Primer on Privacy and Confidentiality

2009 CAPLAW National Training Conference

June 24, 2009
8:45 A.M. – 12:00 P.M.

Alicia A. Gilleskie, Esq.

Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.
2500 Wachovia Capitol Center
Raleigh, North Carolina 27601
Phone: 919-821-6741
Fax: 919-821-6800
agilleskie@smithlaw.com

© 2009 Community Action Program Legal Services, Inc.

Agenda

- Data Assessment and Protection
- Health Insurance Portability and Accountability Act (HIPAA)
- Appendix of Useful Resources

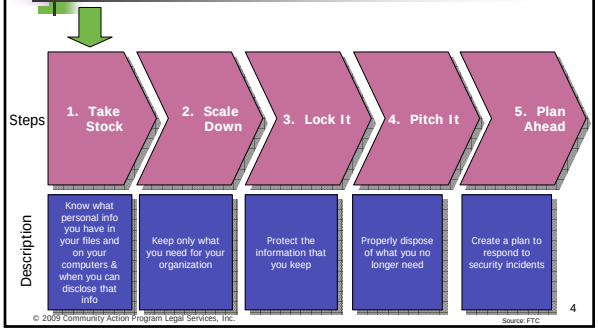
© 2009 Community Action Program Legal Services, Inc.

Why Should Your Organization Care?

- Fraud
- Identity Theft
- Loss of trust/reputation
- Trouble with funding sources
- Lawsuits

© 2009 Community Action Program Legal Services, Inc.

The Big Picture



© 2009 Community Action Program Legal Services, Inc.

Step 1: Take Stock

- Inventory all computers, laptops, flash drives, disks, home computers, and other equipment

- Inventory information by type and location
- Assess how personally identifying information retained

© 2009 Community Action Program Legal Services, Inc.

Step 1: What Info Do You Post Online?

- What personal information, if any, is posted on your web site?
- Is your newsletter posted on the web site, and, if so, does it include individuals' names and other personal information?
- Do you list the names of clients in captions of photos on your site?
- Do you obtain consent for posting client information online?

© 2009 Community Action Program Legal Services, Inc.

Source: Privacy Rights Clearinghouse

Step 1: Unauthorized Disclosure

- Unauthorized disclosure, *even if unintentional*, and even if unknown identity theft could result in:
  - Monetary penalty
  - Lawsuit by the affected individual
  - Citation by government funding source
  - Reputational harm
  - FTC enforcement
  - State Attorney General enforcement
- Disclosure rules vary from state to state

© 2009 Community Action Program Legal Services, Inc.

Step 1: Disclosure Process

A. Know what information is collected, through what means and in what form

B. Determine how the information is used and how it is disclosed by the organization

© 2009 Community Action Program Legal Services, Inc.

Step 1: Disclosure Process

C. Review contract terms, grants from funding sources, statutes or regulations incorporated therein, for confidentiality and disclosure/access provisions

D. Investigate any data disclosure and determine which laws on confidentiality and disclosure apply to the CAA

© 2009 Community Action Program Legal Services, Inc.

Step 1: What Info is Collected and in What Form?

- Similar to "taking stock"
- What type of "personal" data is collected?
  - Medical/health-related info?
  - Financial info?
- In what form is it collected?
  - Paper forms?
  - CAA-wide database?
  - Funding agency database?
  - Differences among programs or is there a standardized intake form?



© 2009 Community Action Program Legal Services, Inc.

Steps 1: Review Terms of Contracts and Grants

- Contracts/Grant Agreements may:
  - Require grantee to maintain confidentiality of client info
  - Permit/require government-funded sources access to records
- State contracts may:
  - Require compliance with state agency's internal confidentiality policies/guidelines or with a general state disclosure statute
- Grantees should identify:
  - Confidentiality provisions in fine print or referenced as a regulation citation
  - Conflicting provisions among programs

© 2009 Community Action Program Legal Services, Inc.

Step 1: What Confidentiality and Disclosure Laws Apply?

- Freedom of Information Act and the Privacy Act of 1974, 5 USC §§ 552, 552a
  - NOT applicable to private non-profit CAA's, even if receive federal funding
- Potentially Applicable Federal Laws
  - Patient records from a CAA-run alcohol/drug abuse treatment program are confidential with several exceptions
  - HIPAA
- State laws/regulations are important and vary widely
  - Privacy/confidentiality statutes
  - Public records laws
  - State CSBG statutes, regulations and contract/grant terms and conditions

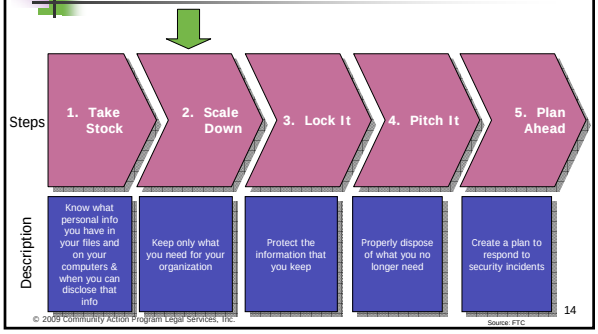
© 2009 Community Action Program Legal Services, Inc.

Step 1: Subpoenas & Centralized Databases

- Subpoenas
  - Law varies from state to state
    - E.g. must notify data subject in "reasonable time that he may seek to have the process quashed" (Massachusetts General Laws 66A(2)(k))
  - Check with local attorney
  - Check contracts to ensure understanding of disclosure obligations
- Centralized Databases
  - Determine who will have access to client info (e.g. funding sources)
  - Obtain consent from clients

© 2009 Community Action Program Legal Services, Inc.

