6) years from the date the document was completed, or at least six (6) years from the date that the document was last in effect, whichever is later.

Health Plan Restriction: As of September 23, 2013, our practice will agree to any request not to disclose patient information about a health care item or service to a health plan (medical or dental) for purposes of carrying out payment or health care operations if the information pertains solely to a health care item or service for which our dental practice has been paid in full, unless otherwise required by law. This applies whether patient pays in full or if payment comes from another source (including another health plan).
Our dental practice will flag restricted information so a claim is not submitted to the health plan, and the health plan does not review the information during an audit.

Other restrictions: Except for the health plan restriction discussed above, our dental practice is not required to agree to a requested restriction. Generally, our dental practice will agree to restrictions only in exceptional circumstances, and when our dental practice can reasonably accommodate them. Determine whether or not we should agree to each request.

If we agree to a restriction, we must not violate the restriction; however, we may use and disclose restricted information in certain situations, such as an emergency treatment, HHS investigation, and public health reporting as permitted by HIPAA.

If we agree to a restriction, the agreement can only be terminated in three ways:

1. The patient requests the termination in writing.
2. The patient orally agrees to the termination and our dental practice documents the oral agreement.
3. Our dental practice informs the patient that we are terminating our agreement to a restriction (however, our dental practice cannot terminate health plan restrictions where our dental practice has been paid in full – see above). The termination only applies to patient information that our dental practice created or received after we informed the patient that the restriction has terminated.

(See Restricted Use or Disclosure form in Appendix)

XV. TRAINING 45 CFR 164.530 (B)

POLICY:
Our dental practice will train all workforce members within a reasonable period of time after they join the practice to comply with the HIPAA policies and procedures that affect their jobs. When there is a material change to our policies and procedures, our dental practice will train the workforce members whose jobs are affected by the change within a reasonable time after the change becomes effective.

PROCEDURES:
Staff Duties – You must be trained to comply with HIPAA when you do your job. All training must be documented. When there is a significant change to our HIPAA policies and procedures that affect your job, you will receive a training update.

Privacy Officer Duties – You are responsible for making sure that each of our workforce members get the HIPAA training they need to do their jobs, including training updates when there is a change in our HIPAA policies and procedures and an annual review of LCCC policies. You must make sure that new workforce members get HIPAA training within a reasonable amount of time after joining the dental practice. When we change our policies and procedures, make sure that the workforce members affected by the change get training within a reasonable time after we put the change into effect.
You must document all HIPAA training, even on the spot refreshers. Keep the training documentation for at least six (6) years from the date the document was created or from the date when the document was last in effect. Whichever is later.

In some cases, retraining may be an appropriate sanction for workforce members who violate any one of our HIPAA policies and procedures. When retraining is used as a sanction, make sure a copy of the training documentation is placed in the person's personnel file.
(See HIPAA Training Sign In Sheet in Appendix,)

XVI. DISCIPLINARY ACTION ("Sanctions") 45 CFR 164.530 (e)

POLICY:
Our dental practice will have and apply appropriate sanctions against workforce, student, volunteer members who violate our HIPAA privacy, security and breach notification privacy policies and procedures. Our dental practice will document all sanctions that are applied.

PROCEDURE:
Staff Duties – Our dental practice applies appropriate sanctions against workforce members who violate our HIPAA privacy, security and breach notification policies and procedures.

Privacy Officer Duties – Once a violation has been discovered, appropriate sanctions must apply. Each time a sanction is applied, you will document the sanction and retain the documentation for six (6) years from the date the document was created or from the date when the document was last in effect, whichever is later.
The individuals involved in determining the appropriate sanctions may be course instructors, administrators, DH Clinic Coordinator, DH Clinic Manager, DH Radiology Coordinator, General Counsel and/or other consultants.

Whistleblowers. Sanctions must not be imposed against whistleblowers whose actions are appropriate under the HIPAA Privacy Rule. Sanctions must not be used as a means of retaliation or intimidation in violation of HIPAA.
Intimidation and retaliation. The dental practice may not use sanctions as a means of intimidation or retaliation against a workforce member who:

- Files a HIPAA complaint with the government
- Cooperates with a government HIPAA investigation or proceeding, or
- Opposes any activity at the dental office that the workforce member believes is unlawful under HIPAA, as long as
- The workforce member's belief is reasonable and in good faith
- The workforce member opposes the activity in a reasonable way and does not impermissibly use or disclose patient information

Sanctions from LCCC Human Resources are as follows:
The Privacy Rules require LCCC to have and apply appropriate discipline to employees who fail to comply with the Policies and Procedures or the Privacy Rules. LCCC's policy is to appropriately discipline any employee who violates the Policies and Procedures or the Privacy Rules.

Type of Discipline*.* LCCC will appropriately discipline employees who fail to comply with the Policies and Procedures or the Privacy Rules, in accordance with the disciplinary policies set forth in LCCC's employee Handbook, training and LCCC's policies and procedures. Discipline will vary depending on the nature of the employee's misconduct, but discipline includes sanctions up to and including termination of employment.

