Information Privacy and Security



IMLA Mid-Year Meeting of State League Counsel

GEORGIA MUNICIPAL ASSOCIATION

© Georgia Municipal Association, Inc. 2016. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2016 Mid Year Seminar, held April 15-18, 2016 in Washington, DC. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

What could happen if . . .

- Sensitive, personal information disclosed/breached AND City or League
  - Had not properly protected the information
  - Had no policies or procedures for protecting the information
  - Had policies or procedures for protecting the information but did not consistently follow or enforce them

What could happen if . . .

- Bad press
- Loss of trust
- Disruption of business
- Legal fees
- Costs of internal and external investigations
- Employment lawsuits
- Misuse of incident for political gain
- Oversight by outside parties
- Removal of leadership
- Invasion of privacy lawsuits
- Open records requests
- Cost of breach response

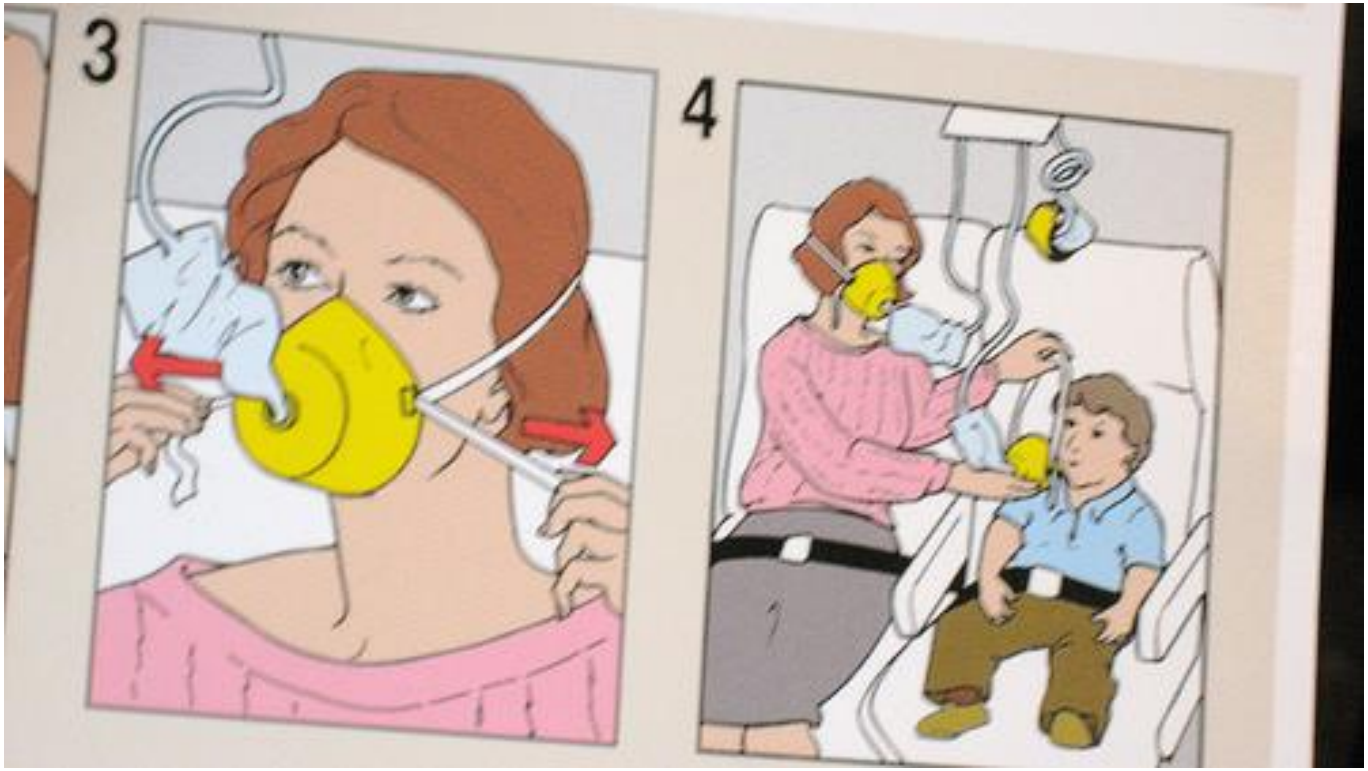
What could happen if . . .

- In addition, if city or league has or might have a HIPAA healthcare component:
  - Penalties imposed by Department of Health and Human Services Office for Civil Rights
  - Ongoing monitoring by HHS
- In addition, if city or league accepts credit and other payment cards:
  - Increased compliance obligations in order to keep taking the cards
  - Liability for fraudulent transactions (card present)
  - Worst case – loss of ability to accept the cards

What could happen if . . .

- In addition, if city or league has or might have a HIPAA healthcare component:
  - Penalties imposed by Department of Health and Human Services Office for Civil Rights
  - Ongoing monitoring by HHS
- In addition, if city or league accepts credit and other payment cards:
  - Increased compliance obligations in order to keep taking the cards
  - Liability for fraudulent transactions (card present)
  - Worst case – loss of ability to accept the cards

League compliance comes first



GMA invested time and resources in its own compliance before educating city clerks and elected officials about compliance.

Actions for Breach Prevention and Response

- Information inventory + risks, applicable laws and requirements
- HIPAA status review (identifying HIPAA covered entities and business associates)
- Policies and procedures: training, enforcement
- Contracts: business associate agreements, subcontractor business associate agreements, information privacy and security provisions whenever vendor accesses/maintains/uses confidential information
- Incident reporting and response
- Breach response

Getting Buy In from Leadership

- Executive Director named GMA Information Security Officer, General Counsel named GMA Information Privacy Officer
- Deputy Executive Director for Risk Management and Employee Benefits (Retirement Plan, Health, Dental, Life Plans) named Information Privacy Officer for HIPAA Plans (Health and Dental)
- Information Security Team includes CFO, Director of Information Technology, Director of Public Relations, Human Resources Manager

Getting Buy in from Leadership

- Benefits of acting NOW
  - It is the right thing to do!
  - Control the process of protecting the information to limit expense and change corporate culture
  - Prevent or limit investigations by analyzing legal obligations in advance
  - Prevent breaches!
  - Manage Public Relations for any breaches that occur

