University of California San Francisco

UCSF PRIVACY BEAT

Inside this issue:

Do I Need to Add "Secure:", "ePHI:" or "PHI:" On Internal Emails?

Whether internal email communications require encryption is one of our most frequently asked questions. As you know, HIPAA requires that electronic communications containing Protected Health Information (PHI)* must be transmitted in a manner that protects the confidentiality and security of the information. Simply adding the words (with colon) "SECURE:", "ePHI:", or "PHI:" to the subject line of your email messages will ensure the message is transmitted securely. For example, "SECURE: New Patient Appointment".

Technically, emails transmitted internally (i.e., from one @ucsf.edu email address to another @ucsf.edu email address) do not leave the UCSF network and therefore, do not require the secure email trigger words referenced above. However, the best practice is to send all email messages containing PHI securely. This best practice should be followed, regardless of whether it is sent to an internal or external email address, for these important reasons:

1. If the message is inadvertently routed to a non-UCSF email address, it will land in the UCSF secure email server, from where you can lock the message so that the recipient cannot open it.
2. If the message is forwarded externally by one for your recipients, it will automatically be encrypted and transmitted securely.

By securing your email, you can rest assured that your email is encrypted and that the information contained in your email can only be accessed by the recipients listed. For more information on secure emailing, please contact the IT Service Desk at (415) 514-4100 or visit https://it.ucsf.edu/services/secure-email.

**PHI is individually identifiable health information, and therefore health information containing at least one of the 18 HIPAA identifiers is PHI and must be protected. For additional information, please review the UCSF Privacy and Confidentiality Handbook at http://tiny.ucsf.edu/privacyhandbook.*

Do You Know What Data is Hidden in Your PowerPoint Presentations?

Scenario: You and your colleagues conducted an interesting quality improvement project in your department and would like to share the results of this project with other colleagues within a professional organization to which you belong. As part of this project, you utilized patient-level data in an Excel spreadsheet to create a chart displaying the outcome of your analysis, and copied the chart into a PowerPoint presentation that you later shared with others in your professional organization.

Sound familiar? **This seemingly innocuous practice has been a major privacy risk for UCSF**. Be aware that the charts and graphs within your presentation may contain embedded sensitive data, such as PHI and other sensitive business information. See graphic below. If the file is shared with other individuals, particularly those not affiliated with UCSF, the disclosure may be a privacy breach.

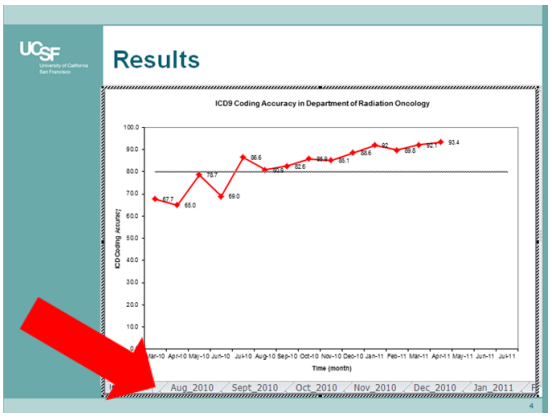


Photo credit: An actual UCSF presentation containing embedded data. Published with author's permission.

What can you do?

The good news is that there is a way to inspect your PowerPoint files for hidden data. Instructions are available on the Microsoft Office website at: https://support.office.com/en-us/article/Remove-hidden-data-and-personal-information-by-inspecting-presentations-b00bf28d-98ca-4e6c-80ad-8f3417f16b58.

Below are some additional best practices for developing presentations for both external and internal audiences:

1. Regardless of the audience, use the minimum amount of information necessary to convey your information. For example, do not include names if they are not necessary.
2. When taking screenshots of PHI, carefully review the image to ensure patients' identifiers (e.g., name, birth date, MRN) are removed or redacted.
3. For external audiences: Only include clinical images for which you have obtained written patient consent for publication. Please remember that some cases may be so unique that they are identifiable even without the subject's identifiers included.
4. For internal audiences: If you absolutely need to provide handouts containing PHI, print your content on colored paper (to easily identify it amongst other non-PHI documents) and collect the documents after your meeting to ensure the hardcopy PHI does not leave the room.

UCSF Privacy Office
3333 California Street,
Suite S1-10G
San Francisco, CA 94118
Box 1922

Phone: (415) 353-2750
Fax: (415) 353-9241
Email:Privacy@ucsf.edu
http://hipaa.ucsf.edu

University of California San Francisco

Kudos Corner—Orthopedic Institute

The Privacy Office is excited to introduce a new segment of our publication called the Kudos Corner. Here, we highlight the departments that have implemented proactive and/or creative efforts to prevent privacy breaches and promote best practices to secure protected health information.

