



HIPAA Privacy & Security in Nursing Homes

Presenter: Susan Clarke, BSc, Health Care Information Security and Privacy Practitioner

Thursday, August 18, 2016

2:00 to 3:00 PM MDT • 12:00 to 1:00 PM AKDT • 10:00 to 11:00 AM HST

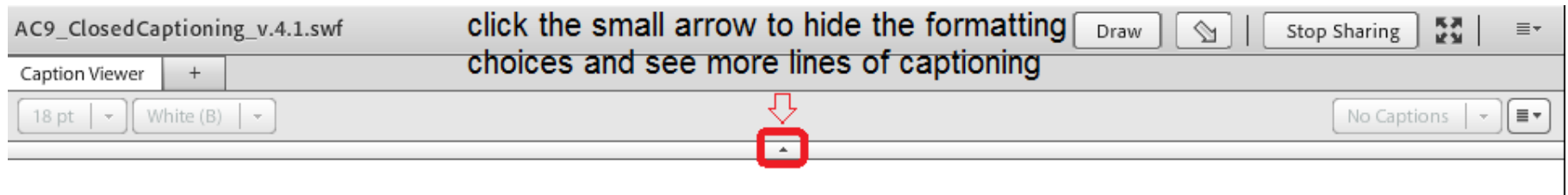
HTS, a department of Mountain-Pacific Quality
Health Foundation

Welcome

- Thank you for spending your valuable time with us today.
- This webinar will be recorded for your convenience.
- A copy of today's presentation and the webinar recording will be available on our website. A link to these resources will be emailed to you following the webinar.
- All phones will be muted during the presentation and unmuted during the Q&A session. Computer users can use the chat box to ask questions which will be answered at the end of the presentation.
- We would greatly appreciate your providing us feedback by completing the survey at the end of the webinar today.

Closed Captioning

- Closed captioning will appear under today's presentation. To see more lines of captioned text, click the small arrow below.





- Mountain-Pacific holds the Centers for Medicare & Medicaid Services (CMS) Quality Innovation Network–Quality Improvement Organization (QIN–QIO) contract for the states of Montana, Wyoming, Alaska and Hawaii, providing quality improvement assistance.
- HTS, a department of Mountain-Pacific, has assisted 1480 providers and 50 Critical Access Hospitals to reach Meaningful Use. We also assist healthcare facilities with utilizing Health Information Technology (HIT) to improve health care, quality, efficiency and outcomes.



- HealthInsight holds the Centers for Medicare & Medicaid Services (CMS) Quality Innovation Network Quality Improvement Organization (QIN-QIO) contract for Nevada, New Mexico, Oregon and Utah; and also holds the CMS end-stage renal disease (ESRD) contract for Networks 16 and 18, serving Alaska, Idaho, Montana, Oregon, Washington and Southern California.
- As a Regional Extension Center (REC), HealthInsight has assisted 1,976 providers and 30 critical access hospitals in Nevada and Utah adopt electronic health record (EHR) technology. The REC also assisted more than 1,400 providers in meeting Meaningful Use Stage 1.

Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter(s)' opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users individual needs.

Session Presenter

Susan Clarke, BSc, Health Care Information
Security and Privacy Practitioner



Acronyms...

- BA: Business Associate
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CEO: Chief Executive Officer
- CIO: Chief Information Officer
- CMS: Centers for Medicare and Medicaid Services
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- HHS: Department of Health and Human Services
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- IT: Information Technology

...and more acronyms

- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- ONC: Office of the National Coordinator
- PHI: Protected Health Information
- SP: Special Publication
- SRA: Security Risk Analysis

Session Overview

- Risks associated with social media, photo, video and abuse policies
- Covered entity, business associate and hybrid facilities
- Understanding the requirements of a HIPAA security risk analysis
- Culture of compliance and risk management planning
- Social Media and acceptable use

