Update on Administration and Enforcement of the HIPAA Privacy, Security, and Breach Notification Rules

Lesley Morgan, Investigator
Contractor for Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

Updates

- Policy Development
- Breach Notification
- Enforcement
- Audit

POLICY DEVELOPMENT

New OCR Guidance on HIPAA and Information Related to Mental and Behavioral Health

- Opioid Overdose Guidance (issued 10/27/2017)
- Updated Guidance on Sharing Information Related to Mental Health (new additions to 2014 guidance)
- 30 Frequently Asked Questions:
  - New tab for mental health in “FAQs for Professionals”
  - 9 new FAQs added (as PDF and in database)
- New Materials for Professionals and Consumers
  - Fact Sheets for Specific Audiences
  - Information-sharing Decision Charts

OCR Website Navigation

- For professionals: https://www.hhs.gov/hipaa/for-professionals/index.html > Special Topics > Mental Health & Substance Use Disorders
- For consumers: https://www.hhs.gov/hipaa/for-individuals/index.html > Mental Health & Substance Use Disorders
- Mental Health FAQ Database: https://www.hhs.gov/hipaa/for-professionals/faq/mental-health

HIPAA Right of Access Guidance

- Issued in two phases in early 2016
  - Comprehensive Fact Sheet
  - Series of FAQs
    - Scope
    - Form and Format and Manner of Access
    - Timeliness
    - Fees
    - Directing Copy to a Third Party, and Certain Other Topics

Access – Scope

- Designated record set broadly includes medical, payment, and other records used to make decisions about the individual
  - Doesn’t matter how old the PHI is, where it is kept, or where it originated
  - Includes clinical laboratory test reports and underlying information (including genomic information)

Access – Scope (cont.)

- Very limited exclusions and grounds for denial
  - E.g., psychotherapy notes, information compiled for litigation, records not used to make decisions about individuals (e.g., certain business records) BUT underlying information remains accessible
  - Covered entity may not require individual to provide rationale for request or deny based on rationale offered
  - No denial for failure to pay for health care services
  - Concerns that individual may not understand or be upset by the PHI not sufficient to deny access

Access – Requests for Access

- Covered entity may require written request
- Can be electronic
- Reasonable steps to verify identity
- BUT cannot create barrier to or unreasonably delay access
  - E.g., cannot require individual to make separate trip to office to request access

Access – Form and Format and Manner of Access

- Individual has right to copy in form and format requested if "readily producible"
  - If PHI maintained electronically, at least one type of electronic format must be accessible by individual
  - Depends on capabilities, not willingness
  - Includes requested mode of transmission/transfer of copy
    - Right to copy by e-mail (or mail), including unsecure e-mail if requested by individual (plus light warning about security risks)
    - Other modes if within capabilities of entity and mode would not present unacceptable security risks to PHI on entity's systems

Access – Timeliness and Fees

- Access must be provided within 30 days (one 30-day extension permitted) BUT expectation that entities can respond much sooner
- Limited fees may be charged for copy
  - Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if applicable); costs for supplies and postage
  - No search and retrieval or other costs, even if authorized by State law
  - Entities strongly encouraged to provide free copies

