



IG Advisors®

Consulting and Training Solutions

Information Governance, the Next Evolution of Privacy and Security

Katherine Downing, MA, RHIA, CHPS, PMP

Sr. Director AHIMA IG Advisors™

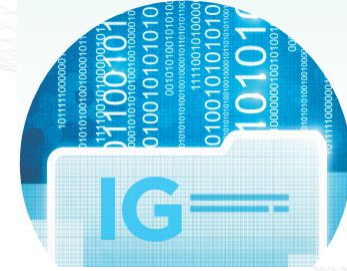
Follow me @HIPAAQueen

2017

IGAdvisors.com



Objectives



Part	IG Topic Area
Part I	“What and Why” of Information Governance in healthcare.
Part II	Identify methods to advance privacy and security practices within an information governance program.
Part III	Why Privacy and Security Programs must evolve
Part IV	Define initial projects to get information governance started.

AHIMA's Information Governance Adoption Model (IGAM™)

- Trusted, Reliable, Information Across the Healthcare Ecosystem to Enable:

- Patient and Consumer Engagement
- Healthier Populations
- Interoperable Care)
- Easy access to information
- Informatics – Information



WHAT IS INFORMATION GOVERNANCE (IG)?

AHIMA DEFINES IG AS “AN ORGANIZATION-WIDE FRAMEWORK FOR MANAGING INFORMATION THROUGHOUT ITS LIFECYCLE AND FOR SUPPORTING THE ORGANIZATION’S STRATEGY, OPERATIONS, REGULATORY, LEGAL, RISK, AND ENVIRONMENTAL REQUIREMENTS.”



Establishes
policy



Determines
accountabilities
for managing
information



Promotes objectivity
through robust,
repeatable
processes



Protects
information with
appropriate
controls



Prioritizes
investments

What is Information Governance?

INFORMATION GOVERNANCE FOR HEALTHCARE INCLUDES:



Adopting an IG program shows an organization's commitment to managing its information as a valued strategic asset.



IG Can Make a Difference - 2016 OCR Audit Findings

- Insider Threat
 - Access Controls
 - Mobile Device Security
 - Lifecycle of PHI and ePHI
 - Business Continuity /Disaster Recovery
 - Incomplete or Inaccurate Risk Assessment.
- Failure to manage identified risks.

Source: Devin McGraw HIPAA Summit 3.29.17. OCR.gov



Insider Threat

- Consider the insider threat
- Malicious
- Accidental
- Solution
 - Threats extend BEYOND threats to PHI
 - Trust and policy are not enough.
 - Organizations must invest in security, risk, and information governance training and enforcement.



HIMSS 2016 Cybersecurity Survey

Phishing attacks	76.7%	79.8%	64.5%
Virus/Malware	67.3%	68.1%	64.5%
Spearphishing attacks	58.0%	61.3%	45.2%
Negligent insider threat activity	52.0%	51.3%	54.8%
Advanced persistent threat (APT) attacks	48.7%	49.6%	45.2%
Malicious insider threat activity	32.7%	34.5%	25.8%
Brute force attacks	30.7%	31.9%	25.8%
Social engineering attacks/elicitatation	30.0%	29.4%	32.3%

Source: 2016 HIMSS Cybersecurity Survey available at:
<http://www.himss.org/hitsecurity>

Mitigating Insider Threat with CyberEducation as part of IG

- Education regarding phishing, whaling, spearphishing should be enterprise wide.
- Be suspicious of unsolicited phone calls, social media interactions, or email messages asking about employees or other internal information.
- Do not reveal financial information via social media or links sent in emails.
- Do not provide company information regarding networks, structures
- Pay attention to the URL of a website!