The Big Picture



© 2009 Community Action Program Legal Services, Inc.

Step 2: Scale Down

- Identify info org no longer needs
- Use Social Security numbers only for required and lawful purposes
  - E.g. reporting employee taxes, verifying client eligibility (if required by funding source)
  - Don't use Social Security numbers unnecessarily (e.g. as an employee or client identification number)

© 2009 Community Action Program Legal Services, Inc.
Source: FTC

Step 2: Posting Paper Files to Your Website

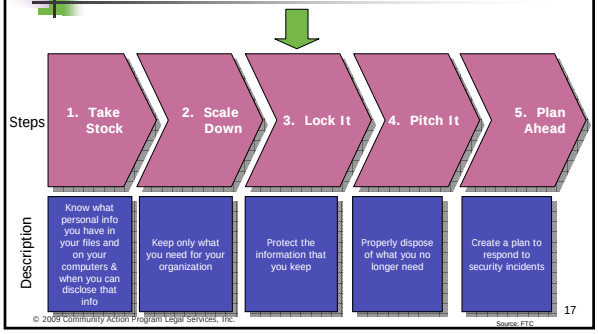
- Do not post confidential files on "nonpublic" portions of web site
- Obtain consent before transferring personal info to web site
- Do not disclose home addresses of officers and directors on forms filed with government
- Photographs of events may contain identifying info in the caption or name of the graphic file

© 2009 Community Action Program Legal Services, Inc.

Source: Privacy Rights Clearinghouse

16

The Big Picture

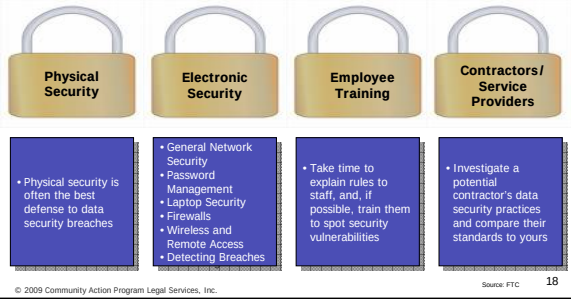


© 2009 Community Action Program Legal Services, Inc.

Source: FTC

17

Step 3: Lock It



© 2009 Community Action Program Legal Services, Inc.

Source: FTC

18

Step 3: Physical Security

- Store any documents (paper or electronic) containing personally identifiable info in a locked room/file cabinet
- Require employees to store files, log off computers and lock file cabinets/office doors on daily basis
- Implement appropriate access controls for building

© 2009 Community Action Program Legal Services, Inc.

Source: FTC

Step 3: Electronic Security

- General Network Security
  - Don't store sensitive consumer data on any computer with an Internet connection
  - Encrypt sensitive info sent to third parties over public networks (e.g. Internet)
  - Regularly update anti-virus/anti-spyware programs
- Password Management
  - Require employees to use "strong" passwords

© 2009 Community Action Program Legal Services, Inc.

Source: FTC

Step 3: Electronic Security

- Laptop Security
  - Restrict use of laptops
  - Assess if sensitive info required to be stored on laptop
  - Require employees to store laptops in secure places
  - Avoid data storage on hard drive
    - Use password entry if store data on hard drive
- Firewalls
  - Use firewall to protect against hacker attacks
  - Consider additional firewalls to protect computers with sensitive information

© 2009 Community Action Program Legal Services, Inc.

Source: FTC

Step 3: Electronic Security

- Wireless and Remote Access
  - Limit access to internal network via wireless connection
  - Encrypt info
    - Makes reading info difficult
    - Adds extra protection to internal network if remotely accessed by employees or service providers
- Breach Detection
  - Use an intrusion detection system
  - Maintain central log files of security-related info to monitor activity on network

Source: FTC

© 2009 Community Action Program Legal Services, Inc.

Step 3: Data Breach Guidance

- Investigate disclosure
- Determine if required to notify law enforcement
  - Report situation and potential risk for identity theft
  - If local police not familiar with investigating information compromises contact local FBI service
- Notify affected individuals
  - Clearly describe breach
  - Explain what responses are appropriate for info taken
  - Include current info about identity theft
  - Provide contact info for law enforcement officer

© 2009 Community Action Program Legal Services, Inc.

Step 3: Employee Training

- Check references or do background checks before hire new employees
  - Especially if employee to access sensitive data
- Ask every new employee to sign confidentiality and security standards agreement
- Know which employees have access to clients' sensitive personally identifying information
- Implement procedures preventing employees that no longer work for org or transfer to another part of org from accessing sensitive information

Source: FTC

© 2009 Community Action Program Legal Services, Inc.

Step 3: Background Checks

Definition

"any written, oral, or other communication of information obtained from a consumer reporting company that is used to evaluate a person's eligibility for credit, insurance, *employment*, or other reasons"[1]

Covered

1. credit reports
2. employment background reports
3. landlord-tenant histories
4. medical histories
5. criminal background checks if purchased from an outside agency that is in the business of providing criminal background checks

Potentially Covered

1. drug tests if an intermediary provides you with the results

Not Covered

1. drug tests provided directly by the lab to you
2. criminal background checks received from state agencies that provide information that is generally available to the public

© 2009 Community Action Program Legal Services, Inc.

