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

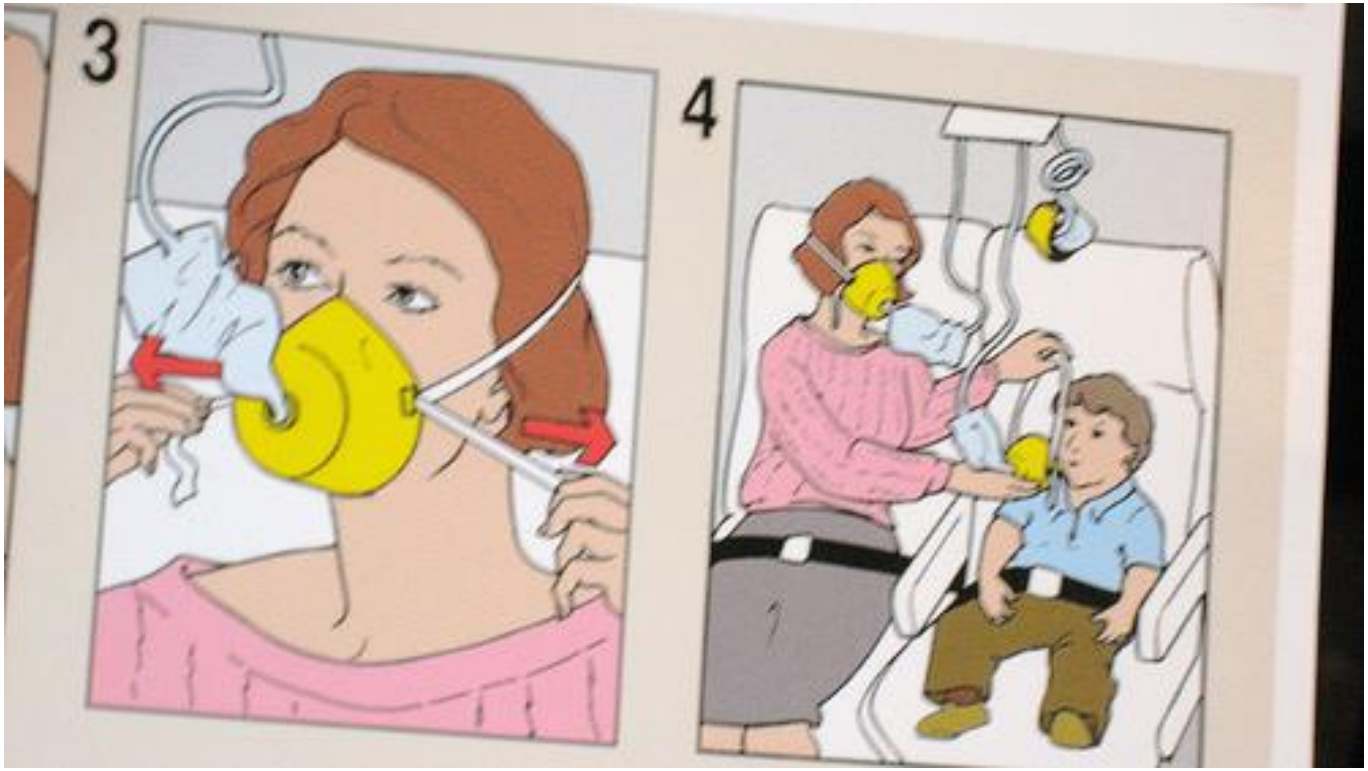
What could happen if . . .

- 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

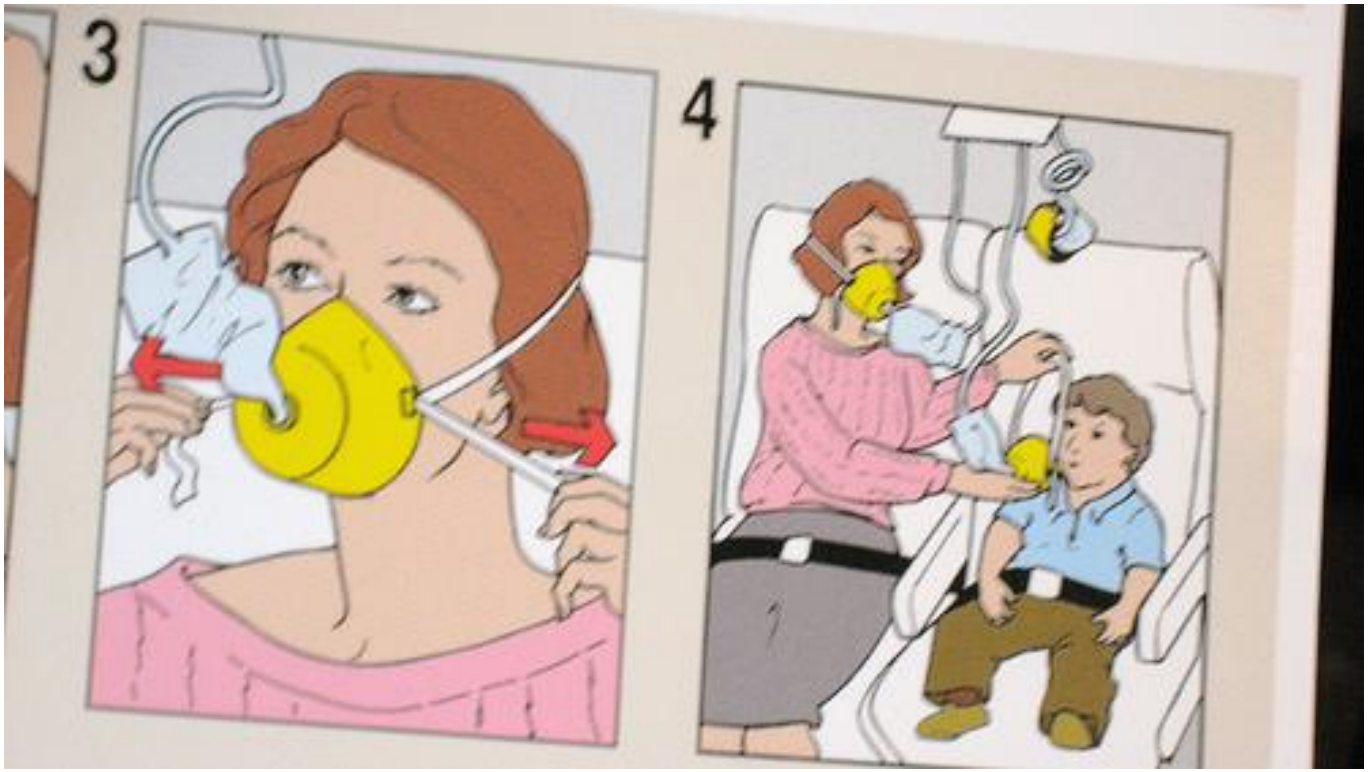
- Why is it so important to Stop Work and Report? Immediate action can . . .
  - reduce harm
  - stop harm from getting worse
  - prevent an incident from becoming a breach
  - protect GMA from penalties, bad press
- NEVER try to hide the incident or fix the problem before reporting



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