Third Party Access to an Individual’s PHI

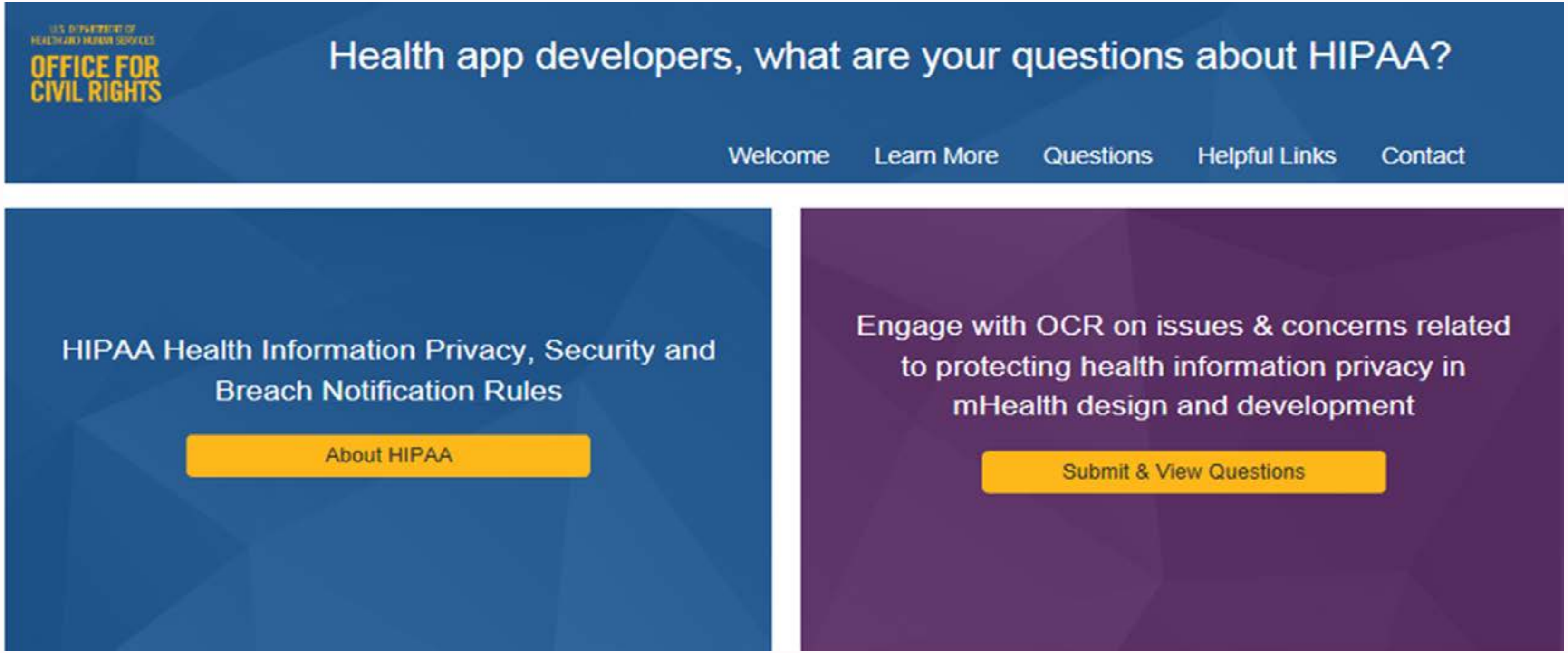
- Individual’s right of access includes directing a covered entity to transmit PHI directly to another person, in writing, signed, designating the person and where to send a copy (45 CFR 164.524)
- Individual may also authorize disclosures to third parties, whereby third parties initiate a request for the PHI on their own behalf if certain conditions are met (45 CFR 164.508)

Platform for users to influence guidance
http://hipaaQsportal.hhs.gov/

HIT Developer Portal

- OCR launched platform for mobile health developers in October 2015; purpose is to understand concerns of developers new to health care industry and HIPAA standards
- Users can submit questions, comment on other submissions, vote on relevancy of topic
- OCR will consider comments as we develop our priorities for additional guidance and technical assistance
- Guidance issued in February 2016 about how HIPAA might apply to a range of health app use scenarios
- FTC/ONC/OCR/FDA Mobile Health Apps Interactive Tool on Which Laws Apply issued in April 2016

Platform for users to influence guidance
http://hipaaQsportal.hhs.gov/



Health app developers, what are your questions about HIPAA?

HIPAA Health Information Privacy, Security and Breach Notification Rules

Engage with OCR on issues & concerns related to protecting health information privacy in mHealth design and development

Cloud Computing Guidance

- OCR released guidance clarifying that a CSP is a business associate – and therefore required to comply with applicable HIPAA regulations – when the CSP creates, receives, maintains or transmits identifiable health information (referred to in HIPAA as electronic protected health information or ePHI) on behalf of a covered entity or business associate.

- When a CSP stores and/or processes ePHI for a covered entity or business associate, that CSP is a business associate under HIPAA, even if the CSP stores the ePHI in encrypted form and does not have the key.