Step 3: Sampling of FCRA Obligations

You Must Have a "Permissible Purpose" To Obtain A Consumer Report

Hiring decisions where the job applicant has given you *written permission* to obtain a consumer report qualifies

You Must Notify The Job Applicant if an Adverse Action is Taken

Your organization must notify a job applicant if you deny him/her employment based at least, in part, on information obtained from a credit reporting agency

The Notification Must Include...

- Name, address, and telephone of CRA reporter
- Statements that:
  - CRA not make adverse decision and unable to explain why decision made
  - Consumer has right to obtain free disclosure of file upon request made within 60 days
  - Of consumer's right to dispute accuracy or completeness of CRA provided information

Source: FTC

© 2009 Community Action Program Legal Services, Inc.

26

Step 3: Do Employees Know When Disclosure is Allowed?

- Need written authorization from client or employee for disclosure
- Exceptions to written authorization:
  - Specific law or court order
    - Some laws require notification and chance to object/seek protective order
  - Imminent danger to the individual

© 2009 Community Action Program Legal Services, Inc.

27

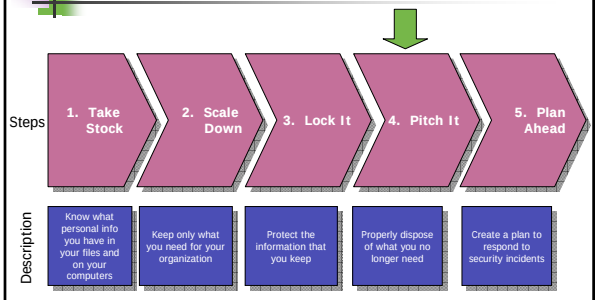
Step 3: Contractors/Service Providers

- Before outsource any business functions, investigate service provider's data security practices
- Address data security issues in service provider contract
- Insist that service providers notify org of any security incidents

Source: FTC

© 2009 Community Action Program Legal Services, Inc.

The Big Picture



Source: FTC

© 2009 Community Action Program Legal Services, Inc.

Step 4: Pitch It (The Disposal Rule)

- "Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."
  - Governs only disposal practices
  - Does not provide guidance as to when documents should be retained or destroyed
  - 16 C.F.R. § 682

© 2009 Community Action Program Legal Services, Inc.

Step 4: How to Properly Dispose of Info

- Post-disposal, info cannot be practicably read or reconstructed
- "Reasonable Measures" of Disposal
  1. Burn/Pulverize/Shred papers
  2. Destroy/erase electronic info
  3. Exercise due diligence in hiring an outside contractor to provide disposal services

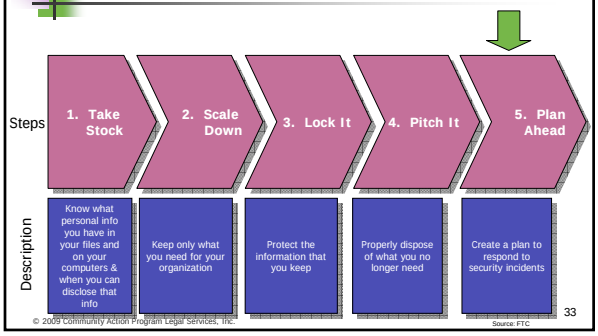
© 2009 Community Action Program Legal Services, Inc.

Step 4: Important tips

- Disposal Rule applies:
  - To any large or small organization
  - Even if consumer report info is incorporated into new document
  - Even if not know that info was derived from a consumer report
- Safest practice: Disposal Rule measures be taken for disposal of any personal or financial information

© 2009 Community Action Program Legal Services, Inc.

The Big Picture



© 2009 Community Action Program Legal Services, Inc.

Step 5: Plan Ahead

- Don't assume that client or employee info may be legally disclosed because a funding source asks for it
- Don't assume that disclosure of personal info in response to a subpoena, without the consent or notification of the subject, is necessarily legal
- Establish point person to address disclosure requests and subpoenas (e.g. in-house attorney)
- Make sure you know who has legal rights to access information on children

© 2009 Community Action Program Legal Services, Inc.

Step 5: Sample Disclosure Policy

[CAA X] attempts, to the greatest extent possible, to protect the confidentiality of information I provide. However, information I provide in this form and otherwise to [CAA X] may be released to other programs within [CAA X], and/or to the government agency/ies which fund and/or audit [CAA X's] program(s) in which I participate if such information is requested or required by the agency. Release of information to other agencies/persons shall be made only upon my additional consent and/or as required or authorized by law. By signing this document, I understand and agree to this information disclosure policy.

© 2009 Community Action Program Legal Services, Inc.

Appendix of Resources

- General Resources
  - See "Protecting Personal Information: A Guide for Business" on FTC website available at http://www.ftc.gov/bcp/edu/microsites/infosecurity/
  - Sample Privacy and Confidentiality Policies available at http://www.nigca.org/planning_toolkit/index.html#five
  - See Privacy Rights Clearinghouse available at http://www.privacyrights.org

© 2009 Community Action Program Legal Services, Inc.

Appendix of Resources

- Take Stock
  - See “Online Privacy for Nonprofits” on the *Privacy Rights Clearinghouse* webiste available at www.privacyrights.org/fs/fs28-nonprofits.htm
  - See "Nonprofit Organizations and Privacy: Responsible Mailing List Management" on the *Privacy Rights Clearinghouse* available at www.privacyrights.org/ar/listman.htm

© 2009 Community Action Program Legal Services, Inc.