Whistleblowers. LCCC will not discipline employees who disclose PHI, so long as:
• the employee believes in good faith that the Health Plan or LCCC has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Health Plan or LCCC potentially endangers one or more patients, workers, or the public;
and
• the disclosure was made to the individuals or agencies and for the purposes set forth in the whistleblower provisions of the Privacy Rules (see section 164.502 of the Privacy Rules)

Crime Victims*.* LCCC will not discipline an employee who is a crime victim and discloses PHI to a law enforcement official, so long as the PHI concerns the suspected perpetrator of the criminal act and the PHI is limited as required by the Privacy Rules (see 45 CFR 164.502(j).

No Intimidating or Retaliatory Acts

The Privacy Rules prohibit LCCC from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against individuals for exercising their rights under the Privacy Rules. LCCC's policy is that LCCC will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their privacy rights, filing a complaint, participating in an investigation, or opposing any improper practice under the Privacy Rules.

XVII. RETALIATION AND INTIMIDATION 45 CFR 164.530 (g) & 45 CFR 160.316

POLICY:
Our dental practice (also applies to our business associates) will not intimidate, threaten, coerce, or discriminate against any person, nor take any retaliatory action against anyone, because he or she:

- Exercises a HIPAA right
- Participates in a process provided for by the Privacy Rule or Breach Notification Rule
- Files a complaint with the dental practice or with the Secretary of HHS concerning the HIPAA compliance of the dental practice or a business associate
- Testifies, assists, or participates in a HIPAA investigation, compliance review, proceeding, or hearing
- Opposes an act that HIPAA makes unlawful, as long as the person has a good faith belief that the act is unlawful, and the way the person opposes the act is reasonable and does not involve disclosing patient information in violation of HIPAA.

PROCEDURE:
Staff Duties – Our dental practice (also applies to our business associates) will not intimidate, threaten, coerce, or discriminate against any person, nor take any retaliatory action against anyone, because he or she:

- Exercises a HIPAA right
- Participates in a process provided for by the Privacy Rule or Breach Notification Rule
- Files a complaint with the dental practice or with the Secretary of HHS concerning the HIPAA compliance of the dental practice or a business associate
- Testifies, assists, or participates in a HIPAA investigation, compliance review, proceeding, or hearing
- Opposes an act that HIPAA makes unlawful, as long as the person has a good faith belief that the act is unlawful, and the way the person opposes the act is reasonable and does not involve disclosing patient information in violation of HIPAA.

Immediately report to the Privacy Officer if you believe or suspect that anyone at our dental practice or at one of our business associates has intimidated or retaliated against you or anyone else.

Privacy Officer Duties – If it is discovered that anyone at our dental practice or at one of our business associates has intimidated or retaliated against someone in violation of this policy, ensure that the intimidation or retaliation stops. See that appropriate sanctions are applied against any workforce member responsible for the intimidation or retaliation, and document the sanctions.

If a business associate engages in impermissible intimidation or retaliation in violation of HIPAA, take reasonable steps to end the violation by the business associate. If the attempt to end the violation is not successful, the dental practice must terminate the business associate agreement when possible.

XVIII. **WAIVER OF HIPAA RIGHTS 45 CFR. 530 (h) & 45 CFR 160.306**

POLICY:
Our dental practice will not require anyone to waive their right to complain to HHS if they believe our dental practice or another HIPAA covered entity is not complying with HIPAA, or any other rights that they have under the Privacy or Breach Notification Rule, as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

PROCEDURE:
Staff Duties – Do not ask patients to waive a HIPAA right as a condition of treatment, payment, or health plan enrollment or eligibility for benefits.

Privacy Officer Duties – Train all workforce members to understand that they may not require or request a patient or other person to waive:

- Any right under the Privacy Rule or Breach Notification Rule, or
- Their right to file a complaint with HHS as a condition for the provision of treatment, payment, enrollment, in a health plan, or eligibility for benefits.

XIX. DOCUMENTATION OF HIPAA COMPLIANCE 45 CFR 164.530 (j) & 45 CFR 160.310

POLICY:
Our dental practice will maintain the following documentation as required by HIPAA:

- HIPAA privacy and breach notification policies and procedures
- Communications required to be in writing
- Documentation of actions, activities, and designations required to be documented

Our dental practice will retain this documentation for a period of at least six (6) years after its creation or last effective date, whichever is later

PROCEDURE:
Staff Duties – Do NOT dispose of, delete, or destroy any electronic or paper HIPAA document for six (6) years from the date the document was created, or six (6) years after it was last in effect, whichever is later. Examples of HIPAA documents include policies and procedures, Notices of Privacy Practices, acknowledgement forms, authorization forms, breach notification documents, etc.

