Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

Industry leading Education

- Today's Webinar
  - **Want an Ironclad HIPAA Defense?**
- Upcoming Webinars
  - **The Relationship Between HIPAA Compliance and Business Associates**
    - Thursday, July 21st 2PM ET

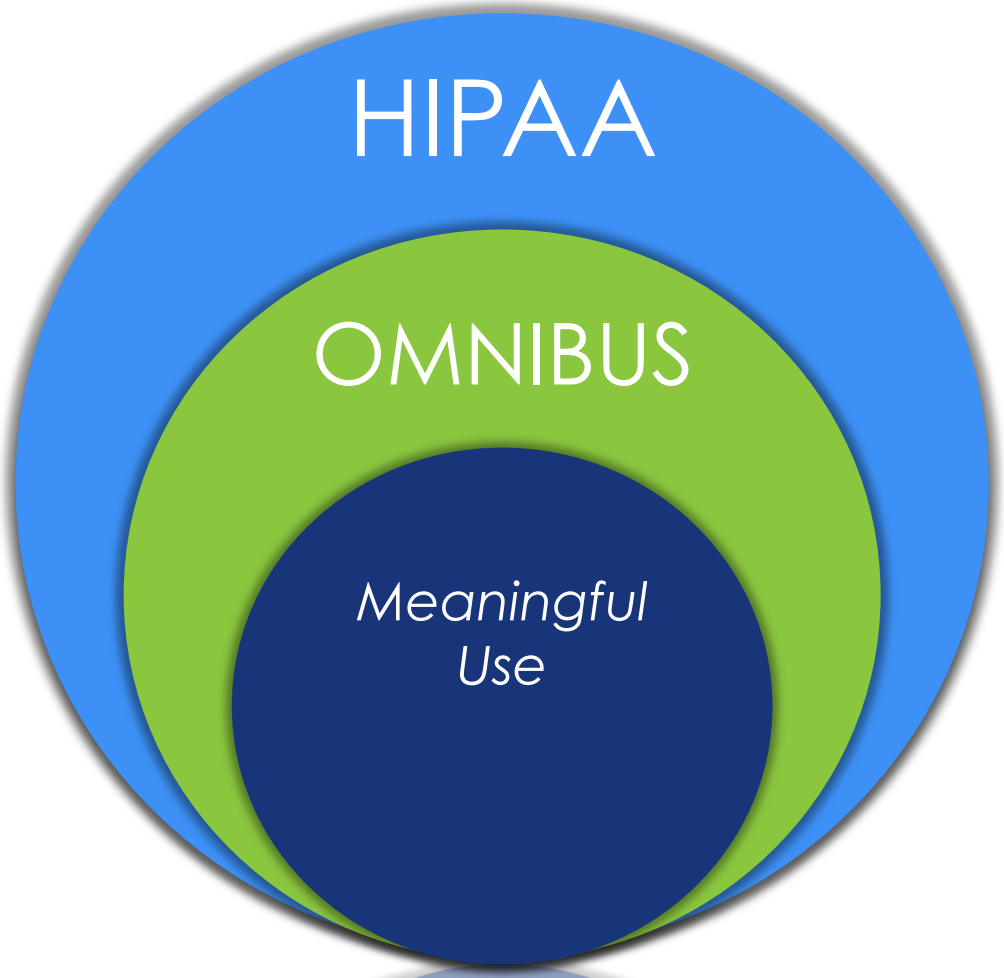
BRIGHTSQUID

For Today

- Please ask questions!
- Upcoming & past webinars: http://compliancy-group.com/webinar/

What is HIPAA?

- HIPAA / HITECH
  - Protect patient confidentiality while furthering innovation and patient care
- Omnibus
  - Business Associates must protect PHI
- Meaningful Use
  - Accelerate adoption of EHR (electronic Health records)
- Compliance vs. Security
  - Fines vs. Risk



- Mark Eyre
  - Brightsquid Dental Link – Director of Customer Operations

- Over 15 years in Technology, Communications and Internet Collaboration
  - Remote access services
  - Financial Services
  - IT Services Consulting
  - Compliance consulting
  - HIPAA Awareness for Business

What is Brightsquid Secure-Mail™

Secure-Mail™ is the compliant messaging system designed to enable dentists, specialists and labs to easily and safely share private patient information.

Founded in 2008 by a Pediatric Radiologist who wanted to safely share images containing private patient data with consulting colleagues around the world.

Because of the service's roots in radiology, Brightsquid Secure-Mail enables the exchange of protected health information and large files while adhering to the most restrictive privacy laws in the world.

The Difference Between Compliance And Security

In the eyes of the law, security is one component of compliance.

- Compliance - Your practice must comply with government regulations. Which include:
  - Security
    - Levels of data ‘obscurity’ that makes access extremely difficult.
    - Encryption – data at rest and in motion.
  - Consent
  - Audit
  - Backup
  - Archive
  - More and more and more…

Protected Health Information

All patient information is considered equal. There is no such thing as "non-sensitive" patient information.

