**SUBJECT**: HIPAA PRIVACY, SECURITY, BREACH NOTIFICATION POLICIES AND PROCEDURES

**PRESENTED DATE**: 8-27-2013, 1-15-2015, 1-19-2017

**REVISED DATE(S**): 1-3-2014, 1-12-2015, 11-29-2016

**POLICY STATEMENT:** All employees of the Wilkes Public Health Dental Clinic will protect the confidentiality of Protected Health Information (PHI) of any patient. This policy is designed to assure compliance with all applicable federal and state laws and regulations that require an individual’s personal health information to be kept confidential and private.

1. PURPOSE:

To ensure compliance with the Federal Law and protect the privacy and security of any protected health information that is accessed, used, or disclosed of any patients of WPHDC. The policies and procedures are designed to be in compliance with the Notice of Privacy Practices of Wilkes County. All employees are expected to read and follow all applicable practices described in the Notice of Privacy Practices.

1. DEFINITIONS:
2. **HIPAA**: The Health Insurance Portability and Accountability Act is a Federal regulation that safeguards health care recipient’s personal health information. The policy provides protection for individuals, while allowing entities to share information for the sake of quality care. HIPAA is governed by the Office of Civil Rights and the U.S. Department of Health and Human Services. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate use of standards for the electronic exchange of health care date; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personal identifiable health care information.
3. **Privacy Rule**: The Privacy Rule is a collection of documented national standards governing how personal health information is used, as well as who is allowed to see it. Specifically, personal health information is individually identifiable information—information that identifies you individually.
4. **Individually Identifiable Health Information**: This is health information that “identifies the individual, or for which there is a reasonable basis to believe it can be used to identify an individual.” This definition is important because it states that some, but not all, of your personal information may be disclosed. If your doctor or care facility shares information with outside parties, they cannot disclose your identity or information that would provide your identity.
5. **Covered Entities**: Only certain entities are subject to HIPAA compliance. An entity may be a person, business or organization. These entities are: health plans, insurance companies, health care providers, and health care service clearinghouses.
6. **Health Care Clearinghouse**: Health Care Clearinghouses are business or organizations that process health information for your doctor or care facility. A clearinghouse company most likely is in the business of translating health information into standardized data.
7. **Business Associates**: Business associates of the covered entities are subject to HIPAA compliance. Such an associate is defined as any entity that performs duties for the covered entity, but is not a part of the covered entity’s work force. Work force individuals may be employees or independent contractors. An example of a business associate would be an outsourced company that processes your doctor’s medical billing. Business associates are subject to HIPAA only if they handle your health information.
8. SCOPE:

All employees (full time and part time), volunteers, WDC Board Members, and individuals involved with patient care at the Wilkes Public Health Clinic.

1. PROCEDURE:

All employees are required to keep protected health information private and confidential. Employees shall limit use and disclosure of protected health information to those purposes necessary to perform their job functions, and to follow the policies and procedures below:

1. Security Management Process

As a Wilkes Public Health Dental Clinic employee, you are not permitted to disclose any confidential information obtained while working for the Clinic without prior approval from your Executive Director. You will also need patient approval. Under no circumstances may you use such information to advance the financial or private interests of yourself or others. Violation of this rule constitutes grounds for dismissal.

1. Workforce Security
2. All employees should be screened and familiar with the Clinic and the general policies.
3. All initial hires will receive HIPAA training as part of the Clinic Orientation.
4. Employees will be given practical applications to avoid misuse of patient information in day-to-day activities.
5. Monthly Staff Meetings will include a review or update on HIPAA policies and procedures as well as attention to any activity that could have resulted in misuse or lack of protection of a patient’s PHI.
6. Upon job separation, the clinic shall remove access to the company’s database and software, change passwords, recover keys, and cancel email.
7. Information Access Management
8. Users of any of the systems (Dentrix, NC Tracks, Dexis, and Third Party Payor Web Address) are restricted and have limited access. Employees who are given rights to any of the systems shall obtain a unique password from the database administrator.
9. All patient information should remain confidential and charts/folders should be stored in a secured manner.
10. Any disposable client information (routing slips, sticky notes, schedules, etc.) that contains a patient’s full name, date of birth, address, government issued ID, birth certificate, or social security number should be shredded at the end of the day or locked in a closed container to avoid a breach in HIPAA. PHI will be shredded in house or through a commercial business that provides a document destruction form.
11. Security Monitoring
12. All PCs and/or laptops that contain protected health information will be positioned so that they are out of the direct view of the patient and/or other staff members who are not involved. If the office is configured in a way that the computer monitors do not protect viewing of this information, privacy screens may be used.
13. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging off when unattended.
14. Upon turning on the computer, the employee must read and agree to the HIPAA Policies Notification which states: “I agree to comply with the Wilkes Public Health Dental Clinic HIPAA privacy, security, Breach Notification Policies and Procedures and assume responsibility for any personal violation of these policies and procedures”.
15. Data administrators will monitor misuse of the system(s).
16. Individual login IDs will be periodically audited to meet HIPAA regulations. It is important for the employee to only access PHI when applicable. The employee’s audit history will be recorded in the security manual. Each employee will be audited at least one time per year. The staff member must keep his or her password confidential, as they will be held accountable for inappropriate patient data accessed under their ID. Sanctions will be applied.
17. Users to the system(s) authorized shall log-on under the username and password provided.
18. Log-off immediately after the system(s) is no longer in use.
19. Clinic employees are responsible for their passwords and accounts. Passwords should be changed every three months.
20. Any changes made to any patient’s information needs to be verified using two forms of ID (ex. Full name, date of birth, address, government issued ID, birth certificate, and social security number) and only accessed when applicable.
21. Facility Access Controls
22. No patient data should be taken outside the clinic unless applicable, patient approved, and authorized by the Executive Director. Employees who work outside the department should have patients’ information locked in containers and restrict phone conversations when discussing patient information.
23. All deliveries from outside vendors should be signed and verified immediately.
24. Device and Media Controls Policy
25. No Clinic employee shall remove, modify, store, or recreate hardware/software or electronic media within or outside the facility that contain private information.
26. Person or Entity Authorization Policy
27. All clinic employees will limit access and use of protected health information to the minimum necessary to accomplish the intended purpose of use.
28. All employees shall have nametag or clinical lab coat with their name visible when in the work area.
29. Non-employees shall sign in and have an I.D. badge visible when in the work area.
30. Required identification of individuals:

