What Virginia’s Free Clinics Need to Know About HIPAA and HITECH

This document is one in a series of tools and white papers produced by the Virginia Health Care Foundation to help Virginia’s free clinics professionalize various aspects of their operations.

Many thanks to Beth A. Bortz for researching and writing this paper.

What Virginia’s Free Clinics Need to Know About HIPAA and HITECH

Traditionally, one of the benefits of providing health care in a free clinic setting has been relative freedom from administrative bureaucracy, paperwork, and federal rules and regulations. Because free clinics haven’t billed for services, and few electronically transfer patient information to external partners, free clinics have been able to operate without needing to know much about the federal laws and regulations surrounding the protection of patients’ private health information when it is transmitted via electronic systems.

The health care delivery environment is changing rapidly, and many of Virginia’s free clinics are trying to adapt. As technology has evolved, most free clinics have moved from paper files to utilizing some sort of electronic system to track and manage patients. Many have a patient information management system, and several have adopted an electronic health record (EHR) system. Many more are now seriously considering adoption of an EHR as they prepare to exchange patient information with local partners such as hospitals, pharmacies, and laboratories in an effort to advance the quality of patient care they offer. Some are also exploring EHRs as part of their overall considerations about becoming a Medicaid provider. Others, who are considering providing certain services for a fee, or contracting with other local entities to provide services, will need an EHR, as well.

As a result of this evolution, it would be prudent for Virginia’s free clinics to become more familiar with both the Health Insurance Portability and Accountability (*HIPAA*) Act and the supplementary Health Information Technology for Economic and Clinical Health (*HITECH*) Act. Understanding the basic elements of both of these federal laws, specifically as they may relate to free clinic operations, is an important element of evaluating current clinic protocols, and planning for future options/operations.

What Is HIPAA and To Whom Does It Apply?

The Health Insurance Portability and Accountability Act (*HIPAA*) of 1996 was enacted to improve the efficiency and effectiveness of the health care system in a new age of technology by establishing a standard set of rules to prevent inappropriate use and disclosure of an individual’s health information, and to require organizations which use health information to protect that information and the systems which store, transmit, and process it.

Organizations must comply with HIPAA if they are classified by the law as either a “covered entity” <u>OR</u> a “business associate.”

***Covered Entities*:**

Virginia free clinics operating under the current business model of "free care, no billing" are not "covered" entities under HIPAA. A covered entity is defined as a practice or organization which:

- Furnishes, bills, or receives payment for health care in the normal course of business, AND
- Transmits any covered transactions electronically.

Both parts of this statement must be true to be a covered entity.

(*To confirm that your free clinic is not a covered entity, please visit www.hipaanews.org/Documents/Flowcharts.pdf*)

If a clinic does furnish, bill or receive payment for health care, then it must also transmit "covered transactions" electronically to be considered a covered entity. This includes transmissions via a third party billing service or vendor.

"Covered transactions" include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which Health and Human Services has established standards under the HIPAA Transactions Rule. (*For a complete list of standard transactions, please visit www.ama-assn.org/resources/doc/psa/hipaa.tcs.pdf*).

It is important to note that fax and voice transmissions are NOT considered transactions via electronic media. Electronic media transactions include those via magnetic tape, disk, CD, internet transmissions, leased or dial-up lines, private networks, and direct data entry.

***Business Associates*:**

The HIPAA regulations also apply to the "business associates" of covered entities. HIPAA defines a business associate as an individual or entity that performs, on behalf of a covered entity, any function or activity involving the use or disclosure of "protected health information" and is not a member of the covered entity's workforce.

"Protected health information" (PHI) is individually identifiable health information held or transmitted, in any form or media, whether electronic, paper, or oral that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual.

This data must also identify the individual or provide a reasonable basis to believe it can be used to identify the individual. Examples of identifiable data include names, social security numbers, zip codes, dates, phone numbers, and addresses.