Privacy Officer Duties – Maintain an electronic and/or hard copy file of our HIPAA compliance documentation. Our HIPAA compliance documentation includes a variety of documents. Here are some examples of HIPAA compliance documentation:

- Current and past designation of the Privacy Officer
- Policies and Procedures
- Notices of Privacy Practices
- Business Associate Agreements
- Signed Acknowledgments of Receipt of Notice of Privacy Practices
- Training Sign in Sheets
- Signed Authorization forms
- Complaints about our privacy practices
- Documentation of disciplinary actions (“sanctions”)
- Restricted Disclosures
- Disclosure logs
- Lists of Designated Record Sets
- Minimum Necessary Restrictions
- Breach Notification letters
- Logs of breaches involving fewer than 500 patients

Our HIPAA documentation must contain current versions of documents such as policies and procedures, Notices of Privacy Practices, and personnel designations. Our HIPAA documentation must also contain any prior versions of those documents unless at least six (6) years has passed since the document was created or since the document was last in effect, whichever is later. Ensure that all required HIPAA documentation is not disposed of, or deleted, destroyed, or lost for at least six (6) years from the date of its creation or the date when last in effect, whichever is later.

Dispose of HIPAA compliance documentation when it is appropriate to do so. If a document identifies or could be used to identify a patient, dispose of the document in a way that “secures” the document under the Breach Notification Rule. Hard copy documents should be shredded or destroyed such that the patient information cannot be read or otherwise reconstructed. Electronic media containing patient information should be cleared, purged, or destroyed consistent with **NIST Special Publication 800-88, Guidelines for Media Sanitization**, such that the patient information cannot be retrieved.

XX. SAFEGUARD PATIENT INFORMATION 45 164.530 (c)(Administrative, Physical, and Technical)

POLICY:
(There are three categories of safeguards: administrative, physical and technical)
Faculty, Staff and Dental Hygiene or Dental Assistant Student Duties - UNDER ALL CATEGORIES, PERSONAL PAGERS, CELL PHONES, PORTABLE COMPUTING DEVICES, AND/OR THEIR CAMERAS/VIDEOCAMERAS, PERSONAL COMPUTERS, PDA'S, BLACKBERRY'S, OR ANY OTHER PERSONAL ELECTRONIC EQUIPMENT IS NOT PERMITTED ON THE CLINIC FLOOR AND ARE PROHIBITED IN PATIENT TREATMENT LABS, CLINICAL SETTINGS AND THE HEALTH SCIENCE and WELLNESS COMPUTER LAB!
AUTHORIZED USERS: THERE ARE FEW INDIVIDUALS THAT MUST USE A CELL PHONE TO DO THEIR JOBS WHEN TROUBLE SHOOTING CLINICAL PROBLEMS; THOSE AUTHORIZED INDIVIDUALS WOULD BE: I.T. STAFF, PROGRAM ASSISTANT/CLINIC MANAGER, DH CLINIC COORDINATOR, AND DH RADIOLOGY COORDINATOR, etc.

If a Dental hygiene or dental assistant student needs to make a phone call to find a patient, etc., they may use the clinic land line telephone. Students may use their cell phones outside of the clinic area on breaks only. This safeguard will be strictly enforced. Professionalism Points may be deducted from a student's lab or clinical grade if a violation should occur.

Work Study students that are working in the reception office area are NOT authorized cell phone users and may not bring their cell phones or other electronic devices into the dental reception, clinical area. Violation of this safeguard will be strictly enforced and could result in termination.

Sharing any patient information in any form on social media such as Facebook, etc., is strictly prohibited. Other sanctions will be determined by the Privacy Officer depending on the severity of the violation and will involve meeting with the Privacy Officer for further HIPAA training. If the violation is severe, further sanctions may involve the Dean and/or LCCC General Counsel.

ADMINISTRATIVE SAFEGUARD POLICY:
POLICY:
Our dental practice will have in place appropriate administrative, technical and physical safeguards to protect the privacy of patient information. Our dental practice will reasonably safeguard patient information from intentional or unintentional use and disclosure in violation of HIPAA. Our dental practice will reasonably safeguard patient information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure of patient information.

PROCEDURE:
Safeguards we currently have in place are as follows:

HIPAA Training:-All students, faculty and staff will be trained regarding HIPAA Policies and Procedures for this dental clinic at least annually.

Patient Appointments: After a patient has checked-in, call the patient from the waiting room by first name only. After the patient is retrieved, address the patient appropriately and respectfully with Mr., Mrs., etc.

Oral Communications: **speak quietly** when discussing a patient's condition in a waiting room or other area where others may hear the conversation. Avoid using names in hallways, student lounge, bathrooms, any location that is considered "public".
Avoid unnecessary disclosures of patient information by monitoring voice levels and being alert for unauthorized listeners. Conduct telephone conversations away from public areas. Use speaker phones only in private areas.

Telephone Messages: Unless a patient has asked not to be contacted by telephone, telephone messages and appointment reminders may be left on answering machines and voicemail systems, but LIMIT the amount of information disclosed in a telephone message.