- CSPs are not likely to be considered "conduits," because their services typically involve storage of ePHI on more than a temporary basis.
- http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html

New Cybersecurity Guidance page

Cyber Security Guidance Material

- HHS OCR has launched a Cyber Security Guidance Material webpage, including a Cyber Security Checklist and Infographic, which explain the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.
  - Cyber Security Checklist - PDF
  - Cyber Security Infographic [GIF 802 KB]

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Cybersecurity Newsletters

- Began in January 2016
- Recent 2017-2018 Newsletters
  - October 2017 (Mobile Devices and PHI)
  - November 2017 (Insider Threats and Termination Procedures)
  - December 2017 (Cybersecurity While on Holiday)
  - January 2018 (Cyber Extortion)
  - February 2018 (Phishing)
  - March 2018 (Contingency Planning)
  - April 2018 (Risk Analyses vs. Gap Analyses)
- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Ransomware Guidance

- OCR recently released guidance on ransomware. The new guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats.

- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted
- OCR posts breaches affecting 500+ individuals on OCR website

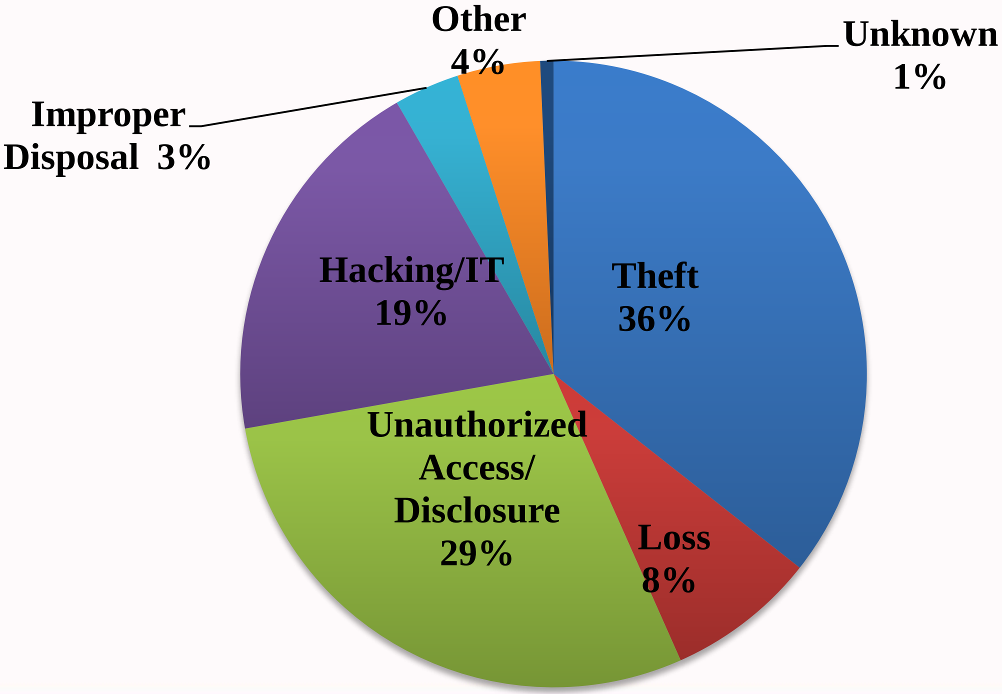
September 2009 through April 30, 2018

- Approximately 2,285 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 44% of large breaches
  - Hacking/IT now account for 19% of incidents
  - Laptops and other portable storage devices account for 25% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 262,262,738
- Approximately 347,103 reports of breaches of PHI affecting fewer than 500 individuals