While it would appear that some free clinics may be business associates because they share protected patient information with local hospitals, laboratories, pharmacies, and physician practices (*all covered entities*), there is an important exception to this HIPAA standard. CFR 164.502(e) states that "disclosures by a covered entity to a health care provider for *treatment* of the individual" are excepted.

Thus if the free clinic is electronically exchanging protected patient information solely for the purpose of providing treatment, and is not engaging in any of the other functions or activities defined as business associate activities or functions, then it is exempt from HIPAA compliance.

The other activities or functions that a free clinic could engage in that would require HIPAA compliance include: claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, and practice management. While it does not appear that Virginia's free clinics are engaged in these activities or functions currently, some may elect to undertake them in the near future. Examples include contracting with an accountable care organization to provide care management to the chronically ill, or charging a fee (even a sliding scale) for services provided.

If you are uncertain as to whether or not your clinic is a business associate, a very helpful flow chart can be found at http://www.hipaabusinessassociates.com/downloads/business_associate_flow_chart.pdf

If your clinic does begin to engage with a covered entity as a "business associate," HIPAA requires that the covered entity include certain protections for the privacy of patient information in a Business Associate Agreement. The agreement must contain specific written safeguards on the individually identifiable health information used or disclosed by its business associates, and may not contractually authorize a business associate to make any use or disclosure of protected health information that would violate the Privacy Rule. For detailed guidance on the preparation of a business associate agreement, please visit www.hhs.gov/ocr/privacy /hipaa/understanding/coveredentities/contractprov.html

What is HITECH and Does It Also Affect Free Clinics?

HITECH (*Health Information Technology for Economic and Clinical Health*) is a related law that was enacted as part of the American Recovery and Reinvestment Act of 2009. It expanded HIPAA's requirements and patient protections, and added teeth for enforcement via substantial civil (financial) and criminal penalties. These penalties apply both to covered entities and business associates.

Recommended Steps to HIPAA Compliance

If you determine that your clinic is currently required to be HIPAA/HITECH compliant, or is likely to be in the future, you will probably need to make some adjustments to your operations. To determine the extent of the adjustments and prepare for them, you will need to designate someone to be responsible for learning about HIPAA/HITECH and overseeing implementation and compliance. While this will require extra time and attention within the clinic, you won't have to re-invent the wheel. Fortunately, tens of thousands of medical practices have made these adjustments in the past 16 years, and there is an abundance of helpful information, forms, and procedures available to assist you.

The bulk of the work related to HIPAA/HITECH compliance will be a one-time effort of learning and introducing the required elements to your clinic. After that, implementation should be routine.

- A recommended first step is to visit www.hipaanews.org, where there is a wealth of fact sheets and procedural recommendations.
- This site identifies six phases required to achieve compliance. They are:
  - Awareness (*staff and volunteer education on what to expect from HIPAA*);
  - Gap analysis (*determining gaps between current and required practices*);
  - Implementation planning (*setting plan, budget, and timeline to meet HIPAA requirements*);
  - Implementation (*deploying the Implementation Plan*);
  - Regular training (*on new policies, procedures, and system changes and updates*);
  - Audit and compliance (*on-going monitoring and enforcement*).
- The site also lists 15 fundamental steps to implement and comply with HIPAA/HITECH. They are:
  - Read and become familiar with regulations; get help where needed.
  - Set objectives and scope of overall compliance effort.
  - Appoint privacy and security compliance officer.
  - Take inventory of computer/information systems (*including paper records*); understand current transactions/code sets environment and uses.
  - Take inventory of security and privacy policies and procedures.

- Identify gaps and weaknesses in office practices, policies, systems, and procedures - as they relate to HIPAA requirements.
- Determine planning priorities and formulate implementation budget.
- Begin promoting HIPAA awareness within office.
- Revise and improve existing security and privacy policies; implement new policies and procedures as needed.
- Deploy new physical and technical safeguards to support policies and procedures.
- Integrate and roll out new or upgraded processes and systems.
- Create reporting and documentation procedures with feedback mechanism.
- Implement necessary ongoing changes.
- Do initial workforce training on new policies and changes, and provide for ongoing training program.
- Provide process for addressing privacy/security breaches when and if they arise.