Faxes: Fax machines MUST be located in secure areas that cannot be easily accessed by visitors or patients. The XMedia Fax system used at Laramie County Community College is HIPPAA compliant Ensure that fax technology is utilized as minimally as possible, and with proper procedures, to maintain PHI Privacy during fax disclosures. Facsimile transmission (fax) of medical records should be limited, since such transmission is considered "unsecure" by HIPAA Privacy and Security Rules and a misdirected fax is subject to Privacy Breach Notification. Options to fax, such as secure e-mails with encryption according to HIPAA Security rules should be utilized, if available. A fax cover sheet should always be utilized with the following information:

- Date
- Fax telephone number.
- Name of the recipient
- Name of the sender
- Appropriate comments regarding the information.
- A disclaimer statement and contact information in case the fax is received in error, including the immediate destruction of any information received by wrong recipients due to fax errors.

The fax transmission of patient information should be sent or received to a device that is manned by authorized health care personnel or designated by the patient in the written request.

Mail: Send mail to the patient's primary address unless the patient requests an alternative address. Postcards may be used for appointment reminders as long as the patient has not objected and the postcard contains the MINIMUM NECESSARY amount of patient information.

Copies: Copies of records containing patient information will be stamped "copy" in a color other than black so that copies can be distinguished from originals. Traditional x-rays that have been duplicated will be marked "duplicate" patient name and original date of service.

Photocopiers, Scanners and Printers: Some printers, scanners and photocopiers have a built in hard drives. Before our dental practice gets rid of an old or non-working piece of equipment, we will have the hard drive securely wiped by LCCC IT department to prevent unauthorized individuals from accessing any patient information and other sensitive information that may be stored on the hard drive. The hard drives will then be destroyed by a business associate contractor and documentation of destruction will be provided.

If the piece of equipment is leased, we will try to secure leased equipment that has a function to securely wipe the hard drives.

Destruction of Protected Health Information: When it is appropriate to destroy patient information in compliance with applicable federal and state laws and our practice's document retention policies, the information will be destroyed in a way that "secures" it under the breach notification rule.
The Privacy Officer, along with others that deal with security and destruction of documents, will determine when patient information may be disposed of, who may destroy the information, and any safety precautions that apply. This will be in accordance with federal and state laws. A Business Associate Agreement for the entity disposing of the PHI will be on file, before releasing information to that entity.

Academic/clinical records with any identifiable patient information on any portion of a student/patient form that a student is preparing prior to a patient arriving for their appointment MUST be placed in the approved shredder box, if an error is made to the INITIAL paperwork prior to a patient being seen. If a student should make an error to existing paperwork that is actually a part of the patient record, draw one line through the error, initial the error and record the correct information. Errors on electronic records can be corrected by the end of the visit or noted in patient treatment notes. All entries in notes are date and time stamped.

Clinical paperwork of any kind including initial health history DOES NOT GO INTO THE TRASH. Dispose of it in the shredder boxes located in the Program Assistant's office where it will be placed in a secure shred bin and disposed under the appropriate contract and business associate agreement.

The Privacy Officer will ensure that a **business associate agreement** is in place before our dental practice gives any patient information to a recycling or disposal firm. This includes companies that recycle dental x-rays. **Verify** the identity of the vendor's representative before turning over any patient information or devices containing patient information unless you know the representative by sight.

Paper Records: Our dental practice will store paper records and dental charts away from unauthorized persons..

The Program Assistant will pull (or delegate this duty to a trained work study student specifically trained in the dental reception office) patient dental records prior to the patient visit and is responsible for ensuring that the records are safely returned to the dental records files and locked up when not in use.

Patient records or patient recare lists may NOT be removed from the LCCC Dental Hygiene Clinic and are NOT to go beyond the area of the dental clinic offices (SC 122, 125, Instructor Offices) with the exception of those being stored in SC 174.

All (paper) dental records must be securely returned, stored, and locked up when the dental office is closed.
Student Patient tracking records: All student patient tracking records are allowed to leave the clinical site, but be stored in a secure manner. These forms will remain in the student's academic file 1 year from the date the student graduates and will be shredded at that time.

DENTAL HYGIENE or DENTAL ASSISTANT STUDENTS MAY ONLY USE (PAPER) DENTAL RECORDS IN THE DENTAL HYGIENE CLINICAL AREAS.

Special permission may be given to students (by the Privacy Officer) to use the dental charts in a pre-designated room while preparing the dental chart for the student's assignments, or mock board clinical exams. The dental records must be securely returned to the dental records files and locked up.

Patients and Visitors: Visitors and patients will be appropriately monitored during visits to our dental practice. Patients will not be allowed to access other patient's records, patient schedules or other patient information.