Insider Threat - The Link Between Access & CyberThreats



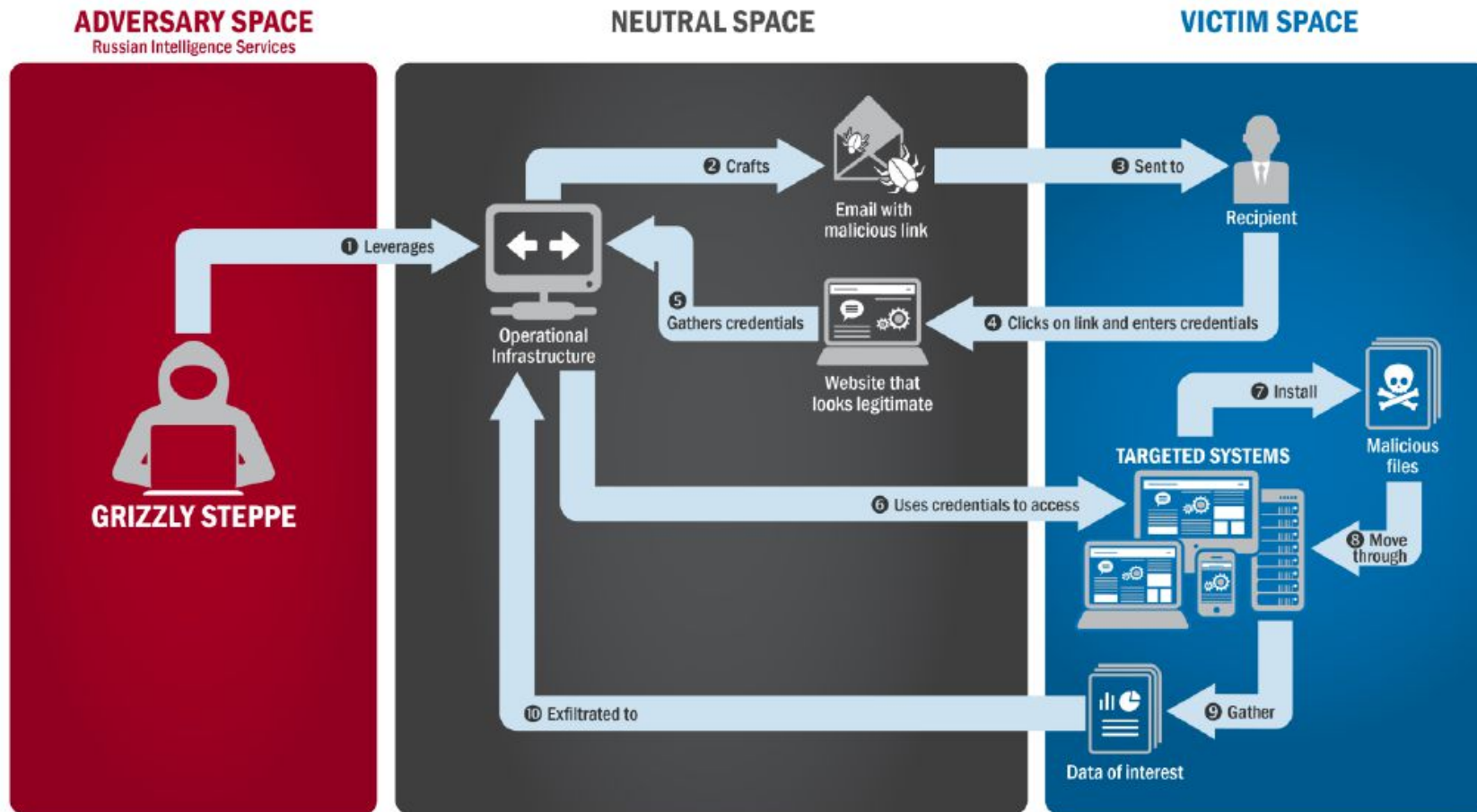
- **Review of Access is a Key First Step**
 - Appropriate Access: reduce privileges
 - Restrict ability to install and run unwanted software
 - Review admin capabilities to user machines
 - Group policy
 - Administrative users should use non-privileged accounts for standard functions such as web browsing!
 - Firewall best practices

Insider Threat Example: GRIZZLY STEPPE – Russian Malicious Cyber Activity Report

- Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with:
 - U.S. Government, political, and private sector entities.