Any information about health status, provision of health care, or payment for health care held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral that can be linked to a specific individual.

- Names
- All geographical identifiers smaller than a state
- Dates (other than year) directly related to an individual (DOB, DOD, Appointment Dates etc…)
- Phone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger, retinal and dental records
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic

All Medical Information Must be Protected

Mr. Jones has a cavity.

Elizabeth Smith had her teeth whitened.

Frank Mercer has HIV.

Mark Eyre’s blood type is A+.

Francis Edwards is afraid of needles.

What's Required to be Compliant

Awareness & Education

Everyone who has access to PHI has had awareness, education and training on HIPAA regulations and compliance. This includes 3rd party hosting services.

Data Disposal

Procedure to address the final disposition and length of time data stored. Auditable record of disposal.

Auditability & Authentication

Procedural mechanisms that record and examine activity in information systems that contain or use PHI.

- Who is accessing the data? (Username/ Password)
- Automatic log off to prevent unauthorized access
- No shared accounts

Security

Encryption, user verification, access codes, offsite storage

Compliant Messaging Requires Authentication

Authenticate

HIPAA says, "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

- A truly compliant messaging system must provide a unique login for each individual user.
- Sharing of accounts is strictly forbidden by HIPAA regulations as it becomes impossible to determine who had access to protected information at any given time.
- Automatic log off to prevent unauthorized access if a user leaves their account unattended.

Compliant Messaging Requires Auditability

Audit

HIPAA says, "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

- You must be able to manage access to information, restricting or closing the accounts on-demand.
- You must keep a secure log of all messages. HIPAA requires secure data storage as long as you need the documents. When no longer required, you need to know patient data is disposed of according to regulations. If your message service doesn't properly dispose of your data, the onus is on you.
- Track message forwarding. You will need to prove there is a record of which messages were forwarded and to where.

Compliant Messaging Requires Chain of Custody Management

Custody

HIPAA says, "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

- It is imperative that you can prove who came in contact with protected patient information. The nature of traditional email does not allow such proof as it transits the Internet through an unknown and unmonitored chain of servers.

- http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
- http://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html
- http://www.hhs.gov/hipaa/for-professionals/faq/578/may-a-covered-entity-reuse-computers-that-store-protected-information/index.html

The very real consequences of violating regulations.

Enforcement, fines, and punitive measures are real

There is no such thing as “non-sensitive” patient information.

- Minimum $1,000/patient violation, max $25,000
- Willful neglect minimum - $50,000/patient violation

http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page

Public notice:

- **Individual Notice** – All individuals affected must be notified in writing within 60 days. If 10 or more individuals can not be contacted, the breach must be posted on your practice website.
- **Media Notice** – Breaches affecting more than 500 people must be reported to prominent media outlets serving the area.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

Loss of reputation:

- Undermine relationships with patients and colleagues
- Long term ramifications on practice reputation
- Patients could sue for reputational damage

http://www.physicianspractice.com/articles/hipaa-omnibus-rule-and-its-possible-impact-malpractice

What's Wrong With Traditional Collaboration

Faxing patient data:

- How long does it take to send a fax?
  - Printing, Dialing, Scanning, Repeat
- What happens to all that paper in your office and theirs?
  - Faxes must be securely stored/destroyed
- Have you ever misdialed a telephone/fax number?

Mailing patient information:

- Time consuming
- Resource heavy
- Expensive

Email:

- Insecure, encryption is not good enough
  - 1 in 5 email accounts will be hacked
  - No chain of custody
- Insufficient attachment size
- Patients CANNOT consent to a dentist sending information to any other medical professional through un-secure methods

Encrypted or not, Email is not Compliant

- Even if your computer is secure, your message passes through dozens of unknown servers en-route to its destination.
- These “middle-man” servers make up the backbone of the email system, but are not secure therefore not compliant.
- Dentists have a duty to take precautions to safeguard private patient data.

Consent is not Compliance

Can I get consent to use e-mail with my patients?

- You must explain the risks associated with traditional e-mail
- You should get written consent from your patients
- Your Practice is still at risk.
  - **You are still liable if a data breach occurs from storing that information on your phone, tablet, laptop or computer system.**

Can I get consent to use e-mail with my colleagues?

- Patients can NOT consent to a dentist sending information to any other medical professional through un-secure methods.

6 Steps to Using Traditional Email in a Compliant Way

You can ONLY use traditional email if:

1. Patient has consented to the use of email (Doctor to Patient only!)
2. Verification email addresses of recipients
3. De-Identify the information
4. Transmit the minimum necessary
5. Encrypt and Decrypt the electronic personal health information that you transmit: [This is VERY difficult]
6. Do not email sensitive information or diagnosis

What Does De-Identified really mean?

