



ASAPS **webinar**

The American Society for Aesthetic Plastic Surgery



HIPPA and Your Aesthetic Practice – What You Need to Know

Date: February 25th - 5:00 PM Pacific / 8:00 PM Eastern

Duration: 60 mins total - 45 Min Presentation with 15 Min Q&A



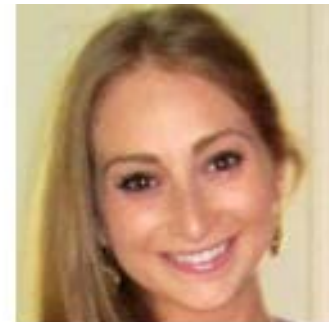
Clyde H. Ishii, MD
Moderator
ASAPS Secretary



Chris Nuland
Attorney
HIPAA Compliance



Bret Heenan
Director of Operations
Etna Interactive



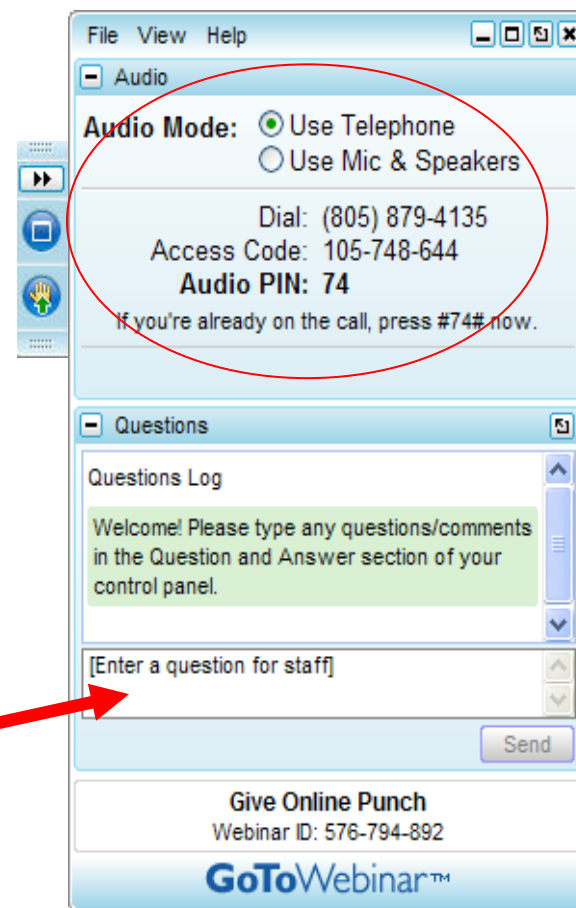
Christina M. Majeed
Chief Product Officer
NexTech Systems

Help with GoToWebinar

Listen to this Webinar on your

- *Computer speakers*
- *Headphones/headset*
- *On the telephone*

**PLEASE ASK QUESTIONS
Throughout the webinar
IN YOUR Question Box**



All ASAPS Webinars are recorded and will be available for download at a later date



ASAPS **webinar**

The American Society for Aesthetic Plastic Surgery



This webinar will provide an overview with the latest updates to HIPAA and identify best practices, challenges and solutions. Learn how to assess and implement the key changes to HIPAA as it relates to:

- Your staff, daily operations and government inquiries
- Website and online marketing – common mistakes and recommendations
- Best practices in the electronic office using Practice Management and EMR



All ASAPS Webinars are recorded and will be available for download at a later date



American Society for Aesthetic Plastic Surgery

WHAT IS HIPAA?