Call to Action—August 8



CHUCK GRASSLEY

UNITED STATES SENATOR for IOWA

[Home](#) | [Calendar](#) | [Contact](#) | [E-Newslett](#)

[f](#) [t](#) [i](#) [c](#)

[ABOUT GRASSLEY](#) | [EXPLORE IOWA](#) | [CONSTITUENT SERVICES](#) | [ISSUES & LEGISLATION](#) | [NEWS CENTER](#) | [STUDENTS](#) | [CONTACT](#)

[Home](#) » [News Center](#) » [News Releases](#)

[News Releases](#)

[Commentary](#)

[Events](#)

[Photo Galleries](#)

[Video](#)

[Audio](#)

[Social Media](#)

[Official Photo](#)

[Communications Staff](#)

[Judiciary Committee](#)

After Grassley Call to Action, Federal Agency Spells Out Nursing Home Obligations on Social Media Exploitation of Residents

Aug 08, 2016

Sen. Chuck Grassley is pursuing solutions to the problem of humiliating social media posts of nursing home residents by nursing home workers. The news outlet ProPublica has documented 47 incidents across the country since 2012 in which nursing home workers posted such photos of nursing home residents on social media. Three of the incidents were in Iowa – in Johnston, Ames and Hubbard.

Since Grassley became involved, the leading nursing home industry association responded to his letter and put out detailed guidance to its members about the social media abuse problem. The inspector general of the Department of Health and Human Services alerted 50 State Medicaid Fraud Control Units to be increasingly aware of the problem and investigate allegations accordingly. The Justice Department expressed concern, noting that protecting seniors from abuse is one of its highest priorities. Facebook, Instagram and Snapchat also expressed concern.

Now, in perhaps the most significant development yet, the Centers for Medicare and Medicaid Services put out a detailed [memo](#) to nursing home safety inspectors explaining that social media exploitation is a prohibited form of abuse. Grassley made the following comment.

"This guidance is welcome and necessary. Nursing homes are obligated under the law to keep their residents free from abuse. Exploitation on social

11

State Survey Agency Responsibility- Review of Facility Policies & Procedures

30 Days=
Sept 5, 2016 !

Surveyors are expected to take the following actions 30 days after the release of this memorandum. During the next standard survey, whether a Traditional or Quality Indicator Survey (QIS) survey, the survey team **must request and review nursing home policies and procedures related to prohibiting nursing home staff from taking or using photographs or recordings in any manner that would demean or humiliate a resident(s).** This would include using any type of equipment (e.g., cameras, smart phones, and other electronic devices) to take, keep, or distribute photographs and recordings on social media. Survey teams should begin this review for standard surveys, effective immediately and implement this policy until each nursing home has been surveyed for the inclusion and implementation of such policies. During any survey, the survey team may request to see such written policies, as necessary based upon identified concerns and/or complaints.

Source=<https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-16-33.pdf>

Facilities take immediate steps

- Review policies related to the use of social media, including any related disciplinary policies.
- Review and update training materials as necessary to address the use of social media.
- Consider options for raising awareness of the importance of resident privacy and the prohibition of posting resident information or photos on social media sites.
- Awareness can include postings on bulletin board, staff meetings, etc.

IMPORTANT: document compliance.

Technology Benefits

- Enhanced communications for employees, staff, residents and families
- Improved efficiency and documentation
- Enable effective marketing, public and media relations
- Many residents have adopted technology and it can improve quality of life
- Technology has provided non disputable evidence.

More in the News...

HHS Office for Civil Rights in Action



Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to \$660,000 HIPAA Settlement



THE UNITED STATES
DEPARTMENT *of* JUSTICE

en ESPAÑOL



HOME

ABOUT

AGENCIES

BUSINESS

RESOURCE

Home » Office of Public Affairs

JUSTICE NEWS

Department of Justice

Office of Public Affairs

SHARE



FOR IMMEDIATE RELEASE

Friday, July 22, 2016

Three Individuals Charged in \$1 Billion Medicare Fraud and Money Laundering Scheme

The owner of more than 30 Miami-area skilled nursing and assisted living facilities, a hospital administrator and a physician's assistant were charged with conspiracy, obstruction, money laundering and health care fraud in connection with a \$1 billion scheme involving numerous Miami-based health care providers.

