Introduction to HIPAA for Psychotherapists

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) can be confusing and scary to psychotherapists. But it is very relevant to Digital Law and Ethics. Much of the protections we put into place are as a result of HIPAA regulations. It is considered best practice to follow these rules even if you are not a covered entity.

This handout gives you a basic overview of the different aspects of HIPAA so that you will learn whether or not you are a covered entity and therefore obligated to comply with HIPAA standards. If you are a covered entity you will learn what you need to do in your practice to comply with HIPAA standards. This is an overview focusing on the areas most relevant to those in private practice. It is not a comprehensive overview of HIPAA. Most of this information is taken directly from United States Department of Human Services training materials.
History of HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law on August 21, 1996. Its purpose was to "improve efficiency and effectiveness of health care system by standardizing the electronic exchange of administrative and financial data." ¹ The Department of Human Services (HHS) was mandated to adopt specific transaction standards, security and electronic signature, unique identifiers for employers, health plans, and healthcare providers. ² HIPAA was the first comprehensive federal health privacy protection implemented into law. ³ The law required that by April 2004 privacy standards were to be in effect for all covered entities. There have been several subsequent additions to the law.

The Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) provisions were added as a part of the American Recovery and Reinvestment Act of 2009. Final regulations for HI-Tech were released in January 2013 and are effective March 2013 with full implementation for providers by September 2013.

In 2010 as part of the Patient Protection and Affordable Care Act, there were new standards added, such as a standard for electronic funds transfers. Penalties for non-compliance were also increased.

¹ United States Department of Health and Human Services "HIPAA Privacy Rules" National Conferences 2003
² Ibid
³ Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
Privacy Rule

The first aspect of HIPAA that will be discussed is the Privacy Rule. There are six key elements to the Privacy Rule.

Key Elements of the Privacy Rule

1. Covered Entity
2. Uses and Disclosures
3. Research
4. Individual rights
5. Administrative Requirements
6. Compliance and Enforcement

1. Privacy Rule-Covered Entities

What is a covered entity?

To understand covered entities you must first understand the definitions of health care providers and business associates.

A Health Care Provider is defined as:
"Any person or organization who furnishes, bills, or is paid for healthcare in the normal course of business."  

A Business Associate is defined as:
A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or for a covered entity. Their business functions may include claims processing, data analysis, quality assurance, benefits management, and practice management. Some examples include a billing service, and accounting services, or a health care clearinghouse such as Office Ally that submits claims on behalf of a provider.

4 Ibid
5 Ibid
6 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html accessed 1/2/13

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
The Department of Human Services defines Covered Entities as "Health care providers who transmit any health information electronically in connection with certain transactions." Providers include individual or group providers, health plans, and health care clearinghouses.  

These health care providers are only a covered entity if "they transmit health information electronically in connection with a transaction covered by the HIPAA Transaction Rule." This applies whether it is done directly or through a business associate such as a billing person.

The transactions that trigger a health care provider to be a covered entity are as follows:

1. "Health care claims or equivalent encounter information
2. Health care payment and remittance advice
3. Coordination of benefits
4. Health care claim status
5. Enrollment or disenrollment in a health plan
6. Eligibility for a health plan
7. Health plan premium payments
8. Referral certification and authorization"

To simplify, the list of transactions above means if you bill online, check health insurance eligibility online, get billing advice online, and/or get authorizations for clients online you are considered a covered entity.

A Business Associate is a concept we will return later in the course and is relevant to therapist’s complying with HIPAA.

---

8 Ibid
9 Ibid
2. Privacy Rule-Uses and Disclosure

Protected health information (PHI) is defined as "individually identifiable health information that includes health information, including demographic information, relates to an individual’s physical or mental health or the provision of or payment for health care, and identifies the individual."\(^{10}\)

A covered entity may not release PHI except as permitted by the Privacy Rule. You are required to release PHI to the patient and to HHS to investigate compliance with the Privacy Rule. \(^{11}\)

*It is important to remember that HIPAA requirements are for all medical providers. There are allowable reasons that PHI can be released in HIPAA that would violate a psychotherapist's confidentiality requirements. Obviously, in those cases, you would defer to confidentiality requirements.*

Covered Entities are allowed to release PHI to carry out essential health care functions such as
- Treatment
- Payment
- Health care operations \(^{12}\)

This is considered Treatment, Payment, and Health Care Operations (TPO)

**Treatment** is defined as "the provision, coordination, or management of health care by one or more health care providers, including consultation between health care providers; or patient referrals." \(^{13}\)