Getting Buy In from Leadership

- Involve leadership in training and procedure development to make sure procedures are tailored for culture
- Draft training materials, draft procedures submitted to Information Security Team for review and discussion
- Revised HIPAA Privacy Notice, HIPAA procedures presented to Health/Dental Plan Board for approval

Getting Buy In from all Workers

- Mandatory Training, Executive Director introduced every session
  - Acknowledge change “We have grown a lot since when we started,” “Rules have changed”
  - Tie to disruptions, costs of familiar breaches “We can’t afford the interruption of a Target or a Home Depot”
  - Tie to viability of League “We must maintain the trust of our membership”
  - Ask for support “I’m going to ask you to be really committed”

Getting Buy In from all Workers

- “What would happen if GMA had a breach and investigation showed that GMA workers ignored privacy and security rules?”
- “For nearly 8o years, the Georgia Municipal Association has been a reliable resource for policymakers under the Gold Dome,” said Tom Q. Gehl, GMA’s Director of Governmental Relations, “and the many years of hard-earned confidence could be ruined in a day if GMA were to be shown as having reckless disregard for confidential information entrusted to the Association’s care.”
- (Mandatory Training for all Employees /Contract Workers)

Getting Buy In from all Workers

- Encourage awareness and reporting of incidents
- “It’s always the cover-up that gets ‘em. Nixon and Watergate, Bill Clinton and Monica Lewinsky. People are very forgiving of mistakes if you sincerely apologize. But attempting to cover up mistakes leads to people talking badly about your company longer and suspecting more wrong-doing than probably actually happened.” Amy Henderson, Director of Public Relations

Getting Buy In from all Workers

- Information Inventory process requires extra work, careful review of existing processes
- “Susan Moore and I will be sponsors of the project. You have been selected to participate because of your role or the role of employees you supervise at GMA as it relates to the use of sensitive information. Your supervisor has been made aware of your appointment to this important project team. Your input and cooperation is greatly appreciated.” (Email from senior leader)

Information Inventory

- "(1) Who…which GMA employees and outside companies have access to GMA sensitive information that must be protected; (2) What…what types of documents do we have access to, and to which programs does the information relate; (3) Why…why do we need access to the information in order to do our jobs; (4) How…how does the information get to GMA/How does it leave GMA; (5) When…when is the information shared with others. The informational flow analysis will be used to update GMA procedures for using, sharing and protecting sensitive information." (Email introducing information inventory project – sent from senior management)

Information Inventory Results

- Document why access is appropriate, eliminate unnecessary access, identify when disclosure between employees could be a breach
- Identify who is authorized to use PHI, identify needs for business associate agreements (if HIPAA PHI) or security provisions in contracts
- Tailor training, procedures



Information Inventory/RA

- What information should be protected, with access limited to those who need it?
- What laws establish protections and govern what happens if mis-used or improperly disclosed/accessed?
- Who gets it? Where does it go? How is it stored?
- How is it currently protected from improper use or disclosure?
- What is risk of improper use or disclosure?
- What changes are appropriate?

Information Inventory and Risk Assessment

- See Handout
- Should result in secure destruction of unnecessary PPHI, updates of contracts
- Will form the basis for procedures and training
- Will form the basis for access controls for electronic information
- Interviews will provide buy-in and promote awareness

Contract Provisions

- Review all contracts with vendors that access or maintain sensitive information and revise when necessary
- Business Associate agreement or subcontractor BA Agreement? PCI involved?
- Insist on encryption during transmission or while on portable device, maintenance in US or EU
- Require the vendor to protect the information, follow industry standards, and pay for costs associated with breach response.

What laws, contracts impose requirements?

- HIPAA privacy and security requirements
  - Hybrid designation of covered health care components, if any (See Handout)
  - Identify who must receive extra training, limits on use/disclosure, security requirements, disclosure requirements
  - Business Associate Agreements
- Payment Card Industry Data Security Standards
  - What systems maintain cardholder data, what type of data, access controls

HIPAA

- Identify status under HIPAA
- GMA operates many programs that involve very sensitive information, but is only regulated by HIPAA when acting as a business associate to a HIPAA covered entity – the GMEBS Health and Dental Plans
- The GMEBS Board is the plan sponsor of a HIPAA covered entity – the GMEBS Health and Dental Plans
- The Board appointed GMA Deputy Executive Director as Privacy Officer to oversee relationships with Business Associates to the Health and Dental Plans (including GMA, BlueCross BlueShield of GA, Aetna)

Payment Card Industry (PCI) Data Security Standards (DSS)

- PCI DSS are minimum requirements for protecting customers' payment card information. PCI DSS were created by the five major payment card brands.
- No law requires PCI DSS compliance.
- Contractual obligation to comply
- Extra training and procedures apply to GMA workers that handle payment card information

Information Privacy/Security Incident Response

- Create written process for information privacy or security incident reporting and response
- Train staff and vendors to report incidents to specified individual or email
- Identify an incident response team
- Line up a law firm to assist

Information Privacy/Security Incident Response

- Use the term “incident” – not “breach.” “Breach” is only used if, after review, it is determined that the incident compromised the privacy and security of the information
- HIPAA breach notification/risk of harm tools are very helpful
- www.hipaacow.org has excellent tools
- Document all actions taken to investigate and minimize harm
- Consider establishing contract with credit monitoring company so they are ready if necessary
- All contracts with vendors handling PPHI should include breach provisions and indemnification
- Legal review is necessary to determine whether notification to individuals or other entities is mandated by law or applicable contracts

Training Strategy

- Training strategy – adopt definition of Personal or Protected or Health Information and require all GMA workers to protect it and report incidents, require acknowledgment of training
- Once incident reported, GMA legal and Security Team determine response based on applicable laws and in accordance with incident response procedure
- Require GMA workers with access to HIPAA PHI and payment card info to have extra training

Excerpts from Basic Training

- This training explains basic responsibilities for:
  - Identifying Personal or Protected/Health Information (“PPHI”)
  - Protecting PPHI
  - Reporting Information Security Incidents
- It is designed for general workforce
- Additional training would be required for those with access to HIPAA Protected Health Information and credit card information

Identifying PPHI

- Workers handle information that must be protected in order for GMA and its programs to comply with laws
- Workers also handle personal information that is not subject to specific laws
- All Workers must protect “PPHI” (Personal or Protected or Health Information)



Identifying PPHI: Ask These Questions

No ↓ Does it contain banking or payment card information? → Yes, PPHI

No ↓ Does it contain an identifier commonly used in ID theft? → Yes, PPHI

No ↓ Does it link an individual to the health or dental plan? → Yes, PPHI

No ↓ Does it link an individual to medical treatment or tests? → Yes, PPHI

No ↓ Does it describe any individual's health history or risks? → Yes, PPHI

No, Not PPHI



8.Report Privacy and Security Incidents!