Assistant Attorney General Leslie R. Caldwell of the Justice Department's Criminal Division, U.S. Attorney Wifredo A. Ferrer of the Southern District of Florida, Special Agent in Charge George L. Piro of the FBI's Miami Field Office and Special Agent in Charge Shimon R. Richmond of the U.S. Department of Health and Human Services-Office of Inspector General (HHS-OIG) Miami Regional Office made the announcement.

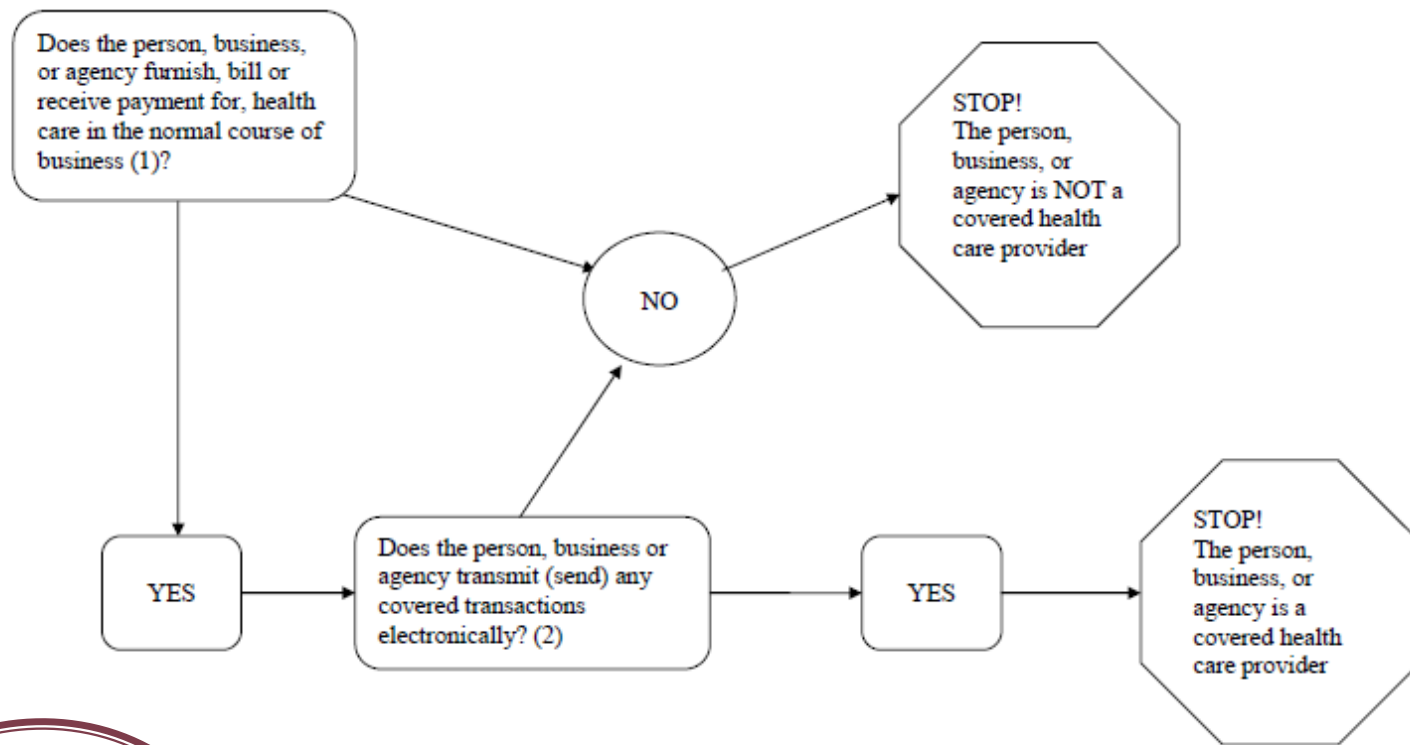
"This is the largest single criminal health care fraud case ever brought against individuals by the Department of Justice, and this is further evidence of how successful data-driven law enforcement has been as a tool in the ongoing fight against health

Care providers manage risk on a daily basis yet security risk management programs are often not as formal as needed.



