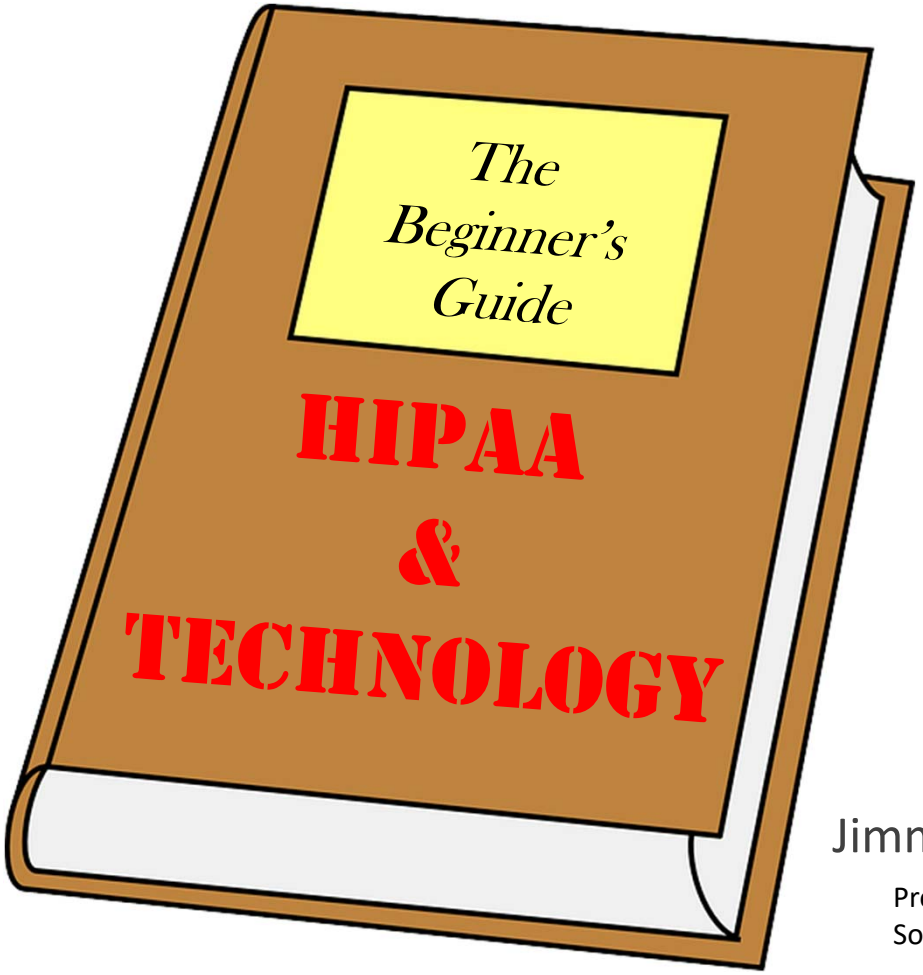

Notes:

Jimmy Georgiou

President/CEO –
SolutionStart & Aspida

Takeaway

Learning Objective:

Provide background and insight on the administrative, technical, and physical safeguards that define the requirements and expectations of HIPAA.

Result:

Increase awareness, creation and adoption of HIPAA compliant policies, procedures and physical networks in the dental practice.

Notes:

Overview

- ☑ Privacy & Compliance
- ☑ Technology
- ☑ Implementation
- ☑ The Four Major Threats

Notes:

Definitions

- **ePHI - Electronic Protected Health Information**
  Information that identifies an individual and is created, maintained or transmitted electronically
- **BA - Business Associate**
  Any person or entity that you have granted access to your patient's ePHI
- **BAA - Business Associate Agreement**
  An agreement the clearly defines the roles and responsibilities of each party regarding the protection of ePHI
- **CE - Covered Entity**
  Any Healthcare Provider, Healthcare Plan or Healthcare Clearinghouse
- **Breach**
  The unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information
- **Incident**
  The act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or it's data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- **NIST - National Institute of Standards and Technology**
  The federal technology agency that works with industry to develop and apply technology, measurements, and standards

Notes:

Business Vulnerabilities

OUTSIDE:

- Fax
- Email
- Phones
- Mail

IN BETWEEN:

- WiFi
- Remote Access
- Firewall

INSIDE:

- User Access Controls
- Patch Management
- Backup
- Policies and Procedures

Notes:

The Four Major Threats

- Your IT Guy
- Your Staff
- Technology Threats
- “True” Compliance

Notes:

Notes:

References - C.F.R - Code of Federal Regulations from The Federal Register

Administrative Safeguards -

i. **§ 164.308(a)(1)(ii)(D)** *Information system activity review.* Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
ii. **§164.308(a)(2)** *Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
iii. **§ 164.308(a)(5)(i)** *Security awareness and training* - Implement a security awareness and training program for all members of its workforce (including management).
iv. **§ 164.308(a)(5)(ii)(A)** *Security reminders* - Implement periodic security updates.
v. **§ 164.308(a)(5)(ii)(B)** *Protection from malicious software* - Implement procedures for guarding against, detecting, and reporting malicious software.
vi. **§ 164.308(a)(5)(ii)(C)** Log-in Monitoring - Implement procedures for monitoring log-in attempts and reporting discrepancies.
vii. **§ 164.308(a)(5)(ii)(D**) Password Management - Implement procedures for creating, changing and safeguarding passwords.
viii. **§ 164.308(a)(7)(i)** *Contingency Plan* - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
ix. **§ 164.308(a)(7)(ii)(A)** *Data Backup Plan* - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
x. **§ 164.308(a)(7)(ii)(B)** *Disaster Recovery Plan* - Establish (and implement as needed) procedures to restore any loss of data.
xi. **§ 164.308(a)(7)(ii)(C)** *Emergency Mode Operation* - Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
xii. **§ 164.308(a)(7)(ii)(D)** *Testing and Revision Procedures* - Implement procedures for periodic testing and revision of contingency plans.
xiii. **§ 164.308(b)(1)** *Business Associate contracts and other arrangements* - A covered entity, in accordance with §164.308 may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.
xiv. **§ 164.312(a)(2)(ii)** *Emergency Access Procedures* - Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
xv. **§ 164.530(a)(1)(i)** *Personnel designations.* A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

Physical Safeguards -

xvi. **§ 164.310(d)(1)** *Device and Media Controls Standard* - Implement policies and procedure that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.
xvii. **§ 164.310(d)(2)(i)** *Disposal* - Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
xviii. **§ 164.310(d)(2)(ii)** *Media Re-Use* - Implement procedure for removal of electronic protected health information from electronic media before the media are made available for re-use.
xix. **§ 164.310(d)(2)(iii)** *Accountability* - Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
xx. **§ 164.310(d)(2)(iv)** *Data and Backup Storage* - Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Technical Safeguards -

xxi. **§ 164.308(d)** *Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
xxii. **§ 164.312(a)(2)(i)** *Unique user identification* - Assign a unique names and/or number for identifying and tracking user identity.
xxiii. **§ 164.312(a)(2)(iii)** *Automatic Logoff* - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
xxiv. **§ 164.312(a)(2)(iv)** *Encryption and Decryption* - Implement a mechanism to encrypt and decrypt electronic protected health information
xxv. **§ 164.312(b)** *Standard: Audit controls* - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
xxvi. **§ 164.312(e)(1)** *Standard: Transmission Security* - Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
xxvii. **§ 164.312(e)(2)(ii)** *Encryption* - Implement a mechanism to encrypt electronic health information whenever deemed appropriate.

Speaker Information

Jimmy Georgiou is the Founder and CEO of SolutionStart, a leading provider of technology solutions and services with a concentration on the Dental Industry.

In conjunction with providing guidance from a technology standpoint, Jimmy began to focus on the impact of HIPAA within the dental industry. After several years of studying and fully understanding the role technology will play in this field, he launched a second company, Aspida, to better address these mandates and regulations.

Launched in 2013, Aspida has quickly established itself as an industry leader in providing HIPAA compliant security products and services - their first product to market being Aspida Mail, a HIPAA Compliant Encrypted Email.

Jimmy is an industry leader in the areas of HIPAA and dental technology and has educated hundreds of dentists and dental professionals through his presentations at dental society meetings and study clubs.

Jimmy Georgiou
President/CEO

www.aspida.us
www.facebook.com/aspida.us

www.solutionstart.com
www.facebook.com/solutionstart