APPROPRIATE ACCESS TO PHI BY WORKFORCE MEMBERS: Each user is ultimately responsible for adhering to this policy. Users must only access/view the minimum set of PHI that they have a legitimate "need to know" regardless of the extent of access provided. Appropriate access to clinical information is defined as providing a user timely access to patient specific information, which is necessary to perform his/her professional responsibilities. Access will be granted for an individual to provide and/or support quality patient care processes, as defined by an individual's professional responsibilities to the patient and the facility.
This policy embraces the following principles related to the collection, processing, maintenance, and storage of patient information.

- Faculty, staff, students and volunteers will access, use, collect, dispose, process, view, maintain, and store patients' clinical and financial information in an honest, ethical and confidential manner.
- The access, use, collection, processing, viewing, maintenance, and storage of patient information will be done in a manner that at a minimum, meets all applicable Federal and State Laws, Rules, Regulations and Accreditation Standards.
- Access to patient information will be limited to individuals with a legitimate "need to know in order to effectively perform their specific job duties and responsibilities. User roles and related permissions are defined and managed within al computer systems that contain PHI.
- Faculty, staff, and students will be granted access to PHI after execution of appropriate confidentiality statement by the workforce member.

- Job descriptions will address what PHI is accessible by which job roles.
- All faculty, staff, students and volunteers must conform to security policies, i.e. not sharing access credentials, to help protect PHI.

Security: This section of this guide is intended to give a general overview of the security compliance measures undertaken by the Laramie County Community College Dental Hygiene Program. This summary *is not* intended to be an exhaustive list, rather an overview of the more common safeguards we employ. Please refer to our detailed polices, any written procedures and Risk Assessments for more information.

1. **Risk Assessment** – Privacy and Security Risk Assessments are to be updated routinely as the Organization's safeguards materially change, but not less than yearly. Security and Privacy assessments were conducted most recently on:11/25/2014 and 11/20/2014 respectively

2. **Workforce Clearance –** All students, faculty and staff undergo a background check prior to admission to the program or hiring as an employee of Laramie County Community College.

3. **Workforce Termination –** All students, faculty or staff members who are terminated will have their access to computer systems and networks removed immediately according to policy timeframes and procedures.

4. **Access to PHI** – All appropriate access to PHI is secured through the use of passwords which are changed routinely; of appropriate strength and unique to each user. All access to PHI is through formal logon. Remote access is secured data in transit and no data is stored on mobile devices**.**

5. **Password Management –** Passwords must be changed every 6 months. Use of more secure passwords, i.e. multiple digit letter number combinations is required**.**

6. **Auto Log-off –** Users are logged off of PCs and Servers after periods of inactivity.

7. **Back-up and Restoration –** Multiple levels of routine and remote back-ups are maintained. They are tested for restoration integrity and are encrypted data at rest and in transit**.**

8. **Encryption for Breach Safe Harbor –** all practice PHI in transit and at rest is encrypted. Emails should also be encrypted if used for PHI**.** Currently analyzing encryption for emails. At present a system is not in place**.**

9. **Malware Prevention –** Anti-virus, firewall(s), intrusion monitoring, detection and prevention and similar safeguards are all up to date and continually maintained**.**

10. **Physical Security –** The Organization has locks, alarms and segregated records and computers / monitors for patient areas, as practical. Maintenance records for all physical security items are kept for the 6-year HIPAA documentation retention period**.**

11. **Media and Devices -** Mobile devices are only used on campus, via secure connection and never store PHI**.**

12. **Audit Controls –** Eaglesoft maintains an audit log of all user activities which is monitored at least quarterly for inappropriate access, use or disclosure. We also monitor error and technical logs for inappropriate activity on a routine basis**.**

13. **Security and Privacy Training –** Laramie County Community College Dental Hygiene and Dental Assisting students, faculty and staff members are trained at new hire, at least annually thereafter and whenever there are material changes to the privacy / security rules or job roles which require a different level of training. Security and privacy reminders are discussed at staff meetings and other opportunities. Tests and documentation of the training is kept for the 6-year HIPAA documentation retention period.

CHNICAL SAFEGUARD PROCEDURES: Under our current LCCC computer systems, these safeguards are not fully accomplished. The Privacy Officer and the I.T. Department continue to work on full compliance, however, we are not there as of this writing. Items needing further compliance are noted with an asterisk (*).

LCCC Dental Hygiene has put a statement in the Informed Consent that patients sign. The statement is as follows: *"I agree that Laramie County Community College Dental Hygiene clinic may send my radiographs in an electronic format and at my request will send them to the email address provided by the dentist of my choice. I am aware that there is some level of risk that third parties might be able to read unencrypted emails."*
(See Patient Bill of Rights/informed Consent in Appendix)

The Dental Hygiene Privacy and Security Policies and Procedures is a working document and as updates to our electronic equipment and LCCC email systems update, etc., occurs, it is our intent to update our policies and procedures on an annual basis.