Appendix of Resources

- Lock It
  - See “Information Compromise and The Risk of Identity Theft” on FTC website available at http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html
  - See “Notice to Users of Consumer Reports: Obligations of Users Under the FCRA” on FTC website available at http://www.ftc.gov/os/2004/11/041119factaapph.pdf

© 2009 Community Action Program Legal Services, Inc.

Appendix of Resources

- Pitch It (Disposal)
  - See additional info on “Consumer Reports” on FTC website available at www.ftc.gov/os/statutes/fcra
  - The text of the Rule can be obtained on the FTC website or in the Code of Federal Regulations, Title 16, Part 682, available at http://www.gpoaccess.gov/cfr

© 2009 Community Action Program Legal Services, Inc.

HIPAA Basics

© 2009 Community Action Program Legal Services, Inc.

What Is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
  - Health insurance portability and fraud/abuse
  - Health care industry "simplification" – applies to covered entities
    - National standards for electronic health care transactions
    - Privacy protections for individual health info ("protected health info" or PHI)
    - Security standards for electronically stored or transmitted PHI (EPHI)

© 2009 Community Action Program Legal Services, Inc.

How Is the HIPAA Privacy Rule Likely to Affect CAAs?

- As sponsors of group health plans for employees
- As providers of health care to clients
- As recipients of employees' and clients' health information from "covered entities" (CEs)
- As "business associates" of CEs

© 2009 Community Action Program Legal Services, Inc.

Who Are Covered Entities?

- Health plans, e.g.:
  - Employer-sponsored group health plans
  - HMOs/insurers
  - Government-sponsored health plans (e.g., Medicare, Medicaid, state children's health insurance plans)
- Health care providers who electronically transmit health info in connection with specified transactions with health plans
- Health care clearinghouses

© 2009 Community Action Program Legal Services, Inc.

Hybrid Entity Designation

- If its activities include both covered and non-covered functions, an organization can designate itself a "hybrid entity"
- Limits application of privacy rule to only those programs that perform covered functions

© 2009 Community Action Program Legal Services, Inc.

What Is the HIPAA Privacy Rule?

- CEs can't use or disclose someone's PHI, except:
  - To that person;
  - In connection with treatment, payment or health care operations;
  - With person's written consent (called an "authorization"); or
  - Without consent, only where required or permitted by Privacy Rule

© 2009 Community Action Program Legal Services, Inc.

What Is the HIPAA Privacy Rule?

- In general, CEs must use/disclose only "minimum necessary" PHI to accomplish intended purpose of use/disclosure
- Privacy rule sets federal "floor" of health privacy protections

© 2009 Community Action Program Legal Services, Inc.

What Is Protected Health Information (PHI)?

- Info (in **any** form) that
  - Is created or received by health care provider, health plan, health care clearinghouse or employer;
  - Relates to:
    - A person's present, or future physical or mental health or condition;
    - Provision of health care to a person; or
    - Past, present, or future payment for the provision of health care to a person
  - Either identifies or could be used to identify the person; and
  - Is transmitted or maintained in **any** form

© 2009 Community Action Program Legal Services, Inc.

What Is Protected Health Information?

- Includes non-medical demographic info (name, address, zip code, birth date, SSN etc.) that can be linked to a person's health care data
- **Excludes** employment records held by CE it is role as an employer

© 2009 Community Action Program Legal Services, Inc.

What Covered Entities Must Do to Comply

© 2009 Community Action Program Legal Services, Inc.

Compliance Requirements

- Notice of privacy practices
- Privacy policies and procedures
- Privacy official
- Safeguard PHI

© 2009 Community Action Program Legal Services, Inc.

Compliance Requirements

- Workforce training and sanctions
  - Workforce = employees, volunteers, trainees and anyone else (paid or unpaid) whose work performance is under CE's direct control
  - Must document that training has been provided
    - Be sure to document what materials were used

© 2009 Community Action Program Legal Services, Inc.

Compliance Requirements

- Business associates
  - Identify business associates and enter into business associate agreements with them
  - American Recovery and Reinvestment Act of 2009 (ARRA) adds new requirements for business associates

© 2009 Community Action Program Legal Services, Inc.

Compliance Requirements

- Mitigation
- Complaint procedures
- No waiver or retaliation
- Documentation and recordkeeping

© 2009 Community Action Program Legal Services, Inc.

Compliance Requirements

- Give individuals the following rights re: their PHI:
  - Authorization
  - Confidentiality
  - Use/Disclosure Restrictions
  - Access
  - Amendment
  - Accounting

© 2009 Community Action Program Legal Services, Inc.

Compliance Requirements

- Comply with HIPAA Security Rule by:
  - Ensuring confidentiality, integrity, and availability of all EPHI that CE creates, receives, maintains, or transmits;
  - Protecting against any reasonably anticipated threats or hazards to the security or integrity of this info;
  - Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required by Privacy Rule; and
  - Ensuring workforce compliance with Security Rule.

© 2009 Community Action Program Legal Services, Inc.
55

Security Rule

- Security Rule includes detailed requirements on:
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Business associate contracts
  - Plan documents of certain group health plans
  - Policies and procedures and documentation
- For further info on Security Rule see http://www.cms.hhs.gov/SecurityStandard/

© 2009 Community Action Program Legal Services, Inc.
56

Compliance Requirements

- Provide notification of breaches of "unsecured" PHI
  - Notify each individual whose PHI was released in breach – in some cases, must provide notice on CE's website or in major print or broadcast media
  - Notice to prominent media outlets if PHI of 500 or more people released
  - Notice to HHS
  - Requirements re: timing and content of notice
- Breach notification requirement becomes effective later this year (after HHS issues guidance required by ARRA)

© 2009 Community Action Program Legal Services, Inc.
57

Enforcement and Penalties

© 2009 Community Action Program Legal Services, Inc.

Enforcement: Civil Violations

- HHS's Office for Civil Rights (OCR)
  - OCR investigates and can seek civil monetary penalties
  - Anyone may file complaint with OCR – but no individual right to sue
  - ARRA (HITECH Act) increased penalties and strengthened enforcement provisions
- State attorneys general can now sue to stop violations and seek civil money damages

© 2009 Community Action Program Legal Services, Inc.

Penalties: Civil Violations

- Penalties can be severe:
  - Even where CE didn't know of a violation, penalties can range from $100 for each violation to $1.5 million per year for all violations of the same requirement

© 2009 Community Action Program Legal Services, Inc.

Enforcement and Penalties: Criminal Violations

- Criminal fines and jail time for intentional violations
- U.S. Dep't of Justice investigates and prosecutes criminal violations

© 2009 Community Action Program Legal Services, Inc.

Is Your CAA's Group Health Plan a Covered Entity?

© 2009 Community Action Program Legal Services, Inc.

Plan vs. CAA

- CAA's group health plan (not CAA itself) is CE
  - Plan document should identify:
    - Who from CAA can act on behalf of plan
    - What powers they have to do so
- CAA's group health plan is different from HMO/insurer with whom it contracts to provide benefits
  - HMO/insurer itself is also a CE

© 2009 Community Action Program Legal Services, Inc.

Covered Entity Analysis: Group Health Plans

- Most employer-sponsored group health plans are CEs; only exceptions are plans that are:
  - Administered by employer (not third party) and
  - Have fewer than 50 participants (i.e., people eligible to participate)

© 2009 Community Action Program Legal Services, Inc.

Determining Plan's Obligations under Privacy Rule

- Health plan's obligations under Privacy Rule depend on:
  - Whether plan is fully insured; and
  - What kind of PHI (if any) employer receives from plan

© 2009 Community Action Program Legal Services, Inc.

Exception for Certain Fully Insured Plans

- Fewer requirements where CAAs who sponsor fully insured plans receive no PHI or only:
  - Enrollment and participation info and/or
  - Summary health info so CAA can:
    - Obtain bids for group health care coverage or
    - Change or terminate plan

© 2009 Community Action Program Legal Services, Inc.

Exception for Certain Fully Insured Plans

- If employer receives only this level of PHI, plan does **not** need to:
  - Maintain or distribute notice of privacy practices (but HMO/insurer should) or
  - Meet most other Privacy Rule compliance requirements
- Plan **only** needs to:
  - Refrain from intimidating or retaliatory acts relating to Privacy Rule; and
  - Not require individuals to waive their rights under Privacy Rule

© 2009 Community Action Program Legal Services, Inc.
67

Fully Insured vs. Self-Insured Plans

- Fully insured plan: employer pays premiums to HMO/insurer, which then assumes the financial risk of paying for participants' health care claims

© 2009 Community Action Program Legal Services, Inc.
68

Fully Insured vs. Self-Insured Plans

- Self-insured plan: employer assumes the financial risk for paying for participants' health care claims
  - Partially self-insured plan: employer pays premiums to HMO for up to a certain amount of claims coverage and pays rest of claims itself
  - For self-insured and partially insured plans, HMO/insurer often acts as third-party administrator (TPA) in enrolling participants and processing claims

© 2009 Community Action Program Legal Services, Inc.
69

Employer Access to PHI from Plan for Plan Administration

- In order for employer to receive additional PHI for plan administration functions, **employer** must:
  - Amend plan document to:
    - Permit PHI disclosure to employer and
    - Restrict uses/disclosures of PHI by employer
  - Certify to plan and to HMO/insurer that plan document has been amended and that employer will take certain required steps (outlined in amendment) to protect PHI

© 2009 Community Action Program Legal Services, Inc.

Employer Access to PHI from Plan for Plan Administration

- Where employer receives additional PHI for plan administration functions, **plan** must:
  - Create/maintain notice of privacy practices ("NPP")
    - If fully insured: must provide NPP to any person who requests it (don't need to distribute it otherwise)
    - If self-insured: must distribute NPP to plan participants
      - By compliance deadline,
      - To new participants when they enroll, and
      - To all participants within 60 days of a material change
  - Both fully insured and self-insured plans must meet all other compliance requirements

© 2009 Community Action Program Legal Services, Inc.

Employer Access to PHI from Plan for Other Purposes

- For employer to access plan participants' PHI for purposes other than plan administration, it should have participants sign an authorization form
  - For example, if employer wants to help participants resolve health care claims or for employment-related purposes

© 2009 Community Action Program Legal Services, Inc.

Health Plan Action Items

- If fully insured, contact your HMO/insurer(s) to discuss level of PHI your CAA receives and compliance roles and responsibilities

© 2009 Community Action Program Legal Services, Inc.

Health Plan Action Items

- If desired, establish procedures to ensure your CAA receives no PHI or only enrollment and participation data and summary health info (and uses it only for proper purposes)
- If CAA wants access to more than this level of PHI, CAA should:
  - Amend plan documents
  - Sign certification and give to plan and HMO/insurer
  - Take steps required by amendment – e.g., provide for adequate separation (firewalls) between plan and CAA, don't use PHI for employment-related purposes etc.

© 2009 Community Action Program Legal Services, Inc.

Health Plan Action Items

- Coordinate with vendors (brokers, TPAs) re: compliance roles and responsibilities
  - Determine which vendors, if any, are business associates and enter into business associate agreements with them
  - Review contracts with others to see if any HIPAA-related provisions are needed

© 2009 Community Action Program Legal Services, Inc.

Health Plan Action Items

- If meet exception for fully insured plans, establish procedures for complying with "no retaliation" and "no waiver" requirements
- If don't meet that exception, become compliant with Privacy Rule requirements
  - Notice of privacy practices, privacy official, privacy policies and procedures, safeguarding PHI, workforce training and sanctions etc.

© 2009 Community Action Program Legal Services, Inc.

Health Plan Action Items

- Establish procedures for your CAA to handle claims advocacy on behalf of plan participants
  - Authorization form – have participants sign before helping them with claims
  - Set policies re: requests from family members for information

© 2009 Community Action Program Legal Services, Inc.

Is Your CAA a Covered Entity?

© 2009 Community Action Program Legal Services, Inc.

Covered Entity Analysis: CAAs as Health Care Providers

- Does CAA furnish, bill or get paid for health care in the normal course of business?
  - "Health care" broadly defined

© 2009 Community Action Program Legal Services, Inc.
79

Covered Entity Analysis: CAAs as Health Care Providers

- If so, does CAA transmit health information in electronic form in connection with the specified transactions with health plans?
  - Electronic form doesn't include paper, phone or dedicated fax (does include emails, flash drives, CDs, faxing from computer)

© 2009 Community Action Program Legal Services, Inc.
80

Specified Transactions with Health Plans

- Health care claims or "equivalent encounter" info
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status inquiries/responses
- Health plan enrollment and disenrollment
- Health plan eligibility
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Claims attachments

© 2009 Community Action Program Legal Services, Inc.
81

Definition of "Health Plan"

- Includes employer-sponsored group health plans
- Includes government-funded health plans, such as Medicaid, Medicare, state children's health insurance programs

© 2009 Community Action Program Legal Services, Inc.

Definition of "Health Plan"

- Does **not** include certain government-funded programs:
  - **Programs whose main purpose is not providing / paying cost of health care**
    - For example: WIC, Food Stamp program
  - Programs whose principal activity is:
    - Directly providing health care or
    - Making grants to fund the direct provision of health care

© 2009 Community Action Program Legal Services, Inc.

Other Ways the Privacy Rule Can Affect Your CAA

© 2009 Community Action Program Legal Services, Inc.

Health Information Needed for CAA Programs

- Providers will require authorization in order to release info directly to CAA
  - Give clients authorization form to fill out and take to providers

© 2009 Community Action Program Legal Services, Inc.

Health Information for Employment-Related Purposes

- ADA, FMLA, paid medical leave, return to work and modified duty, OSHA, pre-employment physicals, substance abuse testing
  - Health care providers will require authorization in order to release info directly to CAA
  - Give employees authorization form to sign and take to providers
  - After info received by CAA, no longer protected by HIPAA

© 2009 Community Action Program Legal Services, Inc.

Health Information for Employment-Related Purposes

- Workers' Compensation
  - No authorization required for disclosures authorized by and to the extent necessary to comply with workers' compensation laws

© 2009 Community Action Program Legal Services, Inc.

Health Information for Employment-Related Purposes

- **Remember:** Employees' health information that employer holds in its role as employer (rather than as sponsor of health plan) is **not** protected by HIPAA
  - But when health plan holds the health info, it is protected

© 2009 Community Action Program Legal Services, Inc.

Business Associate Agreements

- CEs may require CAA to sign business associate agreements

© 2009 Community Action Program Legal Services, Inc.

Relationships with Business Associates

© 2009 Community Action Program Legal Services, Inc.

Who Are Business Associates?

- Contractors or other non-workforce members doing work for CE where work involves use/disclosure of PHI
- A CE can be a business associate of another CE

© 2009 Community Action Program Legal Services, Inc.

Who Are Not Business Associates?

- People/organizations for whom access to PHI is **not** necessary to do their job
- Members of CE's workforce
- Providers to whom CE discloses PHI for treatment purposes

© 2009 Community Action Program Legal Services, Inc.

Business Associates: What CEs Must Do

- Sign written agreements with business associates (must include certain provisions)
  - Be sure to work with an attorney
- If CE knows BA breached agreement, CE must take steps to fix breach and, if unsuccessful either:
  - Terminate agreement or
  - If termination not feasible, notify HHS
- CE **not** required to monitor business associate

© 2009 Community Action Program Legal Services, Inc.

Business Associates: New Requirements

- ARRA changes to BA requirements (effective Feb. 17, 2010):
  - Most provisions of Security Rule that apply to CEs will also apply to BAs
  - Privacy requirements that must be included in BA agreements will apply to BAs by law as well as by contract

© 2009 Community Action Program Legal Services, Inc.

Business Associates: New Requirements

- ARRA provisions re: privacy and security that apply to CEs will also apply to BAs and must be incorporated into BA agreements
- BAs will be required to cure CE breaches of BA agreements in the same way CEs must act to cure BA breaches
- Same civil and criminal penalties that apply to CEs will also apply to BAs
- BA agreements will need to be amended to incorporate these changes

© 2009 Community Action Program Legal Services, Inc.

Some Issues That May Require Negotiation

- Whether person/entity being asked to sign really is a business associate
- Indemnification provisions
- Who decides whether business associate must return PHI to CE or destroy it at end of contract

© 2009 Community Action Program Legal Services, Inc.