Organizations need to understand probability over the cost of safeguard and make informed decisions. All systems contain flaws – technology systems are no different.

Are you a Covered Entity (CE)?



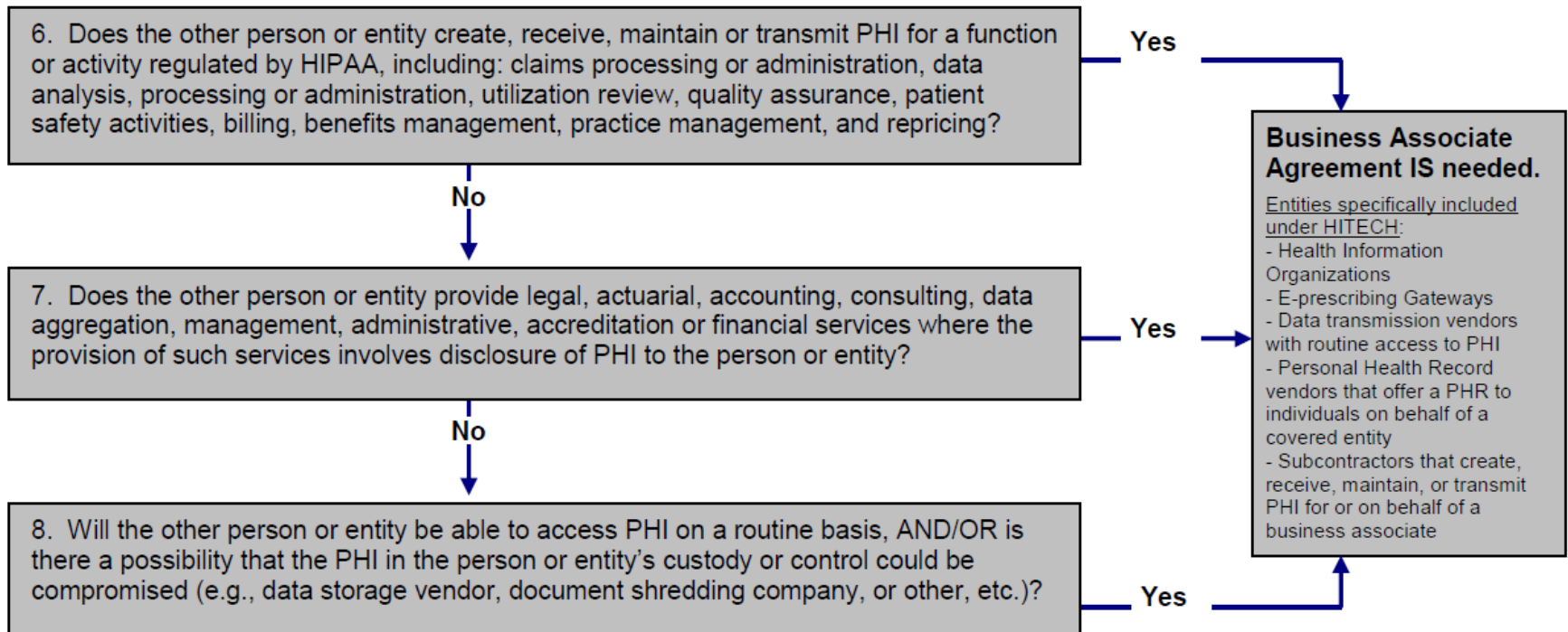
Are you a
CE?
yes/no
/not sure

Healthcare providers that transmit health information electronically using standard transactions are covered entities that **MUST comply with HIPAA.**

Business Associate

- **What Is a “Business Associate?”** A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
- **Business Associate** means an entity that "creates, receives, maintains or transmits protected health information," **in a contractor role with a covered entity**. Subcontractors are also business associates. Examples of business associates are information technology vendors or e-prescribing gateways.