**Payment** is defined as health care provider activities that involve being reimbursed for services rendered.

**Health Care operations** include activities to evaluate services, get credentialed, and other normal business activities

There are also Public Policy Purposes for the release of PHI. They include:
(1) As required by law
(2) For public health
(3) About victims of abuse, neglect or domestic violence
(4) For health oversight activities
(5) For judicial & administrative proceedings


\(^{11}\) Ibid

\(^{12}\) Ibid

\(^{13}\) Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
(6) For Law Enforcement purposes
(7) About decedents (to coroners, medical examiners, funeral directors)
(8) For cadaveric organ, eye or tissue donations
(9) For research purposes
(10) To avert a serious threat to health or safety
(11) For specialized government functions (Military, veterans, National Security, Protective Services, State Dept., Corrections)
(12) For workers’ compensation.” 14

**Minimum Necessary Requirement**

An important aspect of the Uses and Disclosures part of the Privacy Rule is the concept of Minimum Necessary Requirements.

This requirement states:

"Covered entities must make reasonable efforts to limit the use or disclosure of, and requests for, PHI to minimum amount necessary to accomplish intended purpose" 15

*This means that if you release information you must limit it to the minimum amount of information needed to meet your purpose for the release of information.*

*An authorization is required for any release not covered in the Privacy Rule. This authorization must include the expiration date of the authorization and a statement that it is revocable.*

**3. Privacy Rule-Research**

I will not go into this in depth, as it is not relevant to most practitioners. PHI can be used for research with the patient's consent. There are certain limited exceptions to this. For more detailed information please see the Bibliography reference.

---

14 Ibid
15 Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
4. Privacy Rule Individual Rights

The Privacy Rule gives clients a very clear right to be informed of the privacy practices of both their health plans and their health care providers.

*To comply with HIPAA you must offer each of your clients a copy of your Privacy Practices and document that they were offered this document.*

Your Privacy Practices Notice must be in plain language and has to have some specific items included in it.

**Your Privacy Police notice should include:**

1. How you may use and or disclose protected health information (PHI) about your clients.

2. What the client's rights are in regards to the information and an explanation of how those rights might be exercised, including how to make complaints.

3. A statement of your legal duties in regards to the information clearly stating how you are required by law to protect PHI.

4. A statement on who to contact for more information about your policies. This will normally be your name.

5. This notice must include an effective date of the notice. This would be the date you began your privacy policies.  

6. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For example "upon termination of therapy".

*In regulations that go into effect September 26, 2013, your notice must also include*

6. A statement regarding the right of affected individuals to be notified following a data breach. This statement doesn't have to go into details as to the details of the reporting.  

16 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
7. If you keep psychotherapy notes you must have a statement that says that release of psychotherapy notes require a separate authorization. If you don't keep such notes say that in your privacy policy.

Psychotherapy Notes are defined by HIPAA as

"Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date." ¹⁸

*Italics are mine*

8. If you use PHI for marketing or sell it (not applicable to psychotherapists) you must have a statement that states a separate authorization is needed for those purposes. If you use PHI for marketing or sell it you should say that in your privacy policy.

9. You must include a statement that clients can request a restriction of disclosure of PHI to health plans if those services are paid for out of pocket and in full. ¹⁹

Please see the Hi-Tech Rule Section for more information on #9.

**Notice Availability**

1. Your notice must be made available to anyone who requests it and all clients must be offered one at your first meeting.

2. If you have a website your notice must be prominently displayed on the website.

3. It must be posted at any service location in an easily available area where clients may be reasonably expected to read it.


Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
Due to copyright laws, I am unable to reprint HIPAA notices here. However, I am providing some links to places where there are examples.

Since there was an update released January 2013 that needs to be implemented by September 2013-at the time of this writing the policies below have not be revised to include requirements 6-9.

CAMFT has a policy available for members. The link below only works if you are logged into their site

Alameda County Psychological Association also has a sample form http://www.alamedapsych.org/documents/acpahipaa%20form.pdf

NASW has information and a sample policy that may be accessed by members. This has been updated with the September 2013 information.

http://www.naswdc.org/hipaa/

**Access**
Clients have the right to obtain a copy of their PHI. Psychotherapy notes are excepted from this. You may deny this request if you believe that this access would harm a client. The client has a right to appeal this denial by obtaining a second opinion by a licensed heath care provider. For record requests, you are permitted to charge a reasonable cost-based fee for copying and postage.  