500+ Breaches by Type of Breach

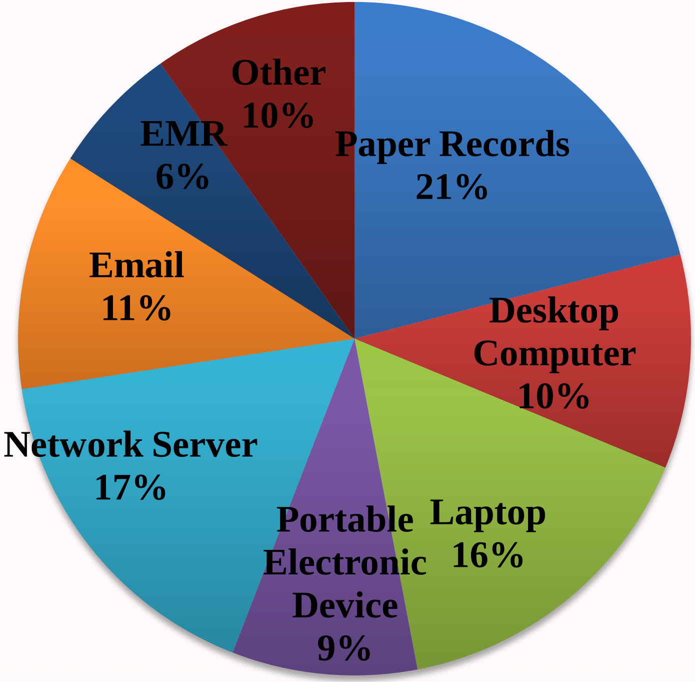
April 14, 2003 – April 30, 2018

Theft 36%



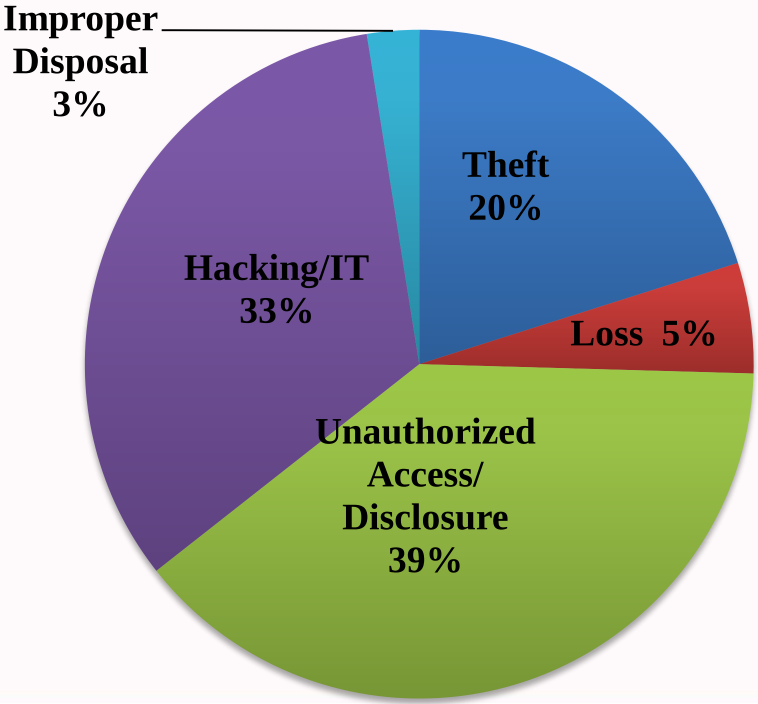
500+ Breaches by Location of Breach

April 14, 2003 – April 30, 2018



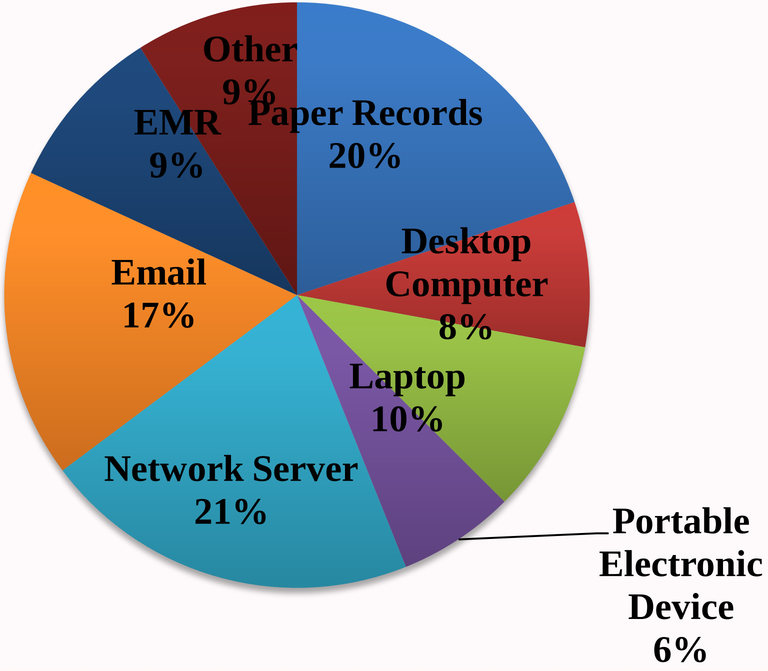
500+ Breaches by Type of Breach

5/1/2015 – 4/30/2018



500+ Breaches by Location of Breach

5/1/2015 – 4/30/2018



What Happens When HHS/OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity’s compliance prior to breach