- All Workers must stop work to immediately report information privacy and security incidents
- Immediately = Right away & same day as discovery



8.Report Privacy and Security Incidents!

What constitutes an "INCIDENT"?

An event that the PPHI Worker believes could result in or has resulted in the ***UNAUTHORIZED****:*

- Access of PPHI
- Use or disclosure of PPHI
- Alteration of PPHI
- Loss or destruction of PPHI

8.Report Privacy and Security Incidents

- My computer says I have a virus.
- Someone else sent an email using my account.
- I lost a flash drive that contained PPHI.
- I lost my laptop.
- My laptop was stolen.
- I lost my work SmartPhone.
- A folder containing medical claims information was stolen from my car.
- I faxed an explanation of benefits form to the wrong person.
- I forwarded an email that contained an individual's question about a claim to the wrong GMA employee - someone who was not authorized to see it.
- My co-worker emailed documents to her personal email before she quit.

Incident Examples

8.Reporting Privacy and Security Incidents

- Make an immediate report to _____. **If the incident involves a suspected virus or alteration or destruction of electronic files or IT assets, email [designated email] and call [designated phone number].**
- Report must include:
  - Name and contact information of Worker reporting incident
  - Description of the PPHI involved
  - Description of the incident, date of discovery
  - Who used/accessed/disclosed PPHI in an unauthorized manner
  - Steps taken to prevent further use/access/disclosure
  - Contact information if another company was involved

Reporting Privacy and Security Incidents - Review

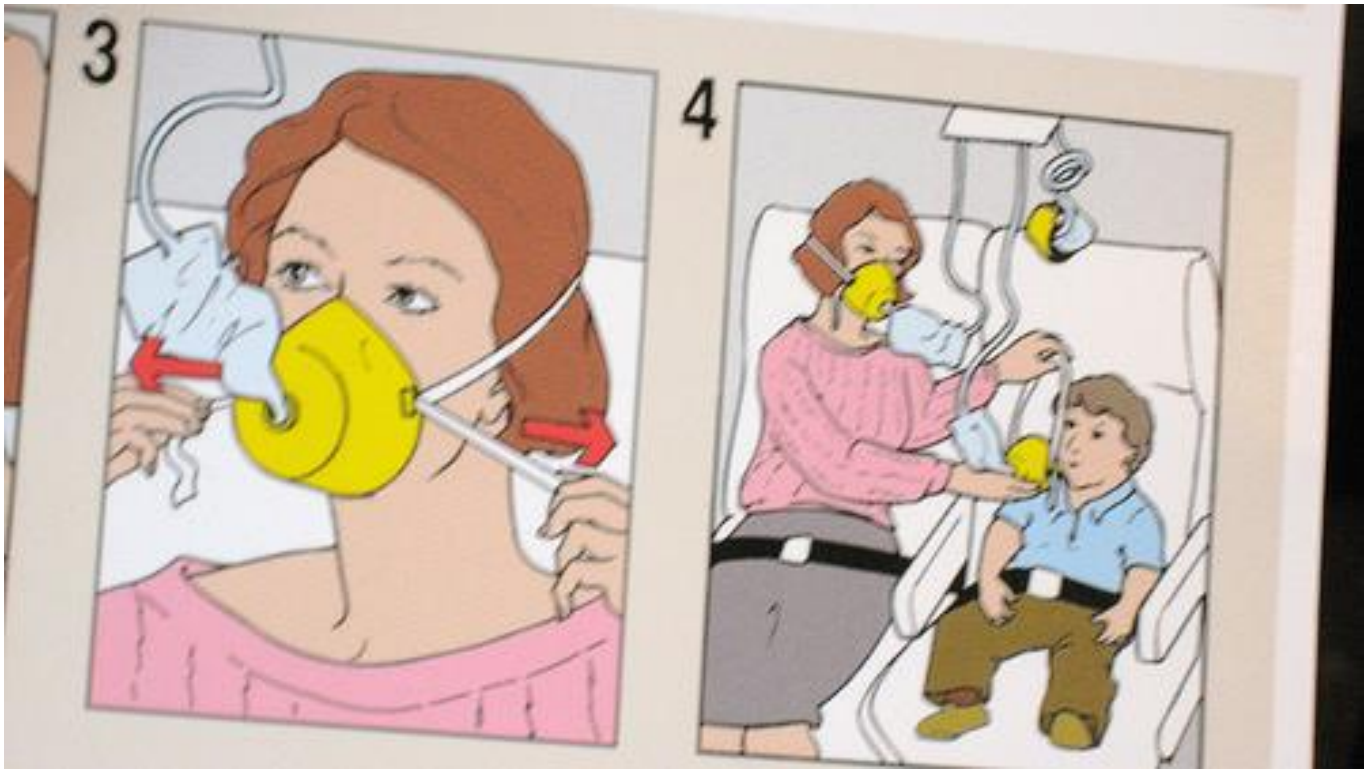
- Why is it so important to Stop Work and Report? Immediate action can . . .
  - reduce harm
  - stop harm from getting worse
  - prevent an incident from becoming a breach
  - protect GMA from penalties, bad press
- NEVER try to hide the incident or fix the problem before reporting



Questions for Leadership about Breach Prevention and Response

- Has the League completed an information inventory? Assessed risks to information? Identified laws that apply to different types of information?
- Is any part of the League a HIPAA covered entity or a HIPAA Business Associate?
- Does the League have information privacy and security policies and procedures that include incident reporting and breach response?
- How often does the League provide training? Do the League's contracts contain information privacy and security provisions?