---

20 If you accept a client's request to see/receive their PHI you must make it available within 5 days and you have 15 days to provide a written copy. You may give them a treatment summary if they agree to accept that. If you are going to deny the request you have 30 days to provide written notice to the client explaining the reasons for the denial.  

**Amendment**
Clients have the right to request that you amend anything in their PHI that they believe is incorrect. You are required to document the request and whether you are granting it or not. Responses need to be made in writing to the client whether you are accepting or denying their request.

---

20 ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
**Disclosure Accounting**

Clients have the right to get an accounting of any disclosure of their PHI you have made for the six years prior to the date of the request. You do not have to account for disclosures made for:

(a) "for treatment, payment, or health care operations; (b) to the individual or the individual’s personal representative; (c) for notification of or to persons involved in an individual’s health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities." 22

*If you use electronically based notes there are some different rules that are explained on page 18.*

**Restriction Request**

Clients have the right to request that you restrict use or disclosure of their PHI in regards to treatment, payment, and disclosures to other providers and family members. You are not obligated to agree to these restrictions. 23

(except as changed in HI-Tech)

**Confidential Communications Requirements**

Clients can request different ways to request their PHI be communicated to them such as a closed envelope rather than a post card. You must accommodate all reasonable requests if a client feels endangered by a possible release of this information without question. 24

*Again here you would be following the more restricted confidentiality rules.*

---

22 Ibid
23 Ibid
24 Ibid
5. Privacy Rule-Administrative Requirements

In this section, I will focus on the administrative requirements that are applicable to private practices. This is not a comprehensive guide to administrative requirements.

The administrative requirements are the requirements that each covered entity must put in place in order to comply with the Privacy Rule. These include:

Having appropriate administrative, technical, and physical safeguards to protect the privacy of PHI." 25This includes things such as locked file cabinets and password protected computer files.

Having all staff receive privacy training as needed for their functions. 26

*This is applicable to practices where there are employees or interns. HIPAA training for staff should be documented.*

Have a designated privacy officer who is responsible for privacy policies and procedures."27

*For most private practices the privacy office will be the psychotherapist.*

Have a contact person designated that receives any complaints." 28

*Again for private practices, the therapist would be the person receiving complaints.* 29

Develop a process for individuals to make complaints to Covered Entity." 30

*This should be outlined in your Privacy Practice Notice.*

There are also documentation requirements –written or electronic for six years. You must have:

–Policies and Procedures for your office

_________________________________________________________________________

25 United States Department of Health and Human Services "Administrative Requirements"

26 Ibid
27 Ibid
28 Ibid
29 Ibid
30 Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
–Documentation that HIPAA training was provided
–Records of any complaints made and their disposition
–Notice of Privacy Practices, Acknowledgement, and Good Faith efforts to obtain Acknowledgments
–PHI Authorizations
–Business Associate Contracts
–Any PHI amendment requests and the results of the request

Again here I have focused on the documentation most relevant to a private practice. You should document that every client was offered a Privacy Notice. Any complaints should be thoroughly documented. Document in writing any requests made for PHI and the disposition of each request. Develop and use a PHI release. Document any training you have received on HIPAA. If you work with a billing or administrative person that is considered a "Business Associate" you should have a contract for that relationship. To see a sample of a Business Associate contract go to Resources Section at the end of the class.

6-Privacy Rule-Compliance and Enforcement
The Office of Civil Rights enforces HIPAA. They focus on promoting voluntary compliance with the law. However, if an entity knowingly violates a clients’ privacy rights the fines are as follows:

–Up to $50,000 & 1 year imprisonment
–Up to $100,000 & 5 years if done under false pretenses
–Up to $250,000 & 10 years if intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm

31 Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
**Transaction Standards**

An important aspect of the Privacy Rules is the Transaction Standards. The Standards were developed to help covered entities communicate more effectively with each other. Before HIPAA there were over 400 different ways to submit health care claims to health plans.  

As discussed previously the transactions are:

1. "Health care claims or equivalent encounter information
2. Health care payment and remittance advice
3. Coordination of benefits
4. Health care claim status
5. Enrollment or disenrollment in a health plan
6. Eligibility for a health plan
7. Health plan premium payments
8. Referral certification and authorization"  

If you complete any of these transactions you are required to follow the HIPAA standards for them.

One area where Transaction Standards are important is if you bill electronically. However, since you either will bill through the insurance company's website or a clearinghouse like Office Ally, you just have to make sure the site you use is HIPAA compliant. It is the same if you use any web based applications. Since HIPAA standards are the law any company dealing with this information would need to be compliant.