General HIPAA Enforcement Highlights as of April 14, 2003 – April 30, 2018

- Over 180,192 complaints received to date
- Over 25,879 cases resolved with corrective action and/or technical assistance
- Expect to receive 24,000 complaints this year

General Enforcement Highlights

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action

- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action

- Resolution Agreements/Corrective Action Plans
  - 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts

- 3 civil money penalties

As of April 30, 2018

Recent Enforcement Actions

2017 - 2018

4/12/2017	Metro Community Provider Network	$400,000
4/21/2017	Center for Children's Digestive Health	$31,000
4/21/2017	CardioNet	$2,500,000
5/10/2017	Memorial Hermann Health System	$2,400,000
5/23/2017	St. Luke's-Roosevelt Hospital Center	$387,200
12/28/2017	21st Century Oncology	$2,300,000
2/1/2018	Fresenius Medical Care North America	$3,500,000
2/13/2018	Filefax	$100,000

Total $11,618,200

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include monitoring

Some Best Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members’ critical role in protecting privacy and security

AUDIT

HITECH Audit Program

- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
  - Intended to be non-punitive, but OCR can open a compliance review (for example, if significant concerns are raised during an audit)
  - Learn from Phase 2 in structuring permanent audit program

History

- HITECH legislation: HHS (OCR) shall provide for periodic audits to ensure that covered entities and business associates comply with HIPAA regulations. (Section 13411)

- Pilot phase (2011-2012) – comprehensive, on-site audits of 115 covered entities

- Evaluation of Pilot (2013) – issuance of formal evaluation report of pilot audit program

- Phase 2 (2016-2017) - desk audits of 207 covered entities and business associates

Phase 2 - Selected Desk Audit Provisions

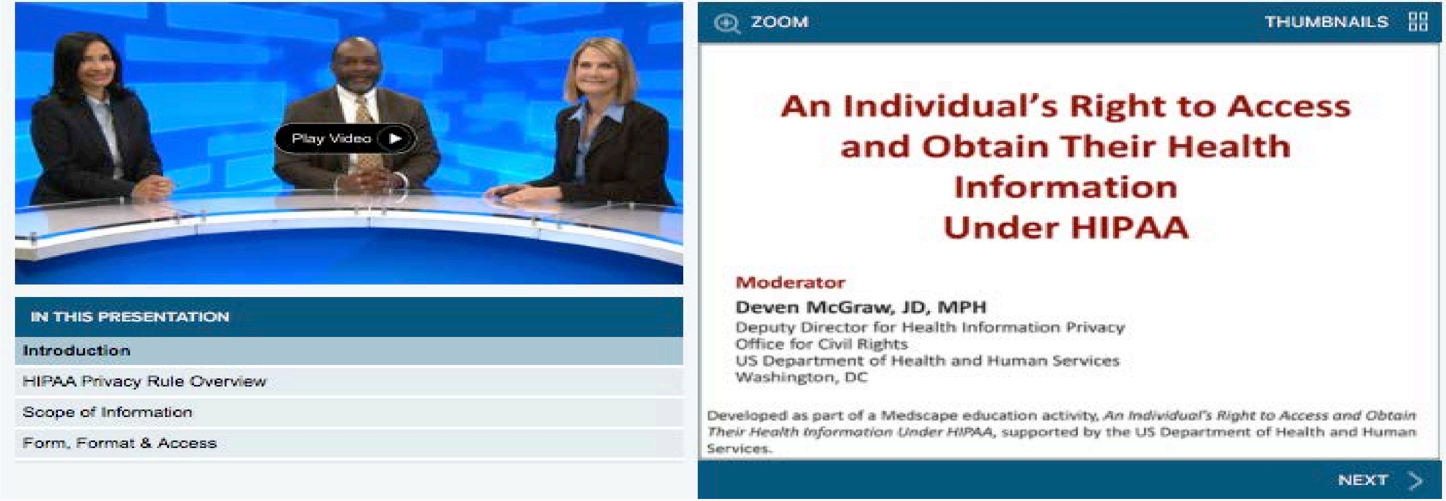
- For Covered Entities:
  - Security Rule: risk analysis and risk management;
  - Breach Notification Rule: content and timeliness of notifications; **or**
  - Privacy Rule: NPP and individual access right
- For Business Associates:
  - Security Rule: risk analysis and risk management **and**
  - Breach Notification Rule: reporting to covered entity
- See auditee protocol guidance for more details: http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