Are you or do you have Business Associates?



What is a Hybrid?

Hybrid Entity – A single legal entity that is a covered entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, nonhealth care components of a hybrid entity may be affected because the health care component is limited in how it can share PHI with the non-health care component. The covered entity also retains certain oversight, compliance, and enforcement responsibilities.

Example: If hospital, nursing home and assisted living facility are one legal entity, then they are a single CE under HIPAA. But if the assisted living facility does not conduct any HIPAA-covered transactions electronically, then the CE has the option of treating itself as a hybrid entity and can choose whether to include the assisted living facility in the healthcare component that is covered under HIPAA



Are you a
hybrid?
yes/no
/not sure

https://privacyruleandresearch.nih.gov/pr_06.asp and HIPAA Briefing Vol 13

HIPAA Review

- Protect the privacy of patient information
- Provide for electronic and physical security of patient health information
- Require “minimum necessary” use and disclosure
- Specify patient rights to approve the access and use of their medical information
- Prevents health care fraud and abuse
- Simplifies billing and other transactions, reducing health care administrative costs

Privacy Rule

- Establishes national standards to protect PHI.
- Applies to **any form of PHI**
- Sets forth requirements to ensure patients' information stays private
- Patient rights

Security Rule

- Establishes national standards to protect individuals' ePHI.
- Apply to **only electronic form** of PHI (ePHI)
- Goal to ensure confidentiality, integrity and availability—CIA triad
- Outlines security safeguards.

Breach Notification Rule requires HIPAA covered entities to notify the Department of Health & Human Services (HHS), affected individuals, and in some cases the media (and business associates to notify covered entities) of breaches of unsecured PHI.

Nicely done HIPAA Basic handbook, 6 pages, link below:

<https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf>

Why Is Privacy Important?

- ✓ People choose to disclose their most intimate information in order to get healthy
- ✓ Care providers earn their trust by guaranteeing privacy
- ✓ Privacy is assured by properly protecting systems and information
- ✓ Breaches undermine patient confidence
- ✓ No confidence and people avoid treatment, lie or omit information, opt-out and potentially get sicker
- ✓ Privacy and security are integral to care

Privacy rule has some flexibility

Privacy rule is somewhat flexible regarding sharing information with family and friends involved in care.

However, other federal and states laws can be more stringent—make sure your facility is compliant for residents in the State that you operate.

If I do not object, can my health care provider share or discuss my health information with my family, friends, or others involved in my care or payment for my care?

Yes. As long as you do not object, your health care provider is allowed to share or discuss your health information with your family, friends, or others involved in your care or payment for your care. Your provider may ask your permission, may tell you he or she plans to discuss the information and give you an opportunity to object, or may decide, using his or her professional judgment, that you do not object. In any of these cases, your health care provider may discuss only the information that the person involved needs to know about your care or payment for your care.

Do I have to give my health care provider written permission to share or discuss my health information with my family members, friends, or others involved in my care or payment for my care?

HIPAA does not require that you give your health care provider written permission. However, your provider may prefer or require that you give written permission. You may want to ask about your provider's requirements.