***Encryption:** Electronic patient information should be encrypted whenever the Security Official determines that it is reasonable and appropriate to do so. Our dental practice will consult with our software vendor and internet provider to determine encryption solutions that would render patient information "secure" under the Breach Notification Rule. Emails sent between our dental practice and other health care providers via a common Internet carrier shall not include patient information unless the email is encrypted.

Internet: Unauthorized access to the Internet from a computer workstation that contains patient information is prohibited.

Portable and Mobile Handheld Computing Devices: Dental Hygiene and Dental Assistant Students and workforce members may **NOT** store patient information on portable or mobile computing devices.
Students and workforce members who store any unsecured patient information on portable or mobile handheld computing devices are responsible for the security of the patient information and are subject to sanctions up to and including termination of school or employment if the device is misplaced, lost or stolen. Students and workforce members must IMMEDIATELY notify the Privacy Officer of a breach or suspected breach of protected health information.

Portable Storage Devices: Patient information MAY NOT be downloaded onto portable storage devices, such as USB devices and CD-ROMs UNLESS its purpose is to provide a patient requested information. All patient requested downloads must be in writing. A patient receiving an electronic copy of patient information may request the copy unencrypted on a portable storage device, and our dental practice will provide the copy in that format if requested and if we can readily produce it.

Clinic Computers:-All computers storing patient information must be turned off when clinic is not in session with the exception of the dental office computers. Dental personnel need to use the software system even while patient treatment clinics are not in session for patient scheduling, patient cancellations, various financial reports, etc. All clinic computers are to be used for clinical applications. Radiographic grading, clinical activities and treatment of patients, only.

Access Authorization/Password Security:-All individuals must log in to all clinic computers using the username and password as provided by LCCC I.T. Data Security Administrator.

Access Authorization/Password Security within EagleSoft:-All users are given access to the EagleSoft according to their job description or if they are a dental hygiene or dental assistant student. All students will have minimal access within EagleSoft to minimize any risk of access, record deletion, etc. Most of the student access is view only, with the exception of medical history, dental radiographic images, periodontal and clinical, and hard tissue charting and treatment notes.

XXI. DE-IDENTIFICATION 45 CFR 164.502 (d) (2)

POLICY:
Our dental practice will properly de-identify patient information when appropriate.

PROCEDURES:
Staff and Student Duties – De-identifying patient information involves removing very specific information that can be used to identify a patient. Staff members who have not been trained to de-identify patient information should not attempt to do so or be assigned to do so.

Use the following method to "de-identify" patient information
Remove from the document all of the following "identifiers" for the patient and for the patient's relatives, household member, and employers:

1. Names, including initials

2. Any geographic subdivision smaller than a state (including address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, - the geographic unit formed by combining all zip codes with the same three digits must contain more than 20,000 people; otherwise, the three digit code must be changed to "000".)

3. All elements of dates (except year) for dates directly related to the individual, including birth date, treatment date, lab work date, date of death; all ages over 89 and all elements of dates (including year) that indicate an age

4. Telephone numbers

5. Fax numbers

6. Electronic email addresses

7. Social security numbers, including the last four digits

8. Medical/dental chart or record numbers

9. Health plan beneficiary numbers

10. Account numbers

11. Certificate/license numbers

12. Vehicle identifiers and serial numbers, including license plate numbers

13. Device identifiers and serial numbers

14. Web Universal Resource (URLs)

15. Internet Protocol (IP) address numbers

16. Biometric identifiers, including finger and voice prints

17. Full face photographic images and any comparable images

18. Any other unique identifying number, characteristic, or code

The information is not considered de-identified if our dental practice (LCCC Dental Hygiene clinic) has any actual knowledge that the information could be used. This applies to information that could be used alone or in combination with any other information to identify an individual who is the subject of the information.

Avoid using redaction to de-identify a document
Remove the identifiers using a method that makes it impossible to read or re-create the identifiers, whether the document being de-identified is in hard copy or electronic format.

DO NOT use a pencil, pen, marker, etc., to hide the 18 identifiers on a paper document. This is because sometimes "redacted" information can still be read, especially if the document is photocopied or scanned. This can lead to a HIPAA violation or breach. Redaction cannot be used as a method of securing patient information under the BREACH NOTIFICATION RULE.

FOR MORE INFORMATION ON THIS RULE GO TO:
www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html

Privacy Officer Duties – Educate and train staff. HIPAA does not apply to PROPERLY de-identified patient information. Using and disclosing properly de-identified patient information when appropriate may help our dental practice avoid HIPAA violations and breaches of unsecured patient information. For example, if an instructor for a course would like to use a patient as a case study, providing the patient records with properly de-identified information can minimize the likelihood of breach. Additionally, if the only information we provide is properly de-identified, then HIPAA rules no longer apply.

XXII. BREACH NOTIFICATION 45 CFR 164.400 & 45 CFR 164.414

POLICY:
When our dental practice or one of our business associates discovers a possible breach of unsecured patient information, our dental practice will investigate and provide timely notification in compliance with HIPAA and applicable state laws, unless our dental practice can demonstrate, through an appropriate assessment of the relevant factors, including the four required factors, that there is a low probability that the information has been compromised.