Status

- 166 covered entity and 41 business associate desk audits were completed in December 2017
- Website updates with summary findings will be published in 2018

Provider Education: An Individual's Right to Access and Obtain their Health Information Under HIPAA

Web-based Video Training for Free Continuing Medical Education and Continuing Education Credit for Health Care Professionals via Medscape



An Individual's Right to Access and Obtain Their Health Information Under HIPAA

Moderator
Deven McGraw, JD, MPH
Deputy Director for Health Information Privacy
Office for Civil Rights
US Department of Health and Human Services
Washington, DC

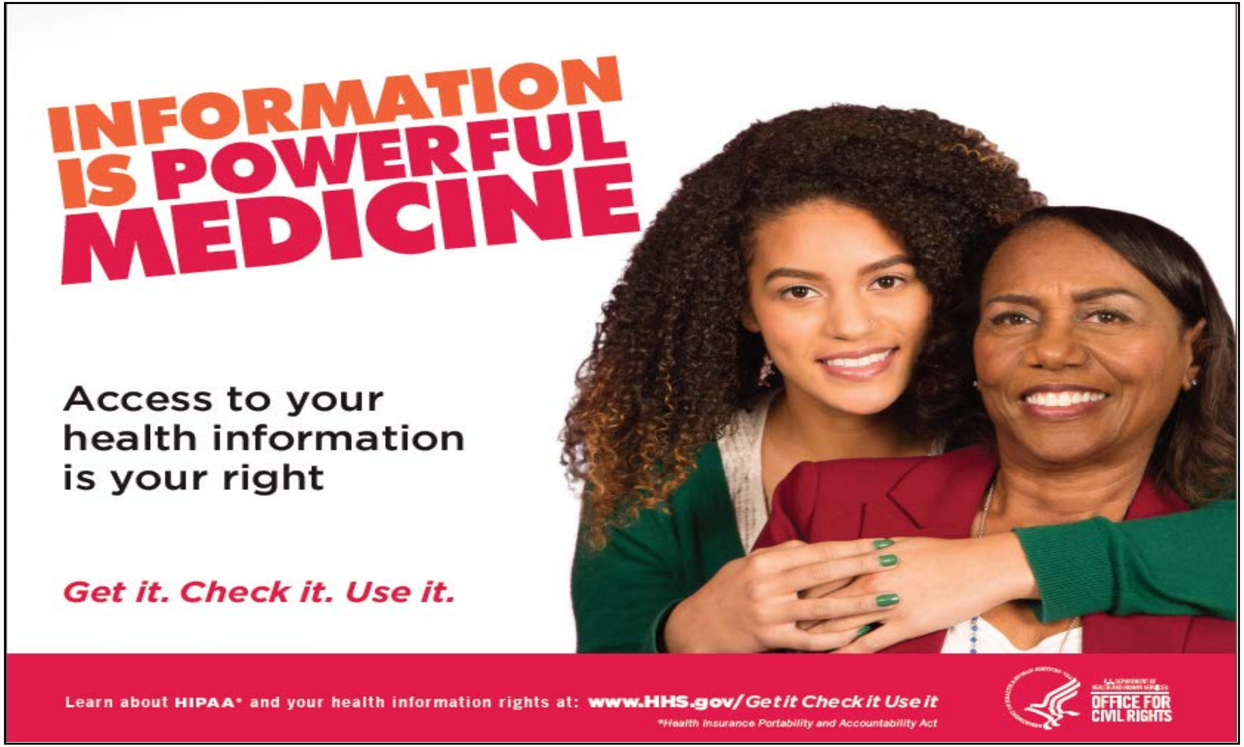
Developed as part of a Medscape education activity, *An Individual's Right to Access and Obtain Their Health Information Under HIPAA*, supported by the US Department of Health and Human Services.