<http://www.hhs.gov/hipaa/for-individuals/faq/523/can-my-health-care-provider-share-or-discuss-my-health-information-with-my-family/index.html>

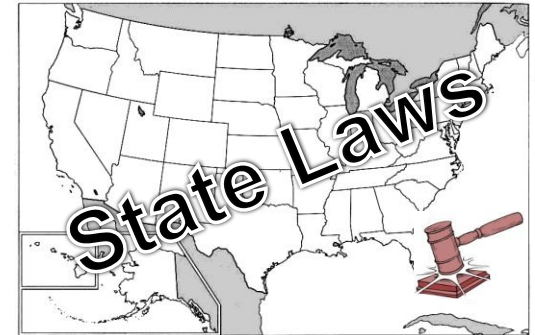


Did you know that the HIPAA privacy rule mandates de-identification in ages over 89 and separates ages into two categories, one below 90 and one ages 90 and above?

Source=<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4765667/>

HIPAA Security Rule requires CE and BAs security measures:

Administrative Safeguards	Physical Safeguards	Technical Safeguards
<p>Establish standards and specifications for your health information security program</p> <p>Examples:</p> <ul style="list-style-type: none">• Security management processes to identify and analyze risks to ePHI• Implementation of security measures to reduce risks• Staff training to ensure knowledge of and compliance with policies and procedures• Information access management to limit access to ePHI• Contingency plan to respond to emergencies or restore lost data	<p>Control physical access to your office and computer systems</p> <p>Examples:</p> <ul style="list-style-type: none">• Facility access controls, such as locks and alarms, to ensure only authorized personnel have access to facilities that house systems and data• Workstation security measures, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users• Workstation use policies to ensure proper access to and use of workstations	<p>Include hardware, software and other technology that limits access to ePHI</p> <p>Examples:</p> <ul style="list-style-type: none">• Access controls to restrict access to ePHI to authorized personnel only• Audit controls to monitor activity on systems containing ePHI• Integrity controls to prevent improper ePHI alteration or destruction• Transmission security measures to protect ePHI when transmitted over an electronic network



Effective Compliance Program

- ✓ Have written policies and standards of conduct.
- ✓ Designated Compliance Officer.
- ✓ Effective training and education.
- ✓ Effective lines of communication.
- ✓ Enforcement of standards through disciplinary guidelines (publicized & enforced).
- ✓ Internal monitoring and auditing.
- ✓ Response and corrective action plan for offenses.
- ✓ Conduct regular risk analysis.

When was
your last risk
analysis
done?

Risk Analysis and Risk Management

Why? Required for HIPAA Covered Entities:

164.308 Administrative safeguards

- Risk Analysis (required)
- Risk Management (required)

How? Conduct a Risk Analysis defined by 45 CFR § 164.308(a)(1)(ii)(A) as, “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the CE or BA”

Risk Analysis and Risk Management

When? HTS recommend conducting security risk analysis yearly or performed as new technology or critical business operations within your organization change.

Where?

HTS offers Security Risk Analysis:

<http://mpqhf.com/corporate/health-and-technology-services/hipaa-privacy-and-security/>

ONC offers a free SRA tools at:

<https://www.healthit.gov/providers-professionals/security-risk-assessment>

Elements of a Risk Analysis

- ✓ Determine the scope of the analysis
- ✓ Gather data
- ✓ Identify potential threats and vulnerabilities
- ✓ Assess current security measures
- ✓ Determine the likelihood of threat occurrence
- ✓ Determine the potential impact of threat occurrence
- ✓ Determine the level of risk
- ✓ Identify measures and finalize documentation
- ✓ Review and update the remediation plan

Do you know your employees?

Insider threat is becoming one of the largest threats to organizations and some cyberattacks may be insider-driven. Although all insider threats are not malicious or intentional, the effect of these threats can be damaging to a Covered Entity and Business Associate and have a negative impact on the confidentiality, integrity, and availability of its ePHI. According to a survey recently conducted by Accenture and HfS Research, 69% of organization representatives surveyed had experienced an insider attempt or success at data theft or corruption. Further, it was reported by a Covered Entity that one of their employees had unauthorized access to 5,400 patient's ePHI for almost 4 years.