Source: Joint Analysis Report (JAR) from Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf



Source: Joint Analysis Report (JAR) from Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

What are the Symptoms of a DoS Attack?

- Inability to access particular website or any website
- S – L – O – W network performance
- Dramatic increase in # of spam emails (DoS attack = email bomb)



Ransomware Techniques Target Insiders

- Vulnerable Web Servers / Firewall Weakness
- Phishing emails
- Brute force hacking
- Drive-by downloading
- Web-based instant message applications



Educating Ransomware

- User receives a message that files have been encrypted and payment is required.
- Do your users know what to do?
 - Contact security officer
 - Contact external / internal resources
 - Legal Council
 - Initiate contingency plans
 - Investigate scope of encrypted data
 - Forensics if needed
 - Law enforcement



Information Governance – Beyond PHI

- IG is an enterprise wide effort to protect **ALL** information and access points, not just clinical information.
- Getting Started with IG Practical Examples:
 1. Information Asset Inventory
 - Enterprise wide understanding of access
 - Data and Information Stewards
 - Data Owners
 2. Information Classification
 3. Data and Information Inventory



Information Governance for Mobile Devices



- Information Governance for mobile computing can include building security into the mobile applications.
- Are your nurses texting your physicians?
- How are they identifying patients?
- Do you offer encrypted texting options?

Information Governance Mobile Device Policy

- Requires a cross functional IG team
- Clarify how mobile devices are being used
 - EHR Access
 - Financial system access
 - Email
- Consider legal and compliance issues
- Consider Mobile Device Management
- Develop your Communications and Training Plan
- Update and Fine-Tune – this one can't stay on the shelf!



Medical and Other Devices

- As we install more smart devices in our hospitals we increase vulnerabilities.
- Medical devices are more vulnerable to cyber-attacks than normal IT endpoints.
 - Lower security maturity
 - Long useful life – end of support software
 - Slow security patch deployment



IG Best Practices for Securing Medical Devices

- We cannot eliminate risk / Mitigation is Key.
 - Encryption
 - Risk Analysis
 - Authorized Devices Only
 - Automatic Log Off
 - Audit Controls
 - Cybersecurity Patches
- We cannot achieve security for these devices, we can only improve it.
- Resources from FTC, FDA, NIST and IHE.



Business Continuity and Disaster Recovery

Key Components of Information Governance

- Disaster Recovery Plan and Business Continuity Plans are part of the organizations overall emergency management plan.
- Tested Policies, Procedures, Systems
- Trained Staff



Extending Breach Investigation Process: it's More than PHI



- Gather all the facts of the potential breach
- Document specifically who, when, where, why and how the situation occurred
- Identify those impacted and what information was potentially compromised
- Analyze & evaluate all the facts objectively to determine whether or not an impermissible access, use, or disclosure of PHI (information!) can be substantiated.

Information Governance Manages through the Full Lifecycle

- Creation of information
- Management of information
- Use, Access, Sharing
- Inventory / Tracking
- Final disposition of information
 - All devices, printers containing PHI
 - ePHI
 - Paper
 - Microfilm



IG for Email



- **Major area of focus for IG programs**
 - Most common business software application
 - Backbone of business communications
 - Leading piece of evidence requested during discovery phase of civil trials – may contain discoverable information in litigation.
 - **Email systems can be hacked, monitored and compromised.**

Commit to Info Gov Best Practices

- Backups
- Risk Analysis
- Staff Training
- Vulnerability Scanning and Patching
- Application Whitelisting
- Incident Response
- Business Continuity
- Penetration Testing



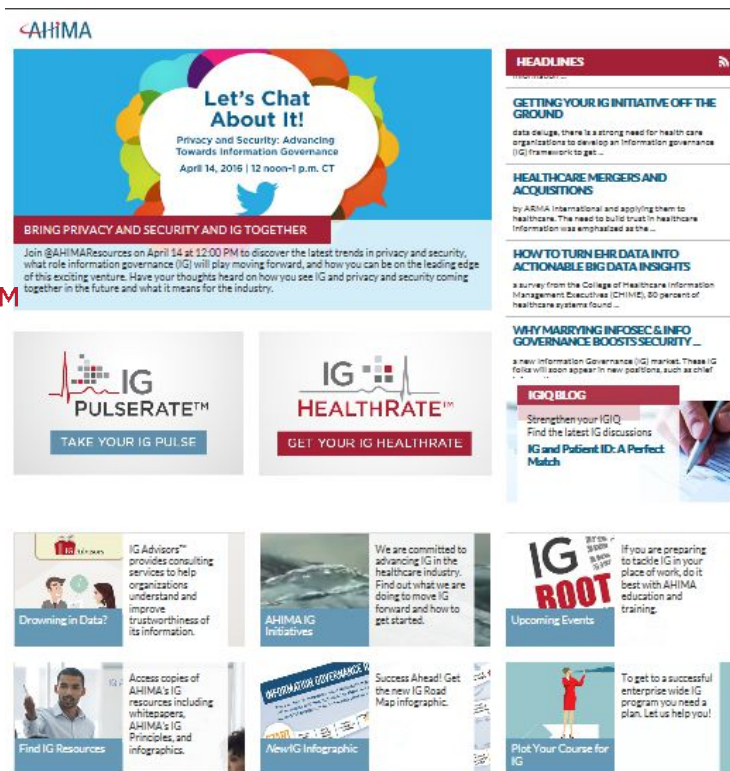
Source: Joint Analysis Report (JAR) from Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Expanding Privacy and Security to IG – Where to Start?

- New areas included in the IGAM relate to the responsibilities of the Privacy/Security Officer
 - Information Asset Inventory
 - Access Controls
 - Breach Management
 - Mobile Device Management
 - Social Media Controls
 - Email Management
 - Enterprise wide training and awareness programs
 - Compliance monitoring
 - Business Continuity and Disaster Recovery
 - Total cost of ownership
 - Patient information request response