Chris Nuland, Attorney

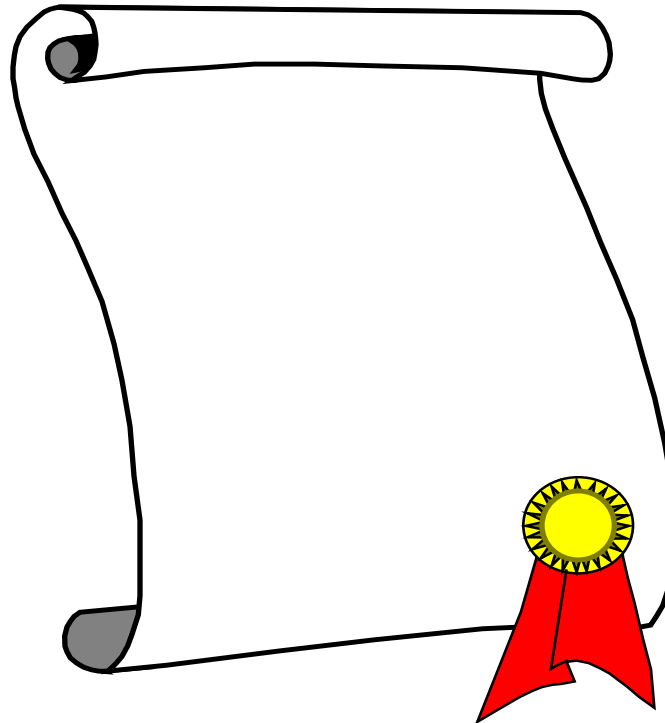
HIPAA Compliance



Jacksonville, FL

What is HIPAA?

- **The Health Insurance Portability and Accountability Act of 1996**



BASIC QUESTIONS AND *ANSWERS*



What Does HIPAA do?

- **Creates national standards to protect individuals' medical records and other protected health information (PHI).**
- **PHI is more than records!! It includes:**
 - **Return to Work Notes**
 - **Patient Lists**
 - **EOBs**

To Whom Does HIPAA Apply?

- **Any physician or practice that submits claims electronically, and/or any Medicare participating practice with more than ten full-time employees.**



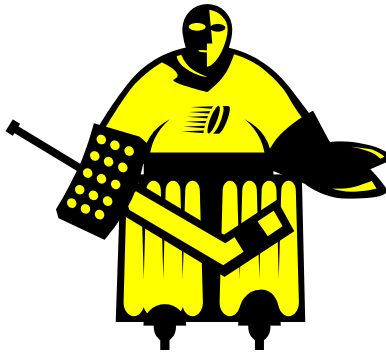
TRANSACTION SETS UPDATE

- **failure to abide by the standard code set rules means your practice may not get paid on any of its electronic claims to Medicare or any third party payor.**

Transaction Code Update

- **universal language for the electronic submission of health care information, and use established standard code sets such as ICD-9 and HCPCS**
- **a letter of HIPAA compliance should be sought from clearinghouses and software manufacturers;**

Privacy Rule



What Must a Physician Do to Comply?

- Provide information to patients concerning their privacy rights.
- Adopt clear, written privacy standards for the practice.
- Train employees.
- Designate a compliance officer
- Secure patient records.

Standard: Treatment and Payment Operations Are Allowed

- **Consent forms should explicitly allow for TPO and:**
- **Consent is necessary for any provider who has a direct patient relationship**
- **Exception for emergency care and indirect providers (labs, etc.)**
- **Physician may refuse to treat patient that refuses to sign a consent form**

*Standard: Disclosures of PHI
must be the minimum necessary
to accomplish the intended
purpose.*

Standard: Physicians must include standards on oral communications in their Policies and Procedures.



Standard: Business Associates

- Physician is not liable for privacy breaches of business associate if the physician has obtained "satisfactory assurances" of compliance from associate.
- "Business Associates" include all persons who may have physical access to PHI. They include contracted billing and collection personnel, accountants, janitorial companies, and sales representatives if they are given access to parts of the office in which medical records are maintained.
- Business Associates must agree to be bound by HIPAA, protect the integrity of the data they receive, alert the Practice of any breaches, and work with the Practice to mitigate any such breaches. Under HITECH, Business Associates must also agree to disclose and mitigate any breaches.
- Business Associates are now directly responsible for complying with Privacy and Security Regulations

Standard: Only the parent or legal guardian of child has right to access records.



Standard: Any use of PHI for fundraising or marketing must be specifically authorized by patient.

Policies and Procedures

All marketing involving PHI must be approved by the HIPAA Compliance Officer, who must ensure that all appropriate consents have been executed.

Standard: Use of PHI for research is allowed so long as identifiable health information is redacted.

Standard: Medicare and Medicaid must comply with the new requirements.

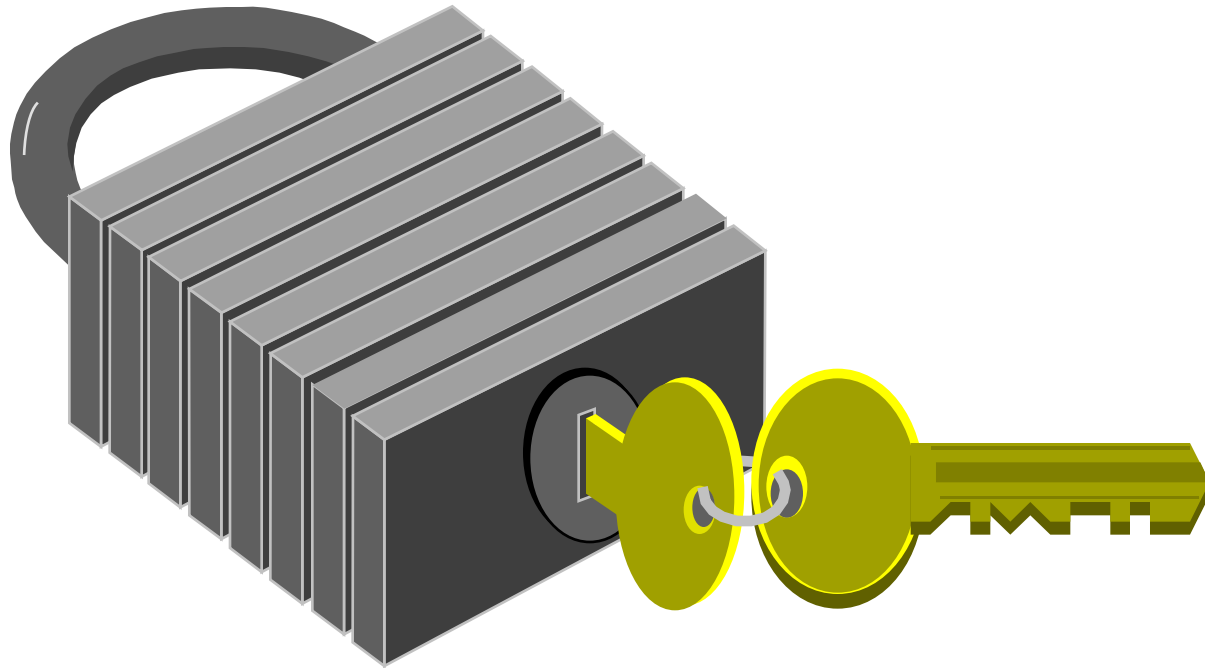
Office of Civil Rights may require records "pertinent to ascertaining compliance" with the Rule.

Policies and Procedures:

All government requests for HIPAA records must be approved by the HIPAA Compliance Officer;

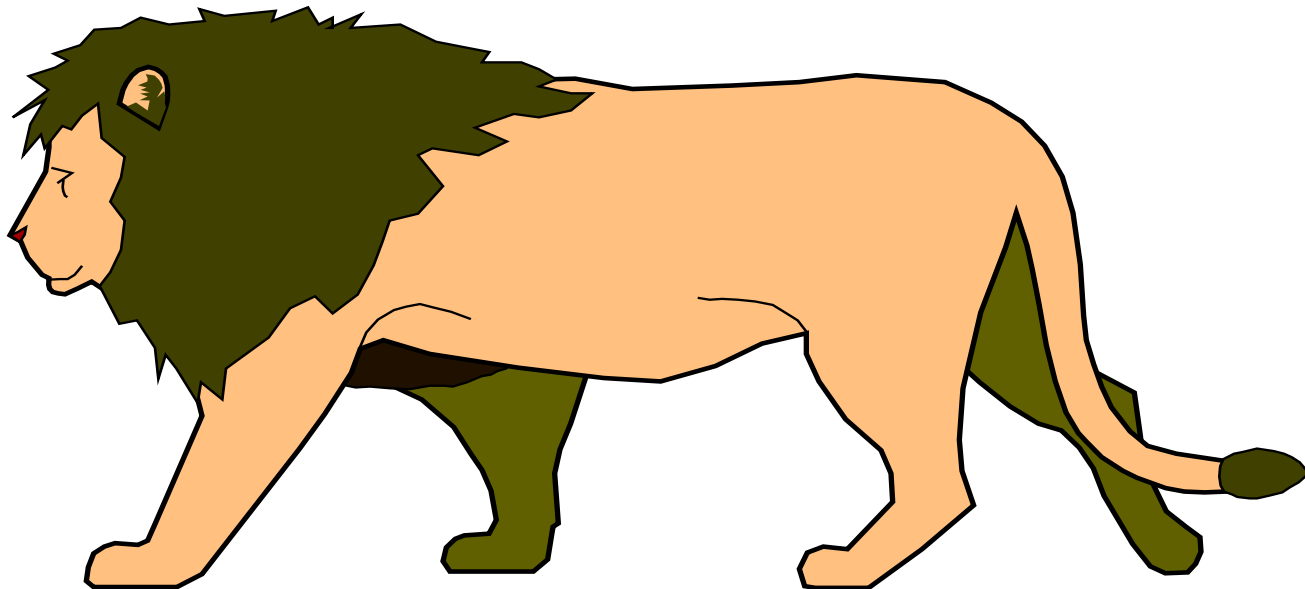
Attendance Logs of all HIPAA training sessions will be maintained for at least six (6) years and made available to the Office of Civil Rights upon request.

HIPAA SECURITY RULE



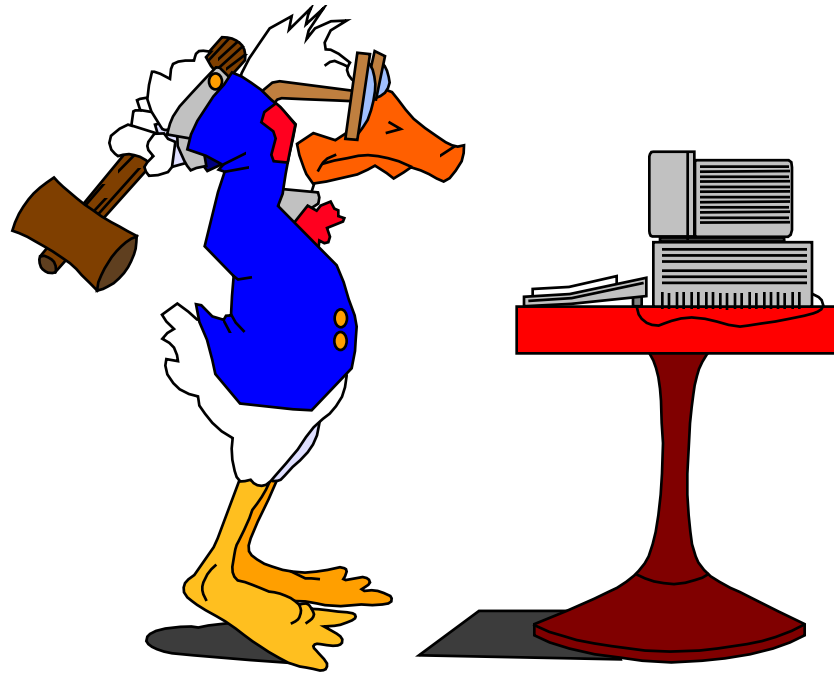
Basic Elements

- **“Reasonable” is key word**
- **Privacy Officer Can be Security Officer**



18 standards

- **Most are similar to Privacy Rule**



Administrative Safeguards

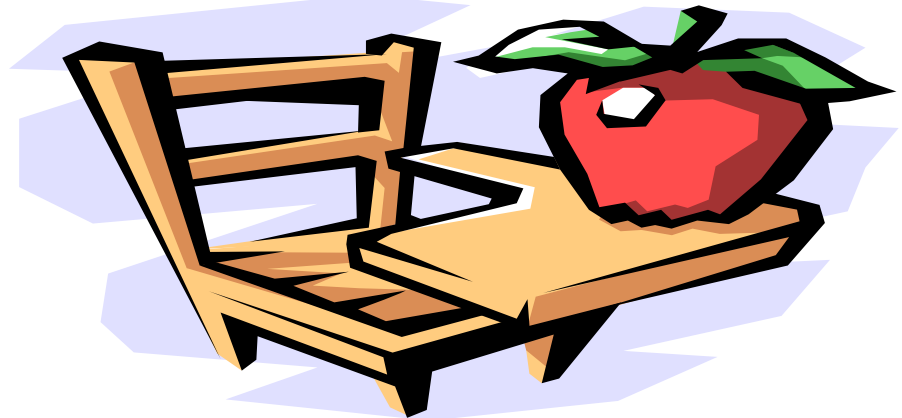
- **Security Management Process Standard:**
 - risk analysis
 - risk management
 - a sanction policy,
 - information system review.
 - For small offices, these steps may be taken internally, and do not require the engagement of so-called HIPAA experts.

Administrative Safeguards

- **Assigned Security Responsibility Standard:** A HIPAA Security Officer must be named, who may be the same person as the HIPAA Privacy Officer.
- **Workforce Security Standard:** The practice must determine who should have access to PHI and under what circumstances, and must ensure that such access is terminated upon termination of an employment. Only those staff members with a need to have access to PHI for a specific purpose will be allowed access to PHI.

Administrative Safeguards

- **Information Access Management Standard:**
Likewise, offices must have policies and procedures as to how authorized persons may access information, such as passwords for electronic information.
- **Security Awareness and Training Standard:**
All staff must be trained in the new security standard.



Administrative Safeguards

- **Security Incident Procedures Standard:** The office must have policies and procedures to deal with unauthorized disclosures; must require identification and response to unauthorized disclosures, mitigation of harmful effects, and document the incidents and their outcomes.
- **Contingency Plan Standard:** Likewise, the office must have policies to deal with the sudden loss of PHI through data backup, an emergency plan, and testing and revision procedures.

Administrative Safeguards

- **Evaluation Standard:** Periodic evaluation to determine if Practice is in compliance with the Security Regulations.
- **Business Associates Standard:** As in the Privacy Rule, Business Associates must guarantee that they will provide security for PHI. The Business Associate Letter incorporated into this Manual is designed to meet this requirement.

Physical Safeguards



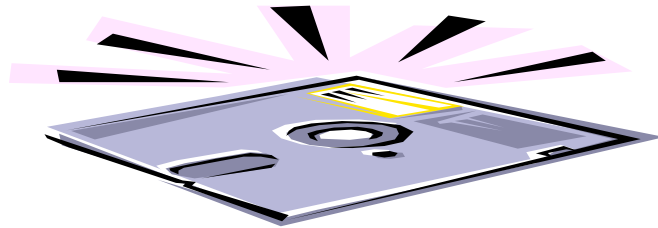
- **Facility Access Controls Standard:** The covered entity must have policies and procedures to control access to PHI and the facility itself.
- **Workstation Use Standard:** Covered entities must have policies and procedures detailing what may or may not be done at a workstation. For instance, a ban on using the internet for personal use may be appropriate.

Physical Safeguards

- **Workstation Security Standard:** Policies and procedures must be developed and implemented to ensure that only authorized employees have access to workstations. Physical barriers (such as doors and locks) and passwords are tools to comply with this requirement.

Physical Safeguards

- **Device and Media Controls Standard:** Offices must have policies to ensure that hardware, software, and media storage (e.g., floppy disks) are erased before being disposed, reused or leaving the building. This Practice will not dispose of any media storage vehicle without first erasing all data from the vehicle.



Technical Safeguards

- **Access Control Standard:** Access to electronic PHI must be restricted by office policies, which include unique user identification and emergency access procedures.
- **Audit Controls Standard:** The actual systems that house PHI must be audited/inspected periodically to ensure the integrity of electronic PHI.

Technical Safeguards

- **Integrity Standard:** Policies and Procedures must be in place to ensure that electronic PHI cannot be inappropriately altered or destroyed.
- **Person or Entity Authentication Standard:** A mechanism must be in place to authenticate the identity of those who gain access to electronic PHI. Passwords are a typical form of authentication.

Technical Safeguards

- **Transmission Security Safeguard:**

Covered entities must take steps to minimize the chance of unauthorized access to electronic transmissions of PHI. Business Associate Agreements and routine audits are to be used to accomplish this goal.

Unique Provider Identification Number (NPI)

- **Now Available from CMS.**
- **Information Publicly Available**

2013 CHANGES- IMPLEMENTATION REQUIRED BY SEPTEMBER 22, 2013

- **FINES INCREASED TO UP TO
\$1,500,000**



GOT YOUR ATTENTION?

- **Business Associates are directly responsible for complying with Privacy and Security Regulations**
- **Patients may request their records electronically**
- **Patients may withhold permission to send PHI to insurers if patients paid in full themselves.**

REPORTING

- **COVERED ENTITIES MUST NOW REPORT ALL BREACHES BY END OF CALENDAR YEAR IN WHICH THEY OCCUR.**



Chris Nuland, Attorney
HIPAA Compliance
Jacksonville, FL

THANK YOU!



American Society for Aesthetic Plastic Surgery

HIPAA BEST PRACTICES ELECTRONIC OFFICE

Christina M. Majeed, M.S. – Chief Product Officer
NexTech



Tampa, FL

HIPAA Best Practices Electronic Office

Christina M. Majeed, M.S.
NexTech Chief Product Officer
February 25, 2013

A Little About Your Speaker

- With NexTech since 1997, Chief Product Officer
- Master's degree from Columbia University in Technology Management
- Led the design, development and implementation of the NexTech EMR for Plastic Surgery and Dermatology
- Led the design, development and launch of NexTech's patented iPad app, and awarded 3 design patents on the application
- Grew the EMR department from a team of 1 to a team of 20, oversaw a development team of 30, as well as lead the NexTech marketing team
- Responsible for key partnerships, business development, and new products for NexTech's specialty markets of over 4,000 doctors

Agenda

Business Owner/ Private Practice Perspective Best Practices:

1. The 4 Items Must Have In Place Event of HIPAA Audit
2. Practice Management and Patient PHI
3. Electronic Medical Records and Patient PHI
4. You Breached...What to do

Best Practices – The 4 Items

1. Business Associate Agreement Signed per Sept. 23 Omnibus Rule
 - Covered Entity = Your Practice
 - Business Associate = Your PM/ EMR Company, Marketing Company, and any company that could see or have access to patient protected health information.

Best Practices – The 4 Items

2. Documented Risk Analysis and Mitigation Plan

- 23 core areas
- Ongoing efforts to minimize risk
- Self-audits/ consultant auditing services

Best Practices – The 4 Items

3. Documented Privacy and Security Policies and Procedures
 - Handbook format incase you get audited or have a breach
 - All employees receive and sign copy
 - Updated yearly

Best Practices – The 4 Items

4. Documented Internal HIPAA Privacy and Security Staff Training
 - What patients need to sign
 - What staff can send and not send as it relates to patient PHI
 - How staff should operate with business associates and patient PHI
 - How staff should operate with patients in front of other patients

Best Practices – PM & PHI

Patient communications within and outside the office:

- Appointment reminders
- Email marketing and reminders
- Surgery schedule on phone – default settings protected PHI
- Office texting you regarding patients, initials vs. full name
- Discussing patient interactions over dinner at a restaurant, etc.
- Discussing patient interactions in office other patients can hear
- Advertising high profile patients and services rendered
- Social media and patient PHI
- Protecting credit card information (PCI compliance)
- Technology certified and encrypted (CCHIT/ ONC Security)

Best Practices – EMR & PHI

Patient access and storage of EMR Data:

- Patient portal and online medical history forms SSL encryption
- Summary of chart accessible to patients ONC 2014 Stage 2 Meaningful Use
- Discussing patient interactions over dinner at a restaurant, etc.
- Discussing patient interactions in office other patients can hear
- Patient photos on iPhone's, iPad's vs. inside the EMR
- Lose device – data not stored on the device but in the software
- Technology certified and encrypted (CCHIT/ ONC Security)
- Faxing over patient chart examples to your business associates

Best Practices – You Breached...

You Breached...What to Do...

Best Practices – You Breached...

Audited, you have a breach, what do you do now...

- Must show 4 areas were covered ahead to minimize the fine
 1. BAA in place
 2. Documented risk analysis and mitigation plan
 3. Documented privacy and security policies and procedures
 4. Documented internal HIPAA staff training
- Shrewd engage HIPAA attorney before audit, prudent especially after audit
- May need to notify patients, HHS, and possibly even media if information compromised
- Fines can range \$100 per violation to 50K per violation with a max fine 1.5M for willful misconduct; State Attorney enforce HIPAA violations with injunctions and civil damages.

Summary

1. The 4 Items Must Have In Place Event HIPAA Audit
 - BAA
 - Documented Risk Analysis and Plan
 - HIPAA Handbook
 - Documented Staff Training
2. Practice Management and Patient PHI
3. EMR and Patient PHI
 - Thoughtful approach for both
4. You Breached...What to do
 - Document, document, document well ahead of time before a breach and CALL HIPAA ATTORNEY

Best Practices – You Breached...