Authorizations

© 2009 Community Action Program Legal Services, Inc.

Authorizations

- Must be written in plain language and include certain info and statements required by the Privacy Rule:
  - Description of PHI to used/disclosed
  - Name/other specific ID of people/class of people authorized to release the PHI
  - Name/other specific ID of people/class of people to whom the PHI may be released
  - Purpose(s) for which PHI can be used/disclosed
  - Expiration date or expiration event

© 2009 Community Action Program Legal Services, Inc.

Authorizations

- Required info/statements (continued):
  - Statements about:
    - Individual's right to revoke the authorization;
    - CE's ability/inability to condition treatment, payment, enrollment or eligibility for benefits on whether person signs; and
    - Potential for info disclosed to be re-disclosed by the recipient and no longer protected by Privacy Rule
- Must be signed and dated
- Copy must be provided to individual

© 2009 Community Action Program Legal Services, Inc.

Authorizations

- Not required for certain uses/disclosures, for example:
  - For law enforcement purposes
  - In court proceedings
  - Re: victims of abuse, neglect, domestic violence
  - For workers' compensation purposes
  - "Incidental" uses/disclosures

© 2009 Community Action Program Legal Services, Inc.

Authorizations

- Rules about when authorizations can be combined, including:
  - Rule that authorization re: psychotherapy notes may only be combined with another authorization for re: psychotherapy notes
- In most cases, CE can't condition provision of treatment, payment, enrollment in health plan or eligibility for benefits on whether person signs authorization

© 2009 Community Action Program Legal Services, Inc.

CAPLAW Conference

Save the dates for

CAPLAW's
2010 National Training Conference

June 16-18, 2010
Savannah, Georgia

© 2009 Community Action Program Legal Services, Inc.

SMITH ANDERSON

Client Alert

March 2009

HITECH Act Expands Scope and Enforcement of HIPAA

Signed into law on February 17, 2009, the American Recovery and Reinvestment Act of 2009 (the "ARRA") includes the most expansive changes to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") since the issuance of the final privacy and security regulations in 2002 and 2003, respectively. Specifically, Title XIII, Subtitle D of the ARRA, known as the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act" or the "Act"), contains provisions that significantly expand the scope and force of the privacy and security regulations under HIPAA. These changes are part of the Obama administration's goal to facilitate the electronic exchange of health information between all healthcare providers.

With these changes, a wide range of businesses may find it necessary to revisit their HIPAA compliance efforts. Many of the Act's provisions are set to become effective February 17, 2010; however, certain provisions may become effective as early as six months from the date of enactment, and certain enforcement and penalty provisions became effective *upon the date of enactment* of the Act. The changes under the Act affect covered entities and their business associates (business associates commonly include technology vendors and consultants that access protected health information while providing services to covered entities), as well as vendors of personal health records. Notably, the Act makes several of the HIPAA privacy and security regulations directly applicable to business associates, subjecting them to the same civil and criminal penalties as covered entities. The Act also includes breach notification provisions, places limits on the sale of protected health information, and expands the enforcement mechanisms and penalties for violations of HIPAA. Some of the more significant provisions of the Act are set forth below.

EXPANSION OF THE HIPAA PRIVACY RULE AND THE HIPAA SECURITY RULE

Currently, only covered entities, and not business associates, are directly subject to the requirements of HIPAA. HIPAA applies to business associates indirectly, by way of the business associate's contractual obligations to the covered entity. The Act changes this by making certain provisions of the HIPAA Privacy Rule and the full spectrum of requirements under the HIPAA Security Rule directly applicable to business associates. Some of these changes are described below.

HIPAA Privacy Rule

The HIPAA Privacy Rule requires covered entities to enter into business associate agreements with their business associates and enumerates required provisions related to the use and disclosure of protected health information ("PHI"). The business associate's compliance with the terms of a business associate agreement, however, is governed by the agreement, and not directly by HIPAA.

The Act changes this by making a business associate's compliance with the terms of a business associate agreement a direct requirement of HIPAA. Specifically, the Act states that when a business associate obtains or creates PHI pursuant to a business associate agreement, it may use and disclose such PHI only if it complies with

each requirement of 45 C.F.R. § 164.504(e) (the HIPAA provision that outlines the requirements for a valid business associate agreement).

The Act also increases the oversight role that business associates have over covered entities with whom they contract. Specifically, the Act requires business associates to: (a) take reasonable steps to cure a breach of a business associate agreement, or (b) terminate the agreement if it knows of a pattern of activity or practice by a covered entity that violates the agreement. If terminating the agreement is not feasible, the business associate may be required to report the covered entity to the Secretary of the Department of Health and Human Services (the "Secretary").

HIPAA Security Rule

Currently, with respect to the HIPAA Security Rule, business associates must contractually agree to use "appropriate safeguards" to prevent the unauthorized use or disclosure of PHI accessed on behalf of a covered entity. This represents only a limited portion of the HIPAA Security Rule requirements. The Act, however, subjects business associates to the full HIPAA Security Rule. Business associates will be required to implement the administrative, physical, and technical safeguards, as well as the organizational requirements, policies, procedures, and documentation requirements of the HIPAA Security Rule.

What Do These Changes Mean?

Business associates will be required to enter into modified business associate agreements to address these changes. Perhaps even more significant, however, is the need for business associates to establish and broaden existing privacy and security policies and procedures to address these new requirements.