Source=Privacy-List listserv, operated by the Office for Civil Rights (OCR)

Social Media/Acceptable use Policy

1. Learn from the Best: CMS website, McKnight's, LeadingAge, National Association of Health Care Assistants (free social media policy for their members). Use google to search on "social media and acceptable use policy" .
2. Work together: Pay attention to how other health care companies address issues related to confidentiality, inappropriate online behavior, social media usage, etc.
3. Involve Staff: Include staff in the development of a social media policy. There is always better "buy in" from staff if they are involved from the very beginning.
4. Be aware of ALL regulatory compliance requirements for your industry.
5. Clearly state that company policies apply to both on- and off-duty use of social networking sites.

Social Media/Acceptable use Policy

6. Extend existing compliance policies to explicitly include the use of social networking sites and other Internet activities
7. Include specific examples of the kinds of statements on social networking sites that could run afoul of HIPAA and other regulations
8. Distribute social networking policies both as a part of employment manuals and separately as stand-alone policies
9. Require employees to acknowledge receiving and reading these policies.
10. Technology changes quickly, stay current and don't be caught in the dark ages.

A parting thought...

Please always remember that checking the box for compliance is important, and protecting the residents and their health records is even more important.

Thanks for your valuable time today.



Mountain–Pacific’s Nursing Home Quality Improvement Leads



Pat Fritz
Wyoming

(307) 568-2797
Pat.Fritz@area-
h.hcqis.org



Leiza Johnson
Alaska

(907) 561-3202
Elizabeth.Johnson@
area-h.hcqis.org



Joy Yadao
Hawaii

(808) 545-2550
Joy.Yadao@area-
h.hcqis.org



Pamela Longmire
Montana

(406) 457-5885
Pamela.Longmire@
area-h.hcqis.org



Mountain-Pacific

Quality Health



Search for:

[Home](#) [Montanans with Medicaid](#) [URx Ask-A-Pharmacist](#) [Health Technology Services](#) [Quality Improvement Organization](#) [Blog](#) [Contact Us](#)



Health Technology Services

You are here: [Home](#) / [Health Technology Services](#)

Health Technology Services

Who We Are

Health Technology Services (HTS) was established in 2010 in response to rapid changes in the U.S. health care delivery system. We are a Trusted Advisor providing expertise to health care entities as they implement new Health Information Technology (HIT) solutions to respond to the mandates and opportunities in the health care industry.

Demonstrating solid expertise in quality outcomes, improved efficiencies and pay for performance, HTS has championed the adoption of HIT to meet these goals.

Who We Serve

HTS works with both provider clinics and hospitals to help manage and align all of your quality program requirements, fully leverage your EHR functionality and data to improve outcomes, simplify and streamline your processes, and maximize your reimbursement opportunities.

HTS Services

HIPAA Privacy and Security

Resources

eClinical Quality Improvement

Webinars and Events

HTS Staff

Contact HTS

PHYSICIANS

Find the latest webinars and info for your clinic on MU, PQRS and more.

HOSPITALS

Find the latest webinars and info for your hospital on MU, PQRS and hospital IQR.

HTS SERVICES

Check out our services to find practical health IT solutions for your facility.

Important Links

Privacy rule:

<http://www.hhs.gov/hipaa/for-professionals/privacy/>

Security rule:

- ▶ <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

Business Associate:

- ▶ <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/businessassociates.html>

Breach Notification Rule:

- ▶ <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/breachnotificationifr.html>

Please let us know if you have questions?

Thought of a question after today's presentation?
Please don't hesitate to [contact HTS](#).



Also...please take just a few minutes to fill out a short survey at the end of our webinar today – we value your comments!

Prepared and presented by:

Susan Clarke, BSc, Health Care Information Security and Privacy Practitioner

HTS, a department of Mountain-Pacific Quality Health Foundation

www.gotohts.com

(cell) 307-248-8179

sclarke@mpqhf.org