1. Clinic employees shall be asked to verify I.D. if not visible.

2. Law Enforcement shall be asked to verify I.D. if not visible.

* I.D. badge number shall be recorded when requesting access to protected health information areas.

3. Business Contacts (Maintenance, Delivery, Vendors, etc.)

* I.D. and business information shall be visible on uniform.
* Persons shall sign a confidentiality agreement as part of the business contract or personnel records.

4. Non-Traditional I.D. and/or escort shall accompany non-

 traditional Employees (Volunteers, Students)

* Temporary I.D. and/or escort shall accompany non-traditional employees.
* Persons shall sign a confidentiality agreement upon starting day.
1. Finance and Administration – Computer Ops shall maintain an updated employee list with access permissions for all staff.
2. The list shall have the employee Name, Position, Division, and Systems Accessible.
3. Transmission Security Policy (Fax, Email, Copying from software system)
4. All fax machines are to be placed in a secure location and any faxes received should be business related and delivered to the proper department/receiver. All faxes or emails containing patient information must have a confirmation that they were received and the confirmation should be scanned into the document center under the appropriate category.
5. Avoid sending confidential information by email. If information is sent, it must be secured by including in a Microsoft Word or Excel file and protected with a password. The e-mail must be encrypted.
6. If the Microsoft work e-mail is accessed on the employee’s personal cellular device, the device must have password protection.

10) Social Networking (Facebook, My Space, Twitter, Instagram, etc.)

This section is further defined as the Social Media Policy.

1. Do not, under any circumstance, mention a patient’s name in a post or a private message. If the word “patient” is going to be mentioned in the post, the post should not be made.
2. As an employee, you should be conscious of what you post and make sure comments do not identify a patient or lead to the identity of a patient or staff member. Additionally, family members of staff should not be listed in a post without expressed permission.
3. No negative comments should be made about the clinic either specifically or in general. This includes information about the internal business of the office.
4. Only employees authorized to do so by the WPHDC may speak on behalf of the clinic, promote programs, services, and important health news/information on social media outlets. This information must be submitted to the Executive Director in writing and approved prior to the post. Examples include job postings and Dental Health Fair information.
5. Should you receive a friend request from a patient, past or present, use your own discretion. If you feel comfortable with them knowing more about you or seeing your pictures then use your best judgment to protect yourself. If not, decline the request.
6. Do not “recommend” to other staff members to be their “friends”. That should be left up to the individual staff member.
7. Be cautious of “friending” a patient. Their motives may be to get you to discuss their personal information you have access to through the clinic, discuss other patients, discuss information about staff members, or entrap you into breaking office confidentiality policies.
8. RISK ANALYSIS:
9. The HIPAA Official will conduct an initial analysis of any potential risks to the confidentiality, integrity, and practice’s electronic health information. The findings will be presented to the staff and addressed in the HIPAA manual.
10. Annually, the HIPAA committee will conduct a Security Risk Analysis. The risk analysis sheets will be retained in the HIPAA manual.
11. Monthly HIPAA risk assessments will also be conducted to ensure PHI is secure. Assessments will be conducted in various parts of the clinic (pedo hall, adult hall, front desk, etc.) and at different times of the day. Assessment findings will be discussed in the monthly staff meetings.
12. Any staff member identified not following policies or procedures to protect patient PHI will have the situation documented in their personnel file and retraining conducted.
13. Periodically, the risk analysis section and forms will be updated and placed in the manual.