The other aspect of transaction standards that is relevant to psychotherapists is CPT and ICD codes. As I write the CPT codes were revised for 2013. You need to stay aware of any changes in CPT codes because if you don't your bills will be denied because you are not in HIPAA compliance. The same goes with ICD codes for diagnosis. You have to use the standardized diagnosis codes in order to bill successfully. You are forced to be in compliance in these areas in order to get paid.

---


33 Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
National Provider Identifiers
An important point relevant to Transaction Standards is The National Provider Identifier (NPI). The NPI is part of the HIPAA Administrative Simplification Standards adopted in 2005 and fully implemented in 2008.

The NPI is a unique 10-digit identification number for HIPAA covered health care providers. The NPI number doesn't include any information about a provider such as their specialty or state of practice. 34

Health care providers must share their NPI with other health care providers, health plans, clearinghouses, and any entity that may need it for billing purposes.

To get an NPI go to

https://nppes.cms.hhs.gov/NPPES/StaticForward.do?forward=static.npistart

Security Standards

The Security Standards were developed to expressly protect Electronic Protected Health Information. This is a subset of PHI, which is covered by the Privacy Rules.

The Security Standards protect any "identifiable health information a covered entity creates, receives, maintains or transmits in electronic form." 35

What Information is Protected

The Standards state that you must:

"Identify and protect against reasonably anticipated threats to the security or integrity of the information;

Protect against reasonably anticipated, impermissible uses or disclosures; and

Ensure compliance by their workforce." 36

HHS recognizes that smaller providers, such as sole proprietors, have to follow the same standards as big insurance companies. They take that information into consideration as to the level you need to protect the information.

There are several different aspects to the law. The first is

Risk Analysis and Management

This means all health care providers are required to complete a risk analysis, which assess any risk to e-PHI and then implement changes to minimize such risk.

Administrative Safeguards

The second part of the law is the Administrative Safeguards.

This requires that a covered entity identify any potential risks to e-PHI and take security measures to reduce any risks. Like the in the Privacy Rule, there needs to be a person designated a security official.

It also limits release of e-PHI to the minimum necessary information as discussed on page 5. 37

35 http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html accessed 1/2/13

36 Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
Physical Safeguards
The next aspect is physical safeguards. Here is required that physical access to your site is restricted. If you have staff this includes access to different computers and programs. You must have policies in place for the any electronic transfer or disposal of data. It also includes common sense protections liked locked offices and file cabinets.

Technical Standards
The Technical Standards mean that you have to protect how e-PHI is transmitted. This would include having a good anti-virus and firewall protection installed on any computer where you store client data. 38

Organization Requirements
This states that if you know a Business Associate is not following these requirements you must take action to make sure this is addressed.

Policy and Procedures
Like the Privacy Rule, this states that covered entities must have policies in place regarding all these requirements. These policies are supposed to be reviewed regularly.

37 ibid
38 ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
The Health Information Technology for Economic and Clinical Health Act ("HITECH Act").

The newest part of HIPAA is The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). There was a new release of rules from HHS in January 2013. These rules go into effect March 26, 2013, and covered entities must be in compliance by September 26, 2013.

Hi-Tech Breach Rule
A major part of HITECH is the Hi-Tech Breach Rule

To understand this we need to first define a breach.

A Breach is defined as any impermissible use or disclosure of PHI under the Privacy Rule.

Breach Notification Requirements
If you have a breach of a client's PHI the Hi-Tech Breach rule states you must notify the affected client, the Secretary of HHS, and in certain major circumstances the media. In addition, if a business associate has a breach they must notify the covered entity that used their services.

Individual Notice
An individual affected by a breach must be notified in no longer than 60 days. Notification must be by first class mail unless there is a prior agreement to accept notices via mail.

The letter must include:

A description of the breach.
A description of the information involved in the breach.
A list of steps the individual can take to protect them from harm.
A list of the steps you are taking to investigate the breach, mitigate harm and prevent further breaches.

Your contact information.39

39 ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
**Notice to the Secretary**
Notice to the Secretary may be made via the HHS website and again must be done within 60 days.

To submit a report:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

**Burden of Proof**
Again you are required to document that you have met all notification requirements. You are also required to have written policies and procedures if you have any staff.