• One of the most effective starting tools is the HIPAA checklist included below. It can be found online at http://hipaanews.org/checklist.htm

HIPAA CHECKLIST				
#	**Question**	**Not Started**	**In Process**	**Completed**
	Awareness & Education			
1	Has your organization had any Awareness Education on HIPAA Regulations and Compliance?			
2	Do you monitor or receive automated information regarding changes in HIPAA regulations			
	Project Planning			
3	Have you selected a Project Manager and Project Team for your HIPAA Project?			
4	Have you created a Project Plan?			
	Electronic Transactions			
5	Have you applied for the ACSA Electronic Transaction extension for your organization?			
6	Have you completed an inventory of all information systems and work flow processes with regard to Electronic Transactions?			
7	Have you compiled a list of vendors, health plans, business associates and trading partners?			
8	Have you gathered, reviewed and compared your current billing forms, policies, and procedures to the HIPAA Electronic Claims Transaction and Code Set regulations?			

Privacy				
9	Has your organization designated an Information Privacy and Security Officer as required by HIPAA?			
10	Have you developed a Notice of Information Practices to post in your office and distribute to each patient?			
11	Have you gathered, reviewed and compared your current forms, policies, and procedures to the HIPAA Privacy Regulations and State Privacy Regulations?			
12	Have you developed policies and procedures that meet the needs of your Human Resources Department with regard to Privacy requirements for the protection of health information of your staff?			
13	Have you developed processes for documenting, retaining, distributing and discarding Protected Health Information (PHI) as required by HIPAA?			
14	Have you developed processes for receiving, investigating and documenting individual complaints?			
15	Have you developed or revised current consent forms for patients in line with HIPAA regulations?			
16	Do you have all forms that must be read and signed by patients in languages appropriate to their culture?			
Security				
17	Has your organization completed a Security Evaluation on the information systems used in conjunction with maintaining your current and future Protected Health Information?			
18	Does your organization have virus checking software, firewalls and operating systems that provide encryption and other security measures?			
19	Does your organization perform back-ups of your data daily?			
20	Does your organization have a Disaster Recovery and Contingency Plan to meet the HIPAA Security Standards?			
21	Has your organization developed security policies and procedures with regard to confidentiality statements, individually identifying information system users, passwords, automatic logoff, acceptable use, e-mail, internet usage, authentication of workstations, monitoring and documenting unauthorized access, audit trails of users, sanctions for misuse or disclosure and termination checklists?			
22	Has your organization provided for the overall physical security of your information systems, facility, staff, and medical records?			
23	Has your organization developed job descriptions for HIPAA required positions and all other positions in your organization?			
National Identifiers				
24	Have you located, printed and read the Proposed Regulations for National Identifiers to include National Provider Identifier and National Payer Identifier, National Employer Identifier?			
General Information				
25	Have you developed a comprehensive training program for your organizations staff (both present and future) covering all HIPAA standards to include responsibilities and penalties for non-compliance?			
26	Does your organization have a Compliance Officer and General Compliance Plan to cover such things as fraud and abuse, codes of conduct, whistle-blower suits, auditing and monitoring, disciplinary standards and personnel issues, responding to problems, investigations and corrective actions?			

The good news is that while HIPAA/HITECH compliance may seem difficult at first, it gets significantly easier once a system is in place. Moreover, there are a great many resources that have been developed within the last decade to assist medical practices, which can be modified easily for free clinics. Recommended resources include:

- http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-compliance-resources.page
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html
- http://www.hipaabusinessassociates.com
- http://www.hipaanews.org/outline.htm
- http://www.dmas.virginia.gov/hpa-home.htm
- http://www.dmas.virginia.gov/hpa-hipaa_faqs.htm