Examples of such measures include implementing security awareness and training programs for workforce members, creating and implementing policies and procedures governing the use and protection of PHI, designating appropriate privacy and security officials, and conducting periodic privacy risk assessments.

Non-compliance with these changes may constitute a *direct violation* of HIPAA, leaving business associates open to potential contractual liability as well as HIPAA enforcement actions and resulting civil and criminal penalties. The Act sets these provisions to become effective February 17, 2010. The scope of these changes, however, means that affected parties should begin to revisit privacy compliance efforts now.

NEW DATA BREACH NOTIFICATION PROVISIONS

Currently, under HIPAA, a covered entity does not have an affirmative obligation to notify an individual of a data breach involving the unauthorized disclosure of PHI about the individual. A covered entity is obligated merely to track such disclosures and provide an accounting of those disclosures in response to the individual's request. Business associates, on the other hand, are required only to report such disclosures to the covered entity. Where there has been a specified breach of "unsecured" PHI, the Act provides new notification provisions applicable to covered entities, vendors of personal health records, and related entities, and more rigorous reporting requirements applicable to business associates.

Covered entities will be required to notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of a breach that is discovered by the covered entity. This provision applies to a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI. Specified forms of notification, including certain content described under the Act, must be made to the individual without unreasonable delay, but in no event later than 60 calendar days after discovery of the breach.

Business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI must notify the covered entity of a data breach discovered by the business associate. The notice must include, among other things, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed as a result of the breach.

The Act also requires vendors of personal health records, regardless of whether they qualify as covered entities or business associates, to notify the Federal Trade Commission and each affected individual of any such data breaches.

The Secretary is required to issue regulations implementing these breach notification provisions within 180 days of the date of enactment (by August 16, 2009), and such provisions will apply to data breaches discovered 30 or more days from the publication of such regulations.

LIMITATIONS ON SALE OF PHI

The Act includes restrictions limiting the sale of PHI by covered entities and business associates. Absent a specific exception, the Act generally prohibits covered entities and business associates from receiving remuneration in exchange for PHI *unless* the covered entity obtains a HIPAA-compliant authorization from the individual. The authorization must also expressly state whether the PHI may be further exchanged for remuneration by the entity receiving the PHI.

The Act sets out six specific exceptions where this restriction will not apply. The restriction will not apply in cases where the purpose of the exchange is:

- For public health activities;
- For research activities where the price charged reflects the cost of preparation and transmittal of the data;
- For treatment of the individual;
- For the specific health care operation involving the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that, following such activity, will become a covered entity, and due diligence related to such activity;
- For remuneration that is provided by a covered entity to a business associate for activities involving the exchange of PHI; and
- To provide an individual with a copy of the individual's PHI.

The Secretary is required to issue regulations to carry out this provision no later than 18 months after enactment (by August 17, 2010). The limitations on the sale of PHI will apply to exchanges of PHI beginning six months after such regulations are implemented.

EXPANDED ENFORCEMENT RIGHTS

Effective *upon enactment* of the Act, state attorneys general were authorized to bring civil actions against individuals who violate HIPAA. An attorney general bringing a civil action under HIPAA must give the Department of Health and Human Services the opportunity to intervene in the action. The Act also requires the Secretary to formally investigate complaints where a preliminary investigation indicates a potential violation of HIPAA due to willful neglect, but this change is not set to take effect until February 17, 2011.

GREATER PENALTIES FOR HIPAA VIOLATIONS

Effective *upon enactment* of the Act, the civil penalties for HIPAA violations were increased. The Act provides tiered increases in the amounts of such penalties, as follows:

- If the person did not know of the violation, a penalty of at least $100 per violation, not to exceed $50,000 for each violation.
- If the violation was due to reasonable cause and not to willful neglect, a penalty of at least $1,000 per violation, not to exceed $50,000 for each violation.
- If the violation was due to willful neglect, a penalty of at least $10,000 per violation, not to exceed $50,000 for each violation; provided, however, that if the violation is not corrected, the penalty shall be no less than $50,000 per violation.

OTHER NOTABLE CHANGES

In addition, the Act contains new limitations on marketing activities involving PHI by covered entities and business associates and expands certain rights of individuals to receive an accounting of disclosures from a covered entity and to limit disclosures of PHI about the individual.

Affected parties will need to monitor issuance of applicable regulations and any guidance that clarifies or changes these new provisions in order to address them appropriately within their organizations. If you have questions about these or other privacy matters, please contact one of the Smith Anderson lawyers listed below or the Smith Anderson lawyer with whom you work.

Bo Bobbitt
919.821.6612
bbobbitt@smithlaw.com

Alicia Gilleskie
919.821.6741
agilleskie@smithlaw.com

Frederick Zufelt
919.821.6727
fzufelt@smithlaw.com

SMITH, ANDERSON, BLOUNT, DORSETT, MITCHELL & JERNIGAN, L.L.P.

Offices:
2500 Wachovia Capitol Center
Raleigh, North Carolina 27601
Mailing Address:
Post Office Box 2611
Raleigh, North Carolina 27602
Telephone: 919-821-1220
Facsimile: 919-821-6800
Email: Info@smithlaw.com

Reproduction in whole or in part is permitted when credit is given to Smith Anderson.
Copyright © 2009 by Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

Smith Anderson publishes *Alerts* periodically as a service to clients and friends. The purpose of this *Alert* is to provide general information about significant legal developments. Readers should be aware that the facts may vary from one situation to another, so the conclusions stated herein may not be applicable to the reader's particular circumstances.