De-Identified Health Information:

There are two ways to de-identify information

1. A formal determination by a qualified statistician
2. The removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and **is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.**

http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

How Useful is De-Identified Information ?

Dear Dr. Smith,

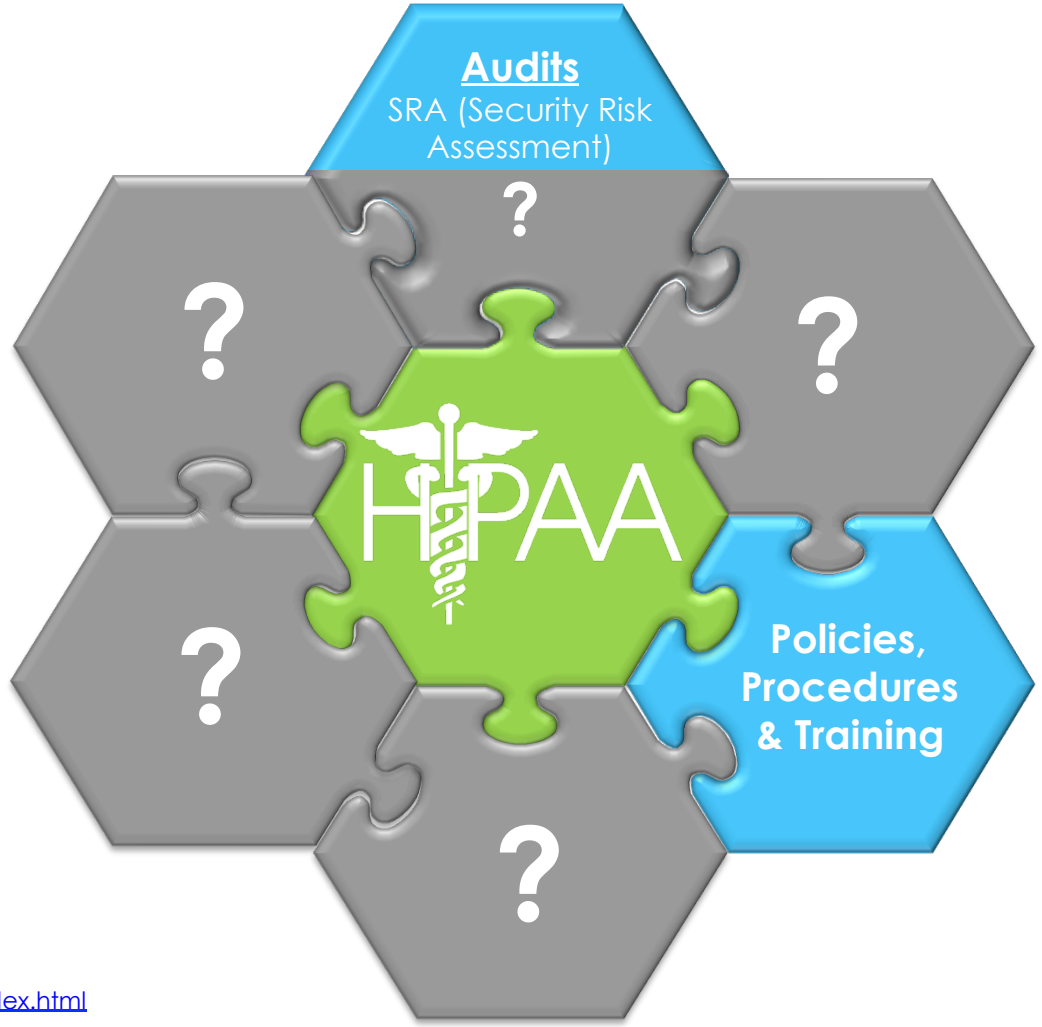
Here is an x-ray of my patient. Please call me so I can tell you their age, gender, chief complaint, medical history and other information related to their needs.

-Mark

Why Should I Worry About HIPAA

HIPAA is the Law

- **Enforcement is on the rise ↑**
  - Record fines levied: **$8,664,800** this year*
  - Three prison sentences
  - Medical license revoked
  - State Attorney General levying fines
- **HIPAA is confusing**
  - SRA (Security Risk Assessment)
  - Policies & Procedures
  - Training
- **Current market solutions only address *pieces* of compliance**



FAIL

* As of June 2016, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

Thank You

Brightsquid feature highlights

- 30 second sign up
- Functions just like familiar email applications
- Prioritizes file attachment – drag and drop
- Safely collaborate and share with anyone, anywhere
- Free access for anyone you invite

Compliant Communication
for $39.95/month

BRIGHTSQUID

www.brightsquid.com

Questions?

For more information, contact:

1-800-238-6503

mark@brightsquid.com

www.Brightsquid.com

855-85-HIPAA

info@compliancygroup.com

www.CompliancyGroup.com