You Breached...What to Do...

Best Practices – You Breached...

Were audited, you have a breach, what do you do now...

- Must show 4 areas were covered ahead to minimize the fine
 1. BAA in place
 2. Documented risk analysis and mitigation plan
 3. Documented privacy and security policies and procedures
 4. Documented internal HIPAA staff training
- Shrewd engage HIPAA attorney before audit, prudent especially after audit
- May need to notify patients, HHS, and possibly even media if information compromised
- Fines can range \$100 per violation to 50K per violate, with a max fine 1.5M for willful misconduct; State Attorney enforce HIPAA violations with injunctions and civil damages.



Christina M. Majeed, M.S. – Chief Product Officer
NexTech
Tampa, FL

THANK YOU!



American Society for Aesthetic Plastic Surgery

HIPAA & YOUR ONLINE MARKETING?

Bret Heenan, Director of Operations

Etna Interactive



San Luis Obispo, CA

HIPAA & Your Online Marketing

Bret Heenan

Director of Operations | Etna Interactive

Your presenter.

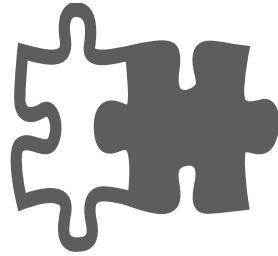
- 25 years in software and system engineering
- A decade in aesthetic medicine
- Experienced in software security, encryption, and operational implications of HIPAA

About this presentation.

- Online marketing and HIPAA
- Common HIPAA mistakes online – and how to avoid them
- Specific recommendations for your site and email communications

Housekeeping.


- Applicable for US-based, HIPAA-covered entities
- Our focus is on communications originating from your site and social media (not on 3rd party sites)
- This is not legal advice, please consult your counsel



Fitting your **website and online marketing** into your compliance plans.

Small part, **big vulnerability.**

- Website and email changes are a small piece of HIPAA compliance, the vulnerability is in how you behave
- Compliance = technical + operational + behavioral changes
- Make a good faith effort to protect patient information, provide notice, secure consent, review compliance and report breaches
- Consult your counsel for more guidance



Breaking trust: mistakes often stem from misunderstandings.

Make sure you and your staff understand.

- What to protect: PHI and privacy
- Who to protect: existing patients AND prospects
- Where to protect: Website form submissions, uploads, emails, text messages, social posts



Secure messaging and
prospective patients.

To **encrypt** or not?

- Enrolling prospects in secure messaging will deter inquiries
- Disclosing risks and securing consent should cover initial inquiry
- Encryption is essential for PHI-laden messages and patient care



HIPAA and **social media.**

Social media communications are covered by HIPAA.

- Patient posts do NOT imply consent
- Never violate privacy or post PHI

SPECIFIC **RECOMMENDATIONS**

Policy recommendations.

- Publish HIPAA & Privacy policies to your site
- Require patients to accept terms and conditions of unsecure email on Web forms
- Use email signatures to notify patients of email risks
- Secure specific HIPAA releases in office
- Execute business associate agreements (BAAs) with partners

Practical recommendations.

- Train, re-train and monitor staff when handling ePHI
- Include minimal ePHI in electronic communications
- Get off of electronic media quickly
- Consider a secure messaging solution
- Follow best practices for accessing, storing and printing records
- Periodically audit your online activities and document findings



Always consult your HIPAA
advisor when setting policy.

Want to Learn More?

- Subscribe to our newsletter
www.etnainteractive.com/newsletter

Thank you.



Bret Heenan, Director of Operations
Etna Interactive
San Luis Obispo, CA

THANK YOU!



American Society for Aesthetic Plastic Surgery

Q&A



WE ARE AESTHETICS

For more information about membership or the candidate program, please contact Alicia Potochniak at Alicia@surgery.org

<http://www.surgery.org/professionals/membership>



THE AMERICAN SOCIETY FOR
AESTHETIC PLASTIC SURGERY, INC.



THE AESTHETIC SURGERY EDUCATION
AND RESEARCH FOUNDATION

The Aesthetic Meeting 2014

San Francisco

BUILDING THE BRIDGE
BETWEEN SCIENCE AND ART

April 24–29

Moscone Center



www.surgery.org/meeting2014

Registration Begins December 2013