Other Changes that were implemented in the HITECH Act include:

**Client's Right to Restrict Access.**
A client has the right to reduce the information a provider gives a health plan. A client can restrict information you give to a health care provider for any service for which they have paid out of pocket in full. 40

**Patient’s Right to an Accounting of Disclosures**
While clients always had a right to an accounting of disclosures, with the exception of disclosure made for treatment, payment, and healthcare operation, the Hi-Tech rule requires that if you keep electronic records the client can request three years worth of disclosures including those made for those reasons. 41

**New Requirements for Business Associates**
Now business associates must follow most of the Privacy Rule requirements and all of the Security Rule. Business associates must have the same administrative physical and technical safeguards that providers do. If you work with a business associate this should be included in your contract with them. 42 Business associates can themselves be held liable for breaches.

---

40 http://www.camft.org/AM/Template.cfm?Section=HIPAA1&Template=/CM/ContentDisplay.cfm&ContentID=1047
Accessed 1/12/13
41 Ibid
42 Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
**Prohibition on Selling a Patient’s PHI**
There was a requirement added that prohibits a covered entity from receiving compensation for selling PHI without an authorization. Obviously, this is something not relevant to psychotherapists.\(^{43}\)

**HIPAA Violations**
How HIPAA violations are assessed is now structured in a 3 Tier system, which distinguishes willful neglect from without knowledge neglect. \(^{44}\) There was a move against voluntary compliance to a more punitive standard.

**Private Cause of Action**
This allows other actions against violators of HIPAA. In CA it means that the Attorney General could advocate on the patient's behalf. \(^{45}\)

**Access to PHI**
If you keep any PHI in electronic form the client has the right to request to receive their PHI in that format. \(^{46}\)

**Sending PHI to Another Person**
A client has the right to request that a covered entity transmit their PHI directly to another person. The request must be in writing and signed by the client. The other person must be clearly identified in the statement along with where the PHI is to be sent. \(^{47}\)

**Deceased People Protections**
Privacy protections for deceased people end 50 years after their death.

**Privacy Policies Revisions**
If you had a Privacy Policy developed prior to these 2013 rules you will have to revise your Privacy Policy and post it prominently at your worksite and on your website by September 26, 2013. Copies must be available for anyone who asks for it.

You revision must include additional statements, which were discussed on pages 7-8 in the Privacy Policy section #'s 6-9.

\(^{43}\) Ibid
\(^{44}\) Ibid
\(^{45}\) Ibid

Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
What do I need to know to comply with HIPAA in plain English

To end this class here is a list of the most important things you will need to do in order to become HIPAA compliant.

1. Develop a Privacy Policy.

2. Post your Privacy Policy prominently at your office and on your website if applicable.

3. Document HIPAA training for yourself and any staff or interns.

4. Review your physical safeguards to assure compliance-including locked office doors and file cabinets.

5. Review technical safeguards to assure compliance include a firewall on any computer that has client date on it and password protected files.

6. Make sure any place you use e-PHI is HIPAA compliant such as online billing or note taking services.

7. Make sure if you outsource billing or other things where people would have access to client information that you have a Business Associates contract and that these Associates are following all of the same safeguards you follow.

8. Develop a PHI release, which includes an expiration date and a statement that it can be revoked at any time.

9. Either develop forms or make sure you have access to ways to document any complaints made or requests made for PHI. California Association of Marriage and Family Therapists have forms for all HIPAA requirements available on their website for members. There are also many places you can buy these forms.

10. Make sure your client's files have notations of any time you release PHI so that if an accounting is requested you can easily gather that information.
Bibliography


Copyright 2013 Cathy Hanville, LCSW-Get Down to Business Consulting
United States Department of Health and Human Services "Entities Covered by the HIPAA Privacy Rule"

United States Department of Health and Human Services "HIPAA Privacy Rule National Conferences2003"
http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/intro.pdf
access September 4, 2012.

United States Department of Health and Human Services "Protected Health Information"
http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/udmn.pdf

United States Department of Health and Human Services "Research"
http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/researchppt.pdf
Additional Resources

Frequently Asked Questions About the Disposal of Protected Health Information
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf

Sample Business Associate Contract

This was revised after the new regulations came out in 2013.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Fast Facts for Covered Entities

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/cefastfacts.html

Communicating with a Patient’s Family, Friends, or Others Involved in the Patient’s Care


Sample HIPAA Forms

If you are a member of CAMFT they have an extensive section of sample forms. You can access them when logged into their website at

http://www.camft.org

Administrative, Physical, and Technical Safeguard Standards Compliance Worksheet

CAMFT also has a worksheet for compliance of administrative, physical, and technical safeguards.