PROCEDURES:
Staff Duties – Be alert for possible breaches and notify the Privacy Officer **immediately** if you suspect a breach has occurred. Following our dental practice's Privacy and Security Policies and Procedures can help minimize possible breaches of unsecured patient information.

Privacy Officer Duties – Put Breach Notification into action. Update the policies and procedures when appropriate, such as when there is a change in the law. Train workforce members to comply with the policies and procedures. In particular, train workforce members to notify the Privacy Officer **immediately** if they even suspect that a breach of unsecured patient information may have occurred. Train staff to follow our dental practice's Privacy and Security Policies and Procedures to minimize possible breaches of unsecured patient information.

Investigating and assessing possible breaches. If a breach is discovered, or if a workforce member or business or a business associate tells you about a possible breach, investigate immediately. If a breach of unsecured patient information has occurred, our dental practice may choose to provide the required notifications without performing a risk assessment. However, notification is not required if our dental practice can demonstrate that there is a low probability that the information has been compromised, based on an analysis of the relevant factors, including the four factors required under the Breach Notification Rule. Document the analysis using our Breach Assessment form. (See Breach Notification form in Appendix).

Sending Notification. If notification is required, consult with Vice President, Administration & Financial Services and LCCC General Counsel and, if necessary, draft notice letters that comply with HIPAA and other applicable law, and provide timely notice (complying with any applicable law enforcement delay) to affected individuals, HHS, and if required, to the media. Breaches involving 500 or more individuals must report to LCCC General Counsel, who then will determine what to report to HHS without unreasonable delay. The breach must be reported no later than 60 days after the discovery of the breach.
A log must be maintained of all breaches involving fewer than 500 individuals and submit the log annually to LCCC General Counsel to be submitted to HHS.

Substitute Notice. If we lack contact information for nine or fewer individuals involved in a breach, consult with LCCC General Counsel and proceed to contact the individuals via phone or using another means reasonable calculated to reach them. Do not provide patient information to unauthorized persons when providing substitute notice.

If we lack contact information for 10 or more individuals affected by a breach, consult Vice President, Administration & Financial Services and LCCC General Counsel to determine whether to post a conspicuous notice about the breach on the homepage of our website for 90 days, or to provide a conspicuous notice in major print or broadcast media in the area where the affected individuals likely reside, then provide substitute notice. Either form of notice must direct individuals to a toll-free telephone number that is active for at least 90 days that people can call to find out if their information was involved in a breach.

Electronic Communications. Determine whether asking patients to sign agreements permitting electronic communications would help the dental practice notify patients in the event of a breach of unsecured patient information. If so, develop an agreement to receive electronic communications and develop and implement a

process for requesting patient signatures and maintaining a record of the patients who have signed the agreement and an up-to-date record of the patient's email addresses, and a record of patients who have withdrawn their agreement to receive electronic communications.

Documentation. Retain all documentation related to our dental practice's compliance with the Breach Notification Rule for at least six (6) years from the date the document was created, or from the date the document was last in effect, whichever is later. Examples of breach notification documentation includes policies and procedures, breach assessment forms, copies of notification letters, logs, media notices, and press releases.
(See Breach Notification form, Breach Assessment form, Breach Log, and Agreement to Receive Electronic Communication form in Appendix)

XXIII. COMPLAINTS 45 CFR 164.530 (d), 45 CFR 164.530 (a) (1), 45 CFR 164.520 (b) (1) (vi) & 45 CFR 160.306

POLICY:
Our dental practice will provide a process for complaints about our HIPAA Privacy and Breach Notification policies, procedures, and compliance. Our practice will document any complaints received and their disposition, if any.

PROCEDURES:
Staff Duties – The Privacy Officer is responsible for receiving and processing complaints about our dental practice's privacy practices. If anyone complains to you about the privacy of patient information at our dental practice, or about how our dental practice complies with HIPAA, immediately put the person in touch with the Privacy Official.

Privacy Officer Duties – The Privacy Officer is designated to receive complaints about the privacy of patient information at our dental practice and about how our dental practice complies with HIPAA. When anyone makes a complaint, you must:

- Receive the complaint (by listening if the complaint is oral, or by reading if the complaint is in writing)
- Enter the time, date, and a brief description of the complaint into our complaint log
- Determine the appropriate disposition of the complaint (any required follow up)
- Communicate and seek advice, if necessary, with Administration and/or LCCC General Counsel

Should a sanction (disciplinary action) be applied against a workforce member who violated a policy or procedure?

Should an unauthorized disclosure be logged in case a patient asks for an accounting of disclosures?

Has there been a breach of unsecured patient information requiring notification?