http://www.medscape.org/viewarticle/876110

Consumer Facing Resources:

Right to Access Your Health Information Under HIPAA

Phase 2 of OCR’s *Information is Powerful Medicine* Campaign



INFORMATION IS POWERFUL MEDICINE

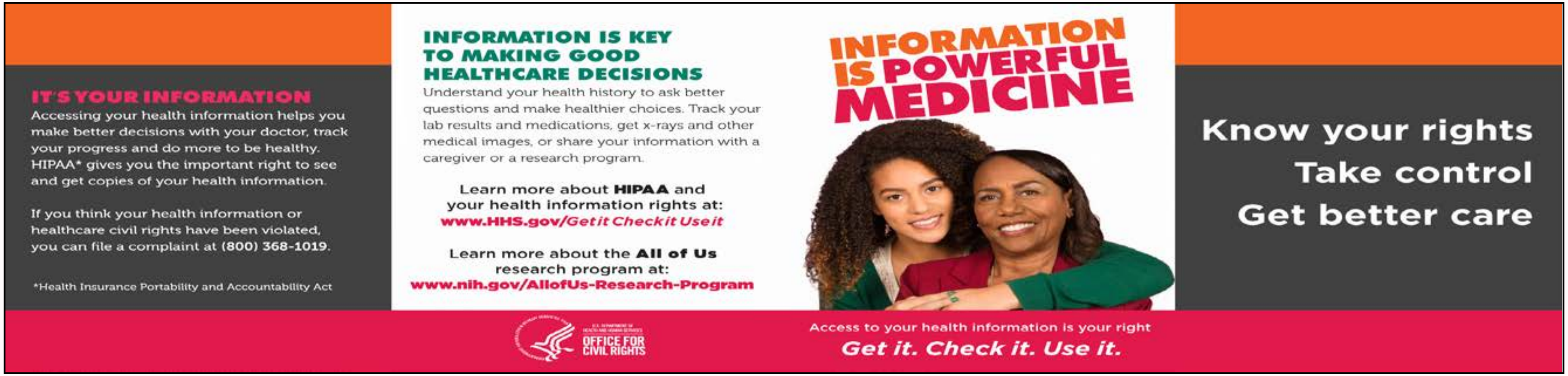
Access to your health information is your right

Get it. Check it. Use it.

Learn about HIPAA* and your health information rights at: **www.HHS.gov/*GetitCheckitUseit***

*Health Insurance Portability and Accountability Act

Pocket Brochure, Exterior and Interior Flap



IT'S YOUR INFORMATION

Accessing your health information helps you make better decisions with your doctor, track your progress and do more to be healthy. HIPAA* gives you the important right to see and get copies of your health information.

If you think your health information or healthcare civil rights have been violated, you can file a complaint at (800) 368-1019.

*Health Insurance Portability and Accountability Act

INFORMATION IS KEY TO MAKING GOOD HEALTHCARE DECISIONS

Understand your health history to ask better questions and make healthier choices. Track your lab results and medications, get x-rays and other medical images, or share your information with a caregiver or a research program.

Learn more about **HIPAA** and your health information rights at:
www.HHS.gov/*Getit Checkit Useit*

Learn more about the **All of Us** research program at:
www.nih.gov/AllofUs-Research-Program

INFORMATION IS POWERFUL MEDICINE

Know your rights
Take control
Get better care

OFFICE FOR CIVIL RIGHTS

Access to your health information is your right
Get it. Check it. Use it.