League can help cities!



GMA now provides information privacy and security training for city clerks and elected officials.

Helping Cities

- City concerns
  - Hybrid designation for HIPAA (which parts of city are HIPAA healthcare components?)
  - Social security numbers (utility billing)
  - Copies of identification documents (drivers' licenses, passports)
  - Payment card information
- Raise awareness with case studies that show political dangers, costs of breaches + failure to protect information

Case Studies

- City of Monroeville, PA



- Skagit County, WA



City of Monroeville

- HHS determined no HIPAA breach because the dispatch center was not a HIPAA covered entity.
  - Investigation by the HHS found unauthorized access to dispatch records, outdated distribution lists
  - Investigation by outside entity found computer use policies violated, sensitive records accessed by unauthorized individuals
  - $50,000 in legal fees, Months of bad publicity http://www.wtae.com/investigations/Complaint-alleges-police-chief-received-shared-info-from-911-call/16880170
- Investigation by PA Attorney General's office
  - Found unauthorized persons viewed sensitive police information including criminal history records

City of Monroeville

- Under Council #1, Police chief Doug Cole was demoted, suspended, fired. Under Council #2, Cole was rehired (pursuant to his lawsuit).
- Under Council #1, Assistant chief Steven Pascarella, who filed the complaint, was promoted to police chief, resigned, and then rehired as a lieutenant. Under Council #2, his employment was terminated, and his lawsuit was settled in 2015.
- Council #1 demanded resignation of city manager because he refused to fire Chief Cole, appointed McKinney.
- Council #2 fired McKinney, settled her lawsuit in 2015.

Skagit County

- HHS OCR investigation found that from September 14, 2011 to September 28, 2011, Skagit disclosed electronic Protected Health Information of 1,581 individuals on its public web server, and then failed to provide required notification
  - From April, 2005 – March, 2014 Skagit failed to implement policies and procedures to detect and correct security violations and failed to train its workforce to comply with security rules
  - From April, 2005 – June, 2012, Skagit failed to maintain policies and procedures to comply with security rule
- $215,000 penalty + 3 years of oversight by HHS OCR

Questions?

Alison Cline Earles, Associate General Counsel, Georgia Municipal Association, Inc.

678-651-1028

aearles@gmanet.com

Worker with Access to PPHI	*Descriptions of documents, information systems that contain PPHI (each type of document or document set should be described in a separate row)*	*Where does it come from? How is it received? What is done with it? Why is the PPHI needed? How long is it necessary to keep*	*Where does it go? For what purpose? Who sends it? How is it transmitted?*	*Where is it stored? Hard copy? Portable Media Devices? Hard Drive of Computer? Email Server?*	*How is it protected during storage, transmission? Risk of Improper Use or Disclosure or Access (High/Medium/Low); proposed action Items to reduce risk.*
Henrietta Clerk	Utility bill applications (contain name, SSN, Address, Phone, Date of Birth, Signature, Account Number, Voided Check, Bank Routing Number and Account Number)			Hard copy saved in desk file. Hard copies for prior years in archives at STORAGE R US. Electronic copies of 2006-2012 on CDs in desk file.	Desk file is locked. Key is secure. Contract with STORAGE R US has security provisions. Access to documents at STORAGE R US is restricted to authorized personnel. CDs are locked. Risk: Medium for hard copies in desk File; High for CDs due to size and location on portable media device. Action Items: update retention policy to require destruction after X years; shred hard copies that are no longer needed; encrypt electronic copies currently on CD and save on backed up server or on CD marked with dates, then securely destroy CDs

Worker with Access to PPHI	*Descriptions of documents, information systems that contain PPHI (each type of document or document set should be described in a separate row)*	*Where does it come from? How is it received? What is done with it? Why is the PPHI needed? How long is it necessary to keep*	*Where does it go? For what purpose? Who sends it? How is it transmitted?*	*Where is it stored? Hard copy? Portable Media Devices? Hard Drive of Computer? Email Server?*	*How is it protected during storage, transmission? Risk of Improper Use or Disclosure or Access (High/Medium/Low); proposed action Items to reduce risk.*

RESOLUTION #13-18

HIPAA HYBRID ENTITY DESIGNATION

WHEREAS, the Health Information Technology for Economic and Clinical Health Act (The "HITECH Act") required certain amendments to the privacy, security, breach notification and enforcement rules of the Health Insurance Portability and Accountability Act ("HIPAA"); and

WHEREAS, said rule changes have been adopted by the U.S. Department of Health and Human Services, 45 CFR Parts 160 and 164; and

WHEREAS, the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations apply to individuals and organizations designed in the law/regulations as covered entities. These covered entities include: (1) group health plans; (2) health care providers who conduct certain transactions electronically, including but not limited to transmission of health care claims, health care payments, enrollment in a health plan, and referral authorizations; and (3) health care clearinghouses. Although the City of Williamsburg as a whole does not primarily engage in these activities, the Fire Department performs functions which qualifies it as a covered health care provider under the HIPAA definition; and

WHEREAS, an organization such as the City of Williamsburg that has both covered entity departments and non-covered entity departments may choose to be designated as hybrid entities. In this case, the City must designate and include in its HIPAA "health care component" those departments of the City that would meet the definition of a covered entity if they were separate legal entities. In this case, although the City as a hybrid entity remains responsible for oversight, compliance and enforcement obligations, with such designation, the HIPAA requirements apply only to the health care component; and

WHEREAS, Council deems it appropriate to designate the City as a hybrid entity under HIPAA.

NOW THEREFORE, BE IT RESOLVED, BY THE COUNCIL OF THE CITY OF WILLIAMSBURG, VIRGINIA:

DESIGNATION OF HEALTH CARE COMPONENT

The City has designated the Fire Department as the department constituting its health care component as the Fire Department would meet the definition of a covered entity if it were a separate legal entity and performs covered functions or transactions under HIPAA as a health care provider due to their emergency medical operations.

The Office of the City Attorney and the Information Technology Departments also perform functions which would make these offices business associates if they were separate legal entities. The Office of the City Attorney is designated as such only to the extent that any protected health information (PHI) is disclosed in the course of providing legal advice and legal services to the Fire Department. The Information Technology Department also performs limited administrative support services for Fire Department electronic records containing PHI, and is designated as such for that limited purpose.

The City, through its Human Resources office, maintains employee health records in its capacity as an employer, which is excluded from the definition of PHI under HIPAA. Further, the City's Human Resources office maintains various employee health insurance records in its capacity as employer sponsor of the City's group health plan. The Human Resources office is not a City health care component. The group health plan offered to City employees is a separate legal entity covered by HIPAA, independent of the City. The plan currently includes medical, vision, and dental care, prescription drug benefit, and an employee assistance program. The plan has HIPAA compliance obligations separate and apart from the City and is not a health care component of the City.

Additionally, the Department of Human Services and the Police Department have or may have medical information contained in their records. Neither the Department of Human Service nor the Police Department would be considered a covered entity under HIPAA if they were separate legal entities and do not perform covered functions or transactions which would qualify these departments as health care providers or business associates under HIPAA or which would obligate either of these departments to adopt privacy rules or practices under HIPAA.

DESIGNATION OF PRIVACY AND SECURITY OFFICERS

The Fire Chief is designated as the Privacy Officer for the City's health care component.

NON-RETALIATION POLICY

The City, its health care component and personnel shall not intimidate, threaten, coerce, discriminate against or take other retaliatory action against anyone for exercising his/her right under the privacy regulations or participating in any process established by the privacy regulations; nor for filing a complaint, participating in an investigation or audit or review proceeding conducted by the City or a government agency under the privacy regulations, or opposing any act or practice made unlawful by the privacy regulations. Any individual who believes that some form of retaliation under the privacy regulations has occurred or is occurring should report such concern to the relevant privacy officer designated above. The privacy officer will then conduct an investigation and, if the retaliation is substantiated, will impose sanctions accordingly.

Adopted: December 12, 2013

Clyde A. Haulman, Mayor

Attest: Donna Scott

Donna Scott, City Council Clerk

GREENWOOD COMMON COUNCIL

RESOLUTION NO. 13-10

A RESOLUTION OF THE GREENWOOD COMMON COUNCIL DECLARING THE CITY OF GREENWOOD, INDIANA A HYBRID ENTITY FOR PURPOSES OF HIPAA AND HITECH

WHEREAS, the federal government enacted the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology Economic and Clinical Health Act of 2009 ("HITECH") to protect patient health information;

WHEREAS, HIPAA and HITECH allow entities that perform covered and non-covered functions to designate themselves as Hybrid Entities

WHEREAS, a Hybrid Entity is defined as a single legal entity that performs both HIPAA covered and non-covered functions that designates health care components in accordance with 45 CFR § 164.504(c)(3)(iii);

WHEREAS, the City has determined that it performs both covered and non-covered functions;

WHEREAS, HIPAA standards must apply to health plans, health care clearing houses, and health care providers that transmit health information in an electronic format;

WHEREAS, Hybrid Entities must only apply HIPAA standards to designated health care components of the entity;

WHEREAS, in order to designate itself a Hybrid Entity, the City must designate and document components of the City that are health care components;

WHEREAS, health care components include components to the extent that they perform covered functions or activities that would make such component a business associate of a component that performs covered functions if the two (2) were separate legal entities;

WHEREAS, Title II of HIPAA sets forth policies, procedures, and guidelines for maintaining security of Protected Health Information ("PHI");

WHEREAS, the City will enact safeguards to prevent disclosure of PHI to another component of the covered entity where HIPAA would prohibit disclosure if the two were separate legal entities; and

WHEREAS, after thoughtful consideration the City believes it is in its best interest to declare itself a Hybrid Entity.

NOW, THEREFORE, BE IT RESOLVED BY THE GREENWOOD COMMON COUNCIL THAT:

Section 1. The City of Greenwood Common Council hereby designates the City a Hybrid Entity pursuant to 45 CFR § 164.103 and 164.105.

Section 2. The following are considered health care components of the City:

- The Human Resources in its function administering the City's health insurance benefits plans for medical, dental, vision, and health flexible spending plans only. This designation does not extend to the Human Resources Department's other functions, including, but not limited to, its administration of the City's workers' compensation and disability benefit programs, its personnel management, and its hiring and disciplinary duties.
- Office of Corporation Counsel in its function involving legal representation of the City's health insurance benefits plans for medical, dental, vision, and health flexible spending plans only and its representation of the Fire Department with respect to its provision of emergency medical services which, if provided external

to the City, would make it a business associate for HIPAA purposes. This designation does not extend to other legal work performed by Office of Corporation Counsel for the City.

- The Finance Division of the Controller's Office in its function involving the billing, payment, and administration of health insurance payments for medical, dental, vision, and health flexible spending plans only, which if provided external to the City, would make it a business associate for HIPAA purposes. This designation does not extend to other financial work performed by the Controller's Office, including, but not limited to, payments relating to the City's workers' compensation and disability benefit programs.
- The Fire Department with respect to its provision of emergency medical services only. This designation does not extend to other work performed by the Fire Department, including providing services as part of the City's workers' compensation program or fire response and investigatory activities.
- The Information Technology Department with respect to its duties relating to providing technology services for the City's health care benefit plans for medical, dental, vision and health flexible spending plans and the Fire Department's emergency medical services, which if provided external to the City, would make it a business associate for HIPAA purposes.
- The Deputy Mayor in his role as designee of the Board of Public Works and Safety as administrator of the City's health benefit plans.

Section 3. Designations of covered entities must be maintained for six (6) years following termination of a covered entity and indefinitely for ongoing covered entities.

Section 4. The City shall institute safeguards and policies to ensure that:

- Each designated health care component shall not disclose PHI to another non-health care component of the City in any circumstance in which HIPAA would prohibit such a disclosure if the health care component and non-health care component were separate and distinct legal entities.
- Designated health care components shall not use or disclose PHI that it creates or receives from or on behalf of the health care component in a way that is prohibited by HIPAA's privacy standard and shall comply with HIPAA's security standards.
- If an employee performs duties for both a health care component and non-health care component of the City, the employee shall not use or disclose PHI created or received in the course of or incident to his or her's work for the health care component in a way prohibited by the HIPAA privacy and security standards.

Remainder of the Page Intentionally Left Blank

Adopted by the Common Council of Greenwood, Indiana, this 17th day of June, 2013.

David Hopper, President
Greenwood Common Council

FOR:	AGAINST:
Linda S. Gibson	
Ronald Bates	
Lisa McLaughlin	
Mike Campbell	

ATTEST:

Jeannine Myers, Clerk

The foregoing Resolution passed by the Common Council of the City of Greenwood, Indiana, on the 17th day of June, 2013, is presented by me this 18th day of June, 2013, at 8:30 o'clock A .m. to the Mayor of the City of Greenwood.

Jeannine Myers, Clerk

The foregoing Resolution passed by the Common Council of the City of Greenwood, Indiana, on the 17th day of June, 2013, is signed and approved by me this 18th day of June, 2013, at 3:30 o'clock P .m. to the Mayor of the City of Greenwood.

MARK W. MYERS, Mayor of the
City of Greenwood, Indiana

DOCKET ITEM:
CA_3

Chesapeake VIRGINIA

City of Chesapeake

Office of the City Attorney
306 Cedar Road
Chesapeake, Virginia 23322
(757) 382-6586
Fax (757) 382-8749

February 4, 2014

To: Mayor Krasnoff, Vice-Mayor de Triquet and Members of the City Council

Re: HIPAA Omnibus Rule Hybrid Entity Organizational Requirement Changes

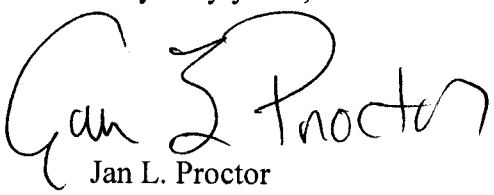
Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the City of Chesapeake ("City") is required to take certain precautions to prevent the disclosure of protected health information transmitted to the City for various purposes. The City has operated under HIPAA as a "hybrid entity," meaning that only certain of its departments, boards and commissions perform covered health care functions and are, thereby, subject to the HIPAA privacy rules. The designated health care components subject to HIPAA are Chesapeake Integrated Behavioral Healthcare (formerly Community Services Board) and the Chesapeake Fire Department, Emergency Medical Services. In addition, the following departments have been considered "business associates" because they may receive protected health information in the course of their business activities with Chesapeake Integrated Behavioral Healthcare or the Chesapeake Fire Department, Emergency Medical Services: Audit Services; the City Attorney's Office; the City Manager's Office; the City Treasurer's Office; the Finance Department; the Information Technology Department; and Parks and Recreation Department, Housekeeping Services. As "business associates," these departments entered into agreements to comply with HIPAA rules.

The recent HIPAA/HITECH (Health Information Technology for Economic and Clinical Health Act) Omnibus Rule, effective September 23, 2013, changed the organizational requirements for hybrid entities. Those departments that have been designated as "business associates" must now be designated as health care components. The attached resolution will affirm the City's designation as a hybrid entity and include all departments that may keep or receive protected health information as health care components. Adoption of the resolution is recommended to ensure compliance with HIPAA.

"The City of Chesapeake adheres to the principles of equal employment opportunity. This policy extends to all programs and services supported by the City."

Please advise if you have any questions in this regard.

Very truly yours,



Jan L. Proctor
City Attorney

JLP:hvm
Enclosure
cc: James E. Baker, City Manager
Wanda Barnard-Bailey, Deputy City Manager
Barbara O. Carraway, Treasurer
Edmund E. Elliott, Fire Chief
Joseph J. Scislowicz, Executive Director, Chesapeake Integrated Behavioral Healthcare
Jay Poole, City Auditor
Nancy Tracy, Director, Finance Department
Peter Wallace, Chief Information Officer, Information Technology Department
Michael D. Barber, Director, Parks and Recreation Department
Anna M. D'Antonio, Assistant to the City Manager

A RESOLUTION DESIGNATING THE CITY OF CHESAPEAKE AS A HYBRID ENTITY UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 AND ACCOMPANYING RULES AND REGULATIONS.

WHEREAS, the City of Chesapeake, Virginia (the "City") is committed to continued compliance with all applicable laws and regulations relating to health care privacy and security, including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and the regulations promulgated thereunder by the U.S. Department of Health and Human Services ("HIPAA Regulations"); and

WHEREAS, the City is a "covered entity" as that term is defined under HIPAA because of the services provided by Chesapeake Integrated Behavioral Healthcare and the Fire Department, Emergency Medical Services; and

WHEREAS, the City Council has determined that the City may more effectively and efficiently administer compliance with HIPAA, HITECH, and HIPAA Regulations by continuing to designate the City as a "hybrid entity," as that term is defined under HIPAA and HIPAA Regulations; and

WHEREAS, all third parties contracting with the City and meeting the definition of a business associate, as defined in 45 C.F.R. § 160.103, will continue to be required to execute a Business Associate Agreement to protect the privacy of protected health information in compliance with HIPAA and HIPAA regulations.

NOW, THEREFORE, BE IT RESOLVED, by the City Council of the City of Chesapeake, Virginia that the City Council hereby continues to designate the City of

City Attorney's Office
City of Chesapeake
Municipal Center
306 Cedar Road
Chesapeake, Virginia
23322
(757) 382-6586
Fax: (757) 382-8749

Chesapeake ("City") as a "hybrid entity" as defined in the HIPAA Regulations.

BE IT FUTHER RESOLVED, the following City departments are hereby designated as health care components of the City:

1) Chesapeake Integrated Behavioral Healthcare; and

2) The Fire Department, Emergency Medical Services.

BE IT FURTHER RESOLVED, the following City departments are also designated as health care components of the City only to the extent that they create, receive, maintain, or transmit protected health information on behalf of Chesapeake Integrated Behavioral Healthcare and the Fire Department, Emergency Medical Services:

a) Audit Services;

b) the City Attorney's Office;

c) the City Manager's Office;

d) the City Treasurer's Office;

e) the Finance Department;

f) the Information Technology Department; and

g) Parks and Recreation Department, Housekeeping Services.

BE IT FURTHER RESOLVED, the City Council hereby authorizes and directs the City Manager or designee to develop and implement policies and procedures and any other actions necessary to cause the City to continue to comply with HIPAA, the HITECH Act, and the HIPAA regulations for hybrid entities.

City Attorney's Office
City of Chesapeake
Municipal Center
306 Cedar Road
Chesapeake, Virginia
23322
(757) 382-6586
Fax: (757) 382-8749

ADOPTED by the Council of the City of Chesapeake, Virginia this ____ day of February, 2014.

APPROVED:

_____
Mayor

ATTEST:

_____
Clerk of the Council

City Attorney's Office
City of Chesapeake
Municipal Center
306 Cedar Road
Chesapeake, Virginia
23322
(757) 382-6586
Fax: (757) 382-8749

MUNICIPALITIES AS HYBRID ENTITIES UNDER HIPAA

by C. Michael Bakewell

In an age when people can share information with mass audiences in an instant, privacy can be challenging to protect. While this applies to many fields, healthcare is a top concern for the protection of confidential records. This article addresses the expectation of municipalities to comply with HIPAA requirements and ways to protect the health information of citizens without undue burden to local government services.

Risks Of HIPAA Noncompliance By "Covered Entity" Municipalities

A municipality that qualifies as a "covered entity" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] must comply with the requirements of HIPAA for the protection of protected health information (PHI).[2]

For municipalities, two possible functions may make the governmental entity a HIPAA "covered entity": (1) a health plan[3] and/or (2) a health care provider that electronically transmits health information in connection with a HIPAA transaction.[4]

If a municipality or other governmental entity performs "covered entity" functions, then it is beyond debate that the governmental entity should comply with the HIPAA Privacy Rule and the HIPAA Security Rule.[5] The penalties for noncompliance can be significant. For instance, in July 2011, the Health System of the University of California in Los Angeles resolved a HIPAA investigation with the United States Department of Health and Human Services (HHS) by agreeing to pay $865,500.00 for alleged employee violations of HIPAA.[6] Similarly, in March 2012, Blue Cross & Blue Shield of Tennessee agreed to pay $1.5 million to settle potential violations of the HIPAA Privacy and Security Rules;[7] and in June 2012, the Alaska Department of Health and Social Services agreed to pay $1.7 million for its alleged failure to have adequate policies and procedures in place to safeguard electronic PHI.[8]

Adding to the legal hurdles that a "covered entity" must address, in early 2009, Congress passed and the President signed the Health Information Technology for Economic and Clinical Health Act (HITECH Act) that enacted a number of changes to HIPAA.[9] Among other changes, the HITECH Act increased the fines for noncompliance or violations of HIPAA occurring after Feb. 18, 2009.[10] In Oct., 2009, the secretary of HHS issued its final interim rule for HIPAA enforcement and civil fines in accordance with the HITECH Act.[11] Under this Interim Final Enforcement Rule, the amount of the civil penalties is based on the degree of a "covered entity's" culpability, and has a dollar limit on identical violations occurring within a calendar year. The yearly limit, however, only applies to identical violations of the same HIPAA provision. The chart below, taken from the Interim Final Enforcement Rule, summarizes the increased civil penalties.[12]

Of concern to a non-compliant municipality should be the announcement by the Office for Civil Rights of the U.S. Department of Health and Human Services in November 2011, that it was commencing random compliance audits of covered entities as required by the HITECH Act.[14] The pilot audit program will perform 115 audits of "covered entities" within one year to assess privacy and security compliance.[15] The HHS website provides information about who may be audited (every covered entity and business associate is eligible for an audit) and how the audit program will work.[16] Recently, the Office for Civil Rights of HHS released its audit protocol. The audit protocol contains the requirements that auditors will review and assess in the audit process to analyze processes, controls, policies and procedures a "covered entity" has in place for HIPAA compliance.[17] The audit protocol contains 77 performance criteria for Security Rule compliance and 88 performance criteria for Privacy Rule and breach notification requirements.[18]

Civil Penalties for HIPAA Violations By Covered Entities and Business Associates

Culpability for Violation	Per Violation	Maximum for Identical Violation of same HIPAA provision per calendar year
Did not know	$100 up to $50,000	$1,500,000
Reasonable Cause	$1,000 up to $50,000	$1,500,000
Willful Neglect—corrected in timely manner	$10,000 up to $50,000	$1,500,000
Willful Neglect[13] — not corrected	$50,000	$1,500,000

ING is the retirement plan provider endorsed by Missouri Municipal League.



How do you measure up? Visit www.INGCompareMe.com and http://www.ingretirementplans.com/mrodemoCHC

ING
Your future. Made easier.®

3019237.G.S ©2011 ING North America Insurance Corporation.
Products and services available through the ING family of companies. C11-0112-011 (02/11)

HHS is serious about HIPAA compliance by "covered entities." For instance, the director of the Office for Civil Rights (OCR) has stated, as part of several HIPAA violation settlements, "We hope that health care providers … understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity."[19] "[W]e expect organizations to comply with their obligations under those rules regardless of whether they are private or public entities."[20]

To avoid costly penalties for non-compliance, a municipality performing "covered entity" functions should thoroughly assess existing policies and procedures and use the OCR's audit protocols as guidelines to conduct another risk assessment and ensure current compliance with the HIPAA Privacy and Security Rules.

Why Choose Hybrid Entity Status

The HIPAA Privacy Rule permits an entity, such as a municipality, to separate its "covered entity" functions from its "non-covered entity" functions so that only the "covered entity" functions are required to comply with the HIPAA regulations.[21] The separation of HIPAA-governed functions creates what is known as a "hybrid entity." A municipality that performs "covered entity" functions should consider "hybrid entity" designation so that its departments that possess medical information on citizens, but do not perform "health plan" functions or "medical provider" functions, will not be required to protect that medical information in compliance with HIPAA.