Retain all documentation related to complaints for at least six (6) years from the date the document was created, or six (6) years from when the document was last in effect, whichever is the later.
At no time will our practice retaliate against an individual for filing a HIPAA complaint.
(See Complaint Log form in Appendix)

XXIV. FUNDRAISING 45 CFR 164.514 (f) & 45 CFR 164.520(b) (1) (iii) (A)

POLICY:
Our dental practice does not conduct fundraising for the benefit of the LCCC Dental Hygiene Clinic. Our dental practice will not use or disclose patient information to raise funds for the dental practice itself and will ensure that 45 CFR 164.514 (f) and 45 CFR 164.520 (b) (1) (iii) (A) are met.

PROCEDURES:
Staff Duties – Do not make fundraising requests to patients or use or disclose patient information for any purpose involving fundraising for monetary gain for the LCCC Dental Hygiene Clinic.

Privacy Officer Duties – Train staff not to make fundraising requests to patients that would benefit the LCCC Dental Hygiene Clinic, monetarily. Do not use or disclose patient information (LCCC Dental Hygiene Clinic) for fundraising purposes.

Our dental practice will not use or disclose patient information to raise funds for the dental practice itself and will ensure that 45 CFR 164.514 (f) and 45 CFR 164.520 (b) (1) (iii) (A) are met and train staff to comply with the applicable procedures.
(See Notice of Privacy Practices in Appendix)

XXV. REVIEW AND REVISE 45 CFR 164.530 (i)

POLICY:
Our dental practice will revise our HIPAA policies and procedures as necessary and appropriate to remain in compliance with HIPAA. It is recommended that a HIPAA Compliance Update Service is contracted or purchased from the American Dental Association or other creditable entity so as the Privacy Officer and others involved in updating the LCCC Dental Hygiene Clinic HIPAA Manual can remain current with federal, state, and local law.

Staff Duties – Our dental practice will revise our HIPAA policies and procedures as necessary and appropriate to remain in compliance with HIPAA. It is the staff's responsibility to read, review, learn and know our HIPAA policies and procedures to ensure our patient's privacy. It is also our staff's responsibility to train, mentor, and guide our student population so that they understand the severity and consequences of their actions regarding patient privacy rights.

Faculty Duties - It is recommended that for any laboratory and clinic in our program (where patients are provided services), that each course faculty person addresses HIPAA in their course syllabus and to indicate that consequences will occur should the student not follow patient privacy practices. Penalties or sanctions should be serious enough so that students understand that they will be held accountable for their actions.

Privacy Officer – Revise our dental practice's privacy and breach notification policies and procedures as appropriate so that our dental practice remains in compliance with HIPAA. When our Policies and Procedures are revised, train our workforce to comply with the new policies and procedures.
If a change affects our Notice of Privacy Practices, revise it appropriately.

Document any changes to our HIPAA policies and procedures, and retain both the new and the old policies and procedures for at least six (6) years from the date the document was created or the date when the document was last in effect, whichever is later.

LARAMIE COUNTY COMMUNITY COLLEGE

ACKNOWLEDGEMENT OF RESPONSIBILITY AND CERTIFICATION OF TRAINING FOR HIPAA AND SECURITY POLICIES AND PROCEDURES

(To Be Signed By All Employees/Students in the Dental Hygiene Department)

I understand and acknowledge that:

It is my legal and ethical responsibility as an authorized user to preserve and protect the privacy, confidentiality and security of all confidential information relating to Laramie County Community College Dental Hygiene Clinic (hereafter, referred to as the dental practice), its patients, activities and affiliates, in accordance with the applicable laws and the dental practice's policy.

I have received HIPAA security and privacy training materials and understand the requirements for security and privacy compliance. I agree to abide by LCCC Dental Hygiene Program guidelines, standards of conduct, and policies set forth. I will access, use or disclose confidential information only in the performance of my duties, when required or permitted by law and disclose information only to persons who have the right to receive that information. When using or disclosing confidential information, I will use or disclose only the minimum necessary information.

I have clarified any questions I have in relation to this information, training and policies.

I agree to immediately report to the Privacy/ Security Officer any changes, incidents or events that may potentially place me in violation of LCCC's compliance policies or any applicable state and federal laws or regulations.

I agree that I will report any suspected or known violations of our Security and/or Privacy compliance practices to the Security/Privacy Officer or other ranking Organization administrative authority prior to making any disclosure to governmental authorities. I understand that such notification does not restrict or limit my ability to notify governmental authorities any time I believe illegal activity has occurred or is occurring.

Under state and federal laws and regulations governing a patient's right to privacy, unlawful or unauthorized access to or use or disclosure of patients' confidential information may subject me to disciplinary action up to and including program dismissal or termination from my employment with Laramie County Community College, civil fines for which I may be personally responsible and criminal sanctions.

Print Name: _____

Signature: _____

Date: _____

Laramie County Community College Representative:

Signature:_____ Date: _____

Privacy & Security Officer: Program Director
1400 E College Drive
Cheyenne, WY 82007

Telephone: 307-778-1386