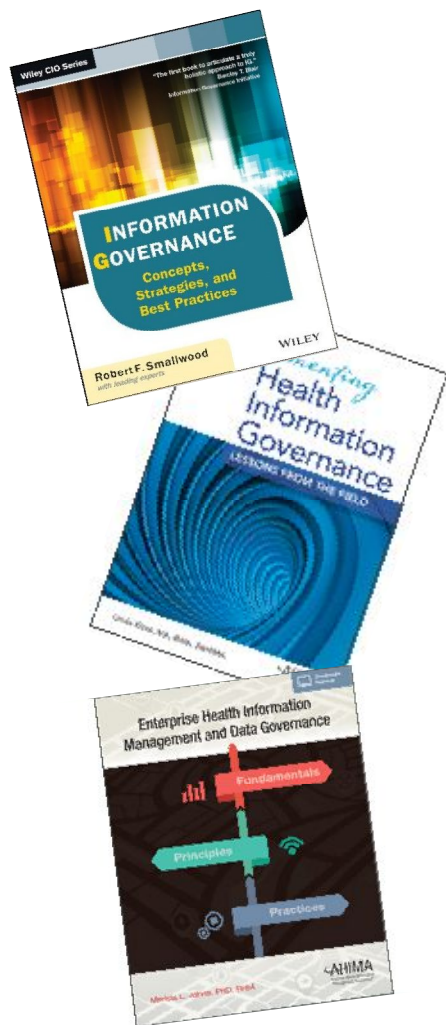


IGIQ.com is your ONE STOP for all Tools and Resources for Information Governance

The screenshot shows the AHIMA IG IQ website. At the top is the AHIMA logo. Below it is a large blue banner with a colorful circular graphic and the text "Let's Chat About It! Privacy and Security: Advancing Towards Information Governance April 14, 2016 | 12 noon-1 p.m. CT". Below the banner is a section titled "BRING PRIVACY AND SECURITY AND IG TOGETHER" with a paragraph of text. To the right is a "HEADLINES" section with three articles: "GETTING YOUR IG INITIATIVE OFF THE GROUND", "HEALTHCARE MERGERS AND ACQUISITIONS", and "HOW TO TURN EHR DATA INTO ACTIONABLE BIG DATA INSIGHTS". Below the headlines is a "WHY MARRYING INFOSEC & INFO GOVERNANCE BOOSTS SECURITY ..." section. Further down is an "IGIQ BLOG" section with a post titled "Strengthen your IG IQ: Find the latest IG discussions IG and Patient ID: A Perfect Match". At the bottom are several smaller tiles: "Drowning in Data?", "AHIMA IG Initiatives", "Success Ahead! Get the new IG Road Map infographic.", "Find IG Resources", "New IG Infographic", and "Plot Your Course for IG".

Information Governance Resources



- **Three IG Books in the AHIMA Store**
 - Information Governance Concepts, Strategies, and Best Practices (Smallwood)
 - Implementing Health Information Governance (Kloss)
 - Enterprise Health Information and Data Governance (Johns)

References and Recommended Reading

- *Enterprise Health Information Management and Data Governance*, 2015. Merida L Johns, PhD, RHIA.
- www.HHS.Gov/HIPAA
- 2016 HIMSS Cybersecurity Survey available at: <http://www.himss.org/hitsecurity>
- Combined HIPAA/Omnibus Rule <http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html>
- U.S. Department of Health and Human Services Office for Civil Rights: HIPAA Administrative Simplification - 45 CFR Parts 160, 162, and 164
- Information Governance, 2014. Robert F. Smallwood
- Cohasset Associates and AHIMA. "A Call to Adopt Information Governance Practices." 2014 *Information Governance in Healthcare*. Minneapolis, MN.
- Cohasset Associates, 2015. Cohasset Associates and AHIMA. "Professional Readiness and Opportunity" 2015 *Information Governance in Healthcare*. Minneapolis, MN. Cohasset Associates, 2015.
- *Implementing Health Information Governance*, 2015. Linda Kloss, MA, RHIA, FAHIMA



A combination of virtual webinars and a one-day, online engagement, this meeting provides a deep dive into the application of IG tools and resources and an understanding of the IG discipline.

February 24

June 2

August 25

September 27

December 8

Visit IGIQ.com to register.



**Information Governance
Strategic Forum
MAY 16 | CHICAGO, IL**

Are You Leveraging Your Organization's Information as a Strategic Asset?

YOU SHOULD BE!

This one-day forum utilizes real-world case scenarios and essential tools and techniques to provide hands-on, practical exercises and in-depth discussion on timely topics to help you initiate an enterprise IG strategy for your organization.

Visit IGIQ.com to register.

What's Next? Moving Your Organization's IG Forward.



- IG consulting and Implementation services (project management)
- GAnalysis and assessment
- On-site or virtual organization-specific training
- Score validation from the IGHealthRate™ system for IGAM Level 5™ sites



- Identify your organization's true level of IG maturity
- Differentiate your organization from its competition and other organizations
- Validate your organization's maturity level with AHIMA
- Receive extensive reporting, guidance, and comparison to other entities of your size and specialty



- Quick check of your organization's IG maturity
- Begin to understand key success factors that impact organizational maturity
- Begin to identify strengths and weakness



- IG Toolkit
- White papers
- Infographics
- Blog

**For more information
contact us at
(844) 554-4447
or visit IGIQ.org.**



- Webinars
- IG Boot Camps
- IG Leadership Forums
- Books
- For more Information on IG education, visit ahima.org/Infogov