If a governmental entity constitutes a "covered entity" or performs a "covered entity" function and has not made a hybrid entity designation, then the entire entity, including all of its departments, is required to comply with HIPAA.[22] For example, (1) the police department, that generally does not perform "covered entity" functions, would have to secure and protect incident reports containing medical information under HIPAA; (2) the city jail, if it dispenses medication or has a notation referring to a prisoner's medical condition, would have to comply with HIPAA; (3) a city utility with a "non-disconnect" customer list containing the customers' medical conditions would be required to comply with HIPAA; or (4) the emergency dispatch (911) department (that dispatches police, fire and ambulance services) because it has data about the medical information of individuals would have to comply with HIPAA for all of its dispatching services.

By choosing hybrid entity status, a municipality may be able to reduce compliance costs and potential liability.

By choosing hybrid entity status, a municipality may be able to reduce compliance costs and potential liability. For instance, all workforce members of a covered entity are required to undergo training on HIPAA policies and procedures.[23] Without a hybrid entity designation by a municipality, those employees who are unlikely to have any contact with PHI, such as building department employees, municipal court employees and street department employees, would still be required to receive initial and on-going HIPAA training. Similarly, a police department or jail that possesses individually identifiable medical information, as well as the employees of those departments, would be required to comply with HIPAA even if those departments perform no "covered entity" functions.

Without hybrid entity designation, a municipality and all of its departments would be required to perform extensive analyses, and adopt and implement a number of policies and procedures simply to ensure compliance with HIPAA. For example, the National Institute of Standards & Technology has issued a guide publication that contains approximately 40 pages of requirements, considerations, questions, analyses and policies for a covered entity to answer, review and implement just for compliance with the Security Rule.[24] In addition, the HITECH Act adopted notice requirements that must be followed if a covered entity uses or discloses PHI in violation of HIPAA and its regulations.[25] Those requirements include notifying the affected individual, as well as notifying HHS (and possibly the media), of the breach of PHI.[26] Since 2009, over 430 entities have reported breaches of PHI to the U.S. Department of Health and Human Services that affect more than 20 million individuals.[27] By adopting hybrid entity status, non-covered entity departments possessing individual health care information would not be subject to those notification requirements for a breach of PHI under HIPAA,[28] and would not otherwise be required to comply with the HIPAA regulations.

Qualifying As A Hybrid Entity

To qualify for hybrid entity status, a governmental entity must be a single legal entity that performs both HIPAA-covered and non-covered functions.[29] Hybrid entity status, however, is not automatic for a municipality meeting this definition. To become a hybrid entity, the governing body of the municipality must designate in writing those health care components and functions that must comply with HIPAA.[30] This written designation must include all of those health care components that would meet the definition of a covered entity if those components were separate legal entities.[31] With a hybrid entity

designation, compliance with HIPAA only applies to the designated health care components;[32] although, the municipality as a whole is still responsible for oversight, compliance and enforcement obligations.[33]

A hybrid entity designation also permits the governmental entity to include in its list of designated health care components the functions of other departments not performing HIPAA-covered functions, but that do perform support activities for the health care components (*e.g.,* those components that act as business associates for the health care components).[34] For example, if the City's finance department performs ambulance billing and that is its only "covered" function, then only that function of the finance department could be included as a health care component in the hybrid entity designation.[35] Thus, medical information collected in other functions of the finance department (such as the medical condition of customers on the "non-disconnect" list for the city-owned utility) would not be subject to HIPAA. Since the HITECH Act requires compliance by business associates with most provisions of the HIPAA Privacy Rule and Security Rule, a governmental entity declaring itself a hybrid entity may wish to consider including the portion of departments performing business associate functions as part of its health care components designation.[36]



Without hybrid entity designation, a municipality and all of its departments would be required to perform extensive analyses, and adopt and implement a number of policies and procedures simply to ensure compliance with HIPAA.

Implementing The Hybrid Entity Designation

Making a hybrid entity designation comes with its own set of compliance requirements. Once a municipality designates its "health care components" and "health care" functions as part of its hybrid entity designation, the municipality must implement certain policies and procedures as a hybrid entity. These include the following:

(1) The municipality must create firewalls between its various health care components and between those components and non-HIPAA components. HIPAA prohibits one health care component from sharing PHI with another health care component or with a non-health care component if the disclosure would be prohibited by HIPAA where the components are separate legal entities.[37]

(2) The municipality must ensure that its designated health care components perform required risk analyses; develop and adopt appropriate policies and procedures; and train the affected workforce members for compliance with the HIPAA Privacy Rule and HIPAA Security Rule.

(3) Any member of the workforce who performs duties for both a health care component and other components of the hybrid entity must not use or disclose PHI obtained in his/her work for the health care component in a manner prohibited by HIPAA.[38] Thus, an employee in the finance department doing ambulance billing could not use PHI (including addresses) to bill a patient/citizen for personal property taxes. Similarly, an employee working in a health plan component who has access to health insurance application forms for employees should not use such information (including addresses) to update the employee's employment records.

Consequently, with hybrid entity status, the governmental entity must develop clear policies, with sufficient training of affected employees, to ensure that PHI is not improperly shared or improperly used within the entity. Nonetheless, a municipality correctly designating its health care components and specific functions of departments that support those health care components can reduce its initial and on-going compliance costs and likely reduce its liability exposure by exempting a number of employees and operations from the requirements of HIPAA.

Conclusion

HIPAA compliance is essential for municipalities that perform "covered entity" functions as defined in the regulations. Because of the variety of services and functions typically provided by a municipality, HIPAA compliance, if required, poses substantial burdens and challenges. With the likely savings of time, expense and paperwork by declaring itself a hybrid entity, such a designation is worth consideration by a "covered entity" municipality.❑

C. Michael Bakewell practices law in the greater St. Louis area and is a graduate of the University of Missouri-Columbia School of Law. He has represented fire protection districts for over 20 years, and has advised several fire protection districts and private medical practices in achieving and maintaining compliance with HIPAA privacy and security regulations. Bakewell is a member of Barken & Bakewell, LLC and can be reached at 314-219-7554.

*You may request a copy of the footnotes for this article by calling Missouri Municipal League at 573-635-9134 or email info@mocities.com.