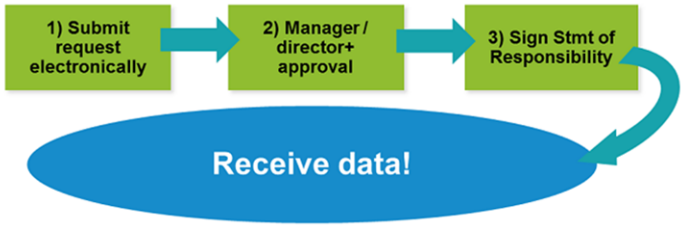
For our inaugural feature, we would like to congratulate the **Orthopaedic Institute (OI) at Mission Bay** on their "HIPAA Breach-Free Days" program. In April 2015, OI Director **Debbie Gee** took inspiration from a visit to a UPS warehouse. Spotting a sign that tracked injury-free days at the location, she reworked the idea for tracking privacy breach-free days by setting milestone targets for her staff.

At 90 days without breaches, staff celebrates with a Root Beer Float Day. At six months without breaches, staff celebrates with a sweet Dessert Social. At nine months, staff celebrates with a luncheon. Other great milestone markers are down the line to incentivize the team and keep everyone motivated to take care when communicating and handling PHI. Debbie expressed that the Orthopaedic Institute "is a very busy practice with over 50,000 visits annually, so if we can be breach-free with all of that activity, I think it is worth it." Thank you to the Orthopaedic Institute and to Debbie for your hard work! For advice on how to develop a program for your own department, contact Debbie.Gee@ucsf.edu.

Pictured above: The Orthopaedic Institute's Spine Department celebrating being breach-free with a root beer float social.

Policy Update: Control of Access

In an effort to improve the security of confidential information in all forms, UCSF Medical Center revised the Control of Access Policy (UCSF MC Policy - 5.01.06). Historically, the policy covered control of access to information for research purposes. It was expanded to cover access to information for research, operations, business, clinical and quality purposes. While the primary purpose of the policy is to help secure the control of access to, and release of, confidential information from UCSF systems, the Medical Center is simultaneously working hard to implement standardized and automated processes to streamline the end-user's experience for requesting data. To do this, the capabilities of Service Now and DocuSign are being leveraged to cover a growing number of clinical and administrative systems and databases that contain restricted information. The policy can be accessed here: http://tiny.ucsf.edu/controlofaccess.



Ultimately, there are three steps for obtaining data:

1. **Request for Information:** The requestor must designate the intended use of the information, source of the data, and the data being requested. This is documented within Service Now.
2. **Approval:** A manager level or above must approve the data request.
3. **Statement of Responsibility:** The user must agree to handle confidential UCSF and patient information securely and responsibly. This is completed via DocuSign.

If you have any questions about complying with the policy or how to ensure data that you've been entrusted with is properly secured, please contact Privacy by emailing Privacy@ucsf.edu.

******Providers******

We are excited to announce that the UCSF Advanced HIPAA Healthcare Provider module has been updated! The module was revised to focus on relevant risks and issues for healthcare providers, such as the use of PHI for teaching and research, complexities relating to patients who are also employees of UCSF, using social media, and handling provider notes. You may access the Advanced HIPAA Healthcare Provider module in the UC Learning Center.

Policy Update: Confidentiality of PHI

UCSF has an updated Privacy and Confidentiality Policy! The policy, called the "Confidentiality, Access, Use, and Disclosure of Protected Health Information and Patient Privacy" covers topics ranging from how UCSF uses patient information, what education UCSF's workforce receives about privacy issues, and the appropriate amount of information to access when conducting activities. The policy also links to other privacy related policies, so it is a good resource for all UCSF workforce members.

Be sure to check out the policy at: http://tiny.ucsf.edu/confidentialitypolicy1.

The UCSF Privacy Office is here for you!

Need help navigating the complex privacy laws? Think you might have a breach and are unsure of what to do next? Do you have a project that involves the exchange of sensitive information? Need a Privacy in-service for your staff? The UCSF Privacy Office can help you with all of these efforts! Please direct your request or question to: Privacy Office Main line: (415) 353-2750; or email: Privacy@ucsf.edu. We would be happy to answer your questions, consult on your project and provide education tailored to your needs.