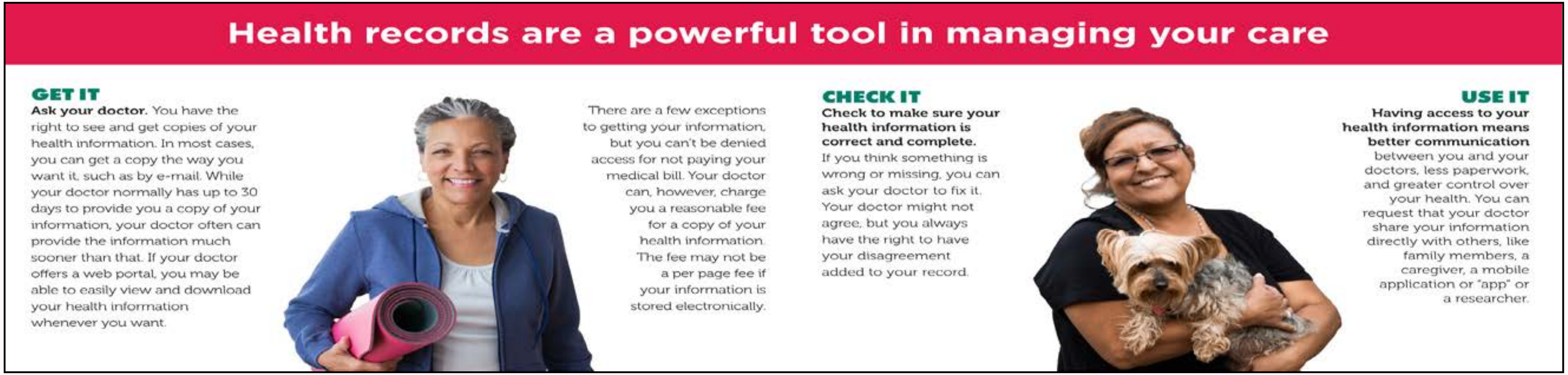
Information is key to making good health care decisions. Understand your health history to ask better questions and make healthier choices. Track your lab results and medications, get x-rays and other medical images, or share your information with a caregiver or a research program.

POCKET BROCHURE

IT'S YOUR INFORMATION

Know your rights
Take control
Get better care

Pocket Brochure Interior View



Health records are a powerful tool in managing your care

GET IT

Ask your doctor. You have the right to see and get copies of your health information. In most cases, you can get a copy the way you want it, such as by e-mail. While your doctor normally has up to 30 days to provide you a copy of your information, your doctor often can provide the information much sooner than that. If your doctor offers a web portal, you may be able to easily view and download your health information whenever you want.

There are a few exceptions to getting your information, but you can't be denied access for not paying your medical bill. Your doctor can, however, charge you a reasonable fee for a copy of your health information. The fee may not be a per page fee if your information is stored electronically.

CHECK IT

Check to make sure your health information is correct and complete. If you think something is wrong or missing, you can ask your doctor to fix it. Your doctor might not agree, but you always have the right to have your disagreement added to your record.

USE IT

Having access to your health information means better communication between you and your doctors, less paperwork, and greater control over your health. You can request that your doctor share your information directly with others, like family members, a caregiver, a mobile application or "app" or a researcher.

Clear and concise

- **Get it:** Covers Form and Format and Manner of Access, Time and Timeliness, Fees
- **Check it:** Check to make sure your health information is correct and complete
- **Use it:** Right to Third Party Access, including a researcher.

HHS.gov
Health Information Privacy

I'm looking for...

INFORMATION IS POWERFUL MEDICINE

Access to your health information is your right

Get it. Check it. Use it.

ACCESS TO YOUR HEALTH INFORMATION IS YOUR RIGHT.

[illegible]

Know your rights. Take control. Get better care.

GET IT

[illegible]

CHECK IT

[illegible]

USE IT

[illegible]

Health records are a powerful tool in managing your care.

INFORMATION IS KEY TO MAKING GOOD HEALTHCARE DECISIONS

[illegible]

KNOW YOUR RIGHTS

[illegible]

LEARN MORE

[illegible]

CAMPAIGN RESOURCES

POCKET BROCHURE

Know your rights
Take control
Get better care

POSTER

INFORMATION IS POWERFUL MEDICINE

WEB BANNERS

INFORMATION IS POWERFUL MEDICINE

HHS.gov/GetItCheckItUseIt

Clear and concise

- Links to Fact Sheets and FAQs
- Videos
- Poster
- Brochure
- Digital Ads and Banners
- Mobile Platform
- Link to Join All of Us Research Initiative

More Information

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr