The Facts; Only the Facts:

As mandated in April 2005, your practice must comply with the Security Rule provision of the Health Insurance and Accessibility Act (HIPAA). The Security Rule mandates that your practice must do the following:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information that your practice may create, receive, maintain, or transmit;

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and

4. Ensure compliance by your team.

Challenges complying with HIPAA

Chances are you have a server some place in your practice. Regardless of where it is located in your office, it represents a significant risk and challenge to your ability to comply with the HIPAA Security Rule. **Here's why:**

- **Physical Security.** Protected health information (PHI) stored on your server is not likely to be secure because if your office is burglarized, your computers will be the likely target.
- **Electronic Security.** Chances are your server is protected from the outside world by consumer-quality routers and firewalls, security tools that nearly any cybercriminal could hack in a matter of minutes. Additionally, the fact that your server is probably not physically secure means that it can be easily accessed by virtually anybody who stumbles across it.
- **Backup Integrity.** Where does one begin with all that can go wrong here? Backup tapes are unreliable. Mirrored drives are useless if your practice floods or burns. And almost half of all backups never restore.
- **Emergency Availability.** HIPAA requires that you must be able to retrieve and access PHI in the event of a local disaster. If your data is not on the cloud, rebuilding your system and restoring your data can be expensive, time-consuming, and impractical.
- **IT Management.** Because the PHI resides in your office, the burden of physical and electronic security, backup, and disaster recovery rests squarely on your shoulders—like you've got nothing better to do!

The Advantages of Curve Dental

In contrast, Curve Dental's cloud-based dental software helps you tackle all of the HIPAA security challenges with little to no effort.
Here's how:

- **Physical Security.** With Curve Dental your data is located in a top-tier Amazon Web Services (AWS) data center with biometric access, video surveillance and professional security carrying sci-fi looking ray guns (just kidding). Nobody gets in unless they're supposed to be there.
- **Electronic Security.** Professional-grade firewalls, intrusion detection systems, and the quality of hardware used in the AWS is not something a practice could or would purchase.
- **Backup Integrity.** Call us paranoid or just super careful, but we automatically back-up and store your data so you don't have to worry about a thing. Plus, we verify a restore and backup of the data in two different physical locations.
- **Emergency Availability.** If an emergency happens in your area all you need is a computer with internet access and a browser in order to access your data.
- **IT Management.** Because all of your data is stored on our system you don't worry about data backups or stress over server crashes.

Security Standards Comparison

Let's compare the cloud with how a traditional client-server system addresses Security Rule requirements. The following series of handy dandy charts clearly show each system performs when it comes to each individual requirement.

A Word of Caution: A check in any box is not meant to indicate that you don't need to evaluate that specific security standard. A check indicates that the software, whether Curve, paper or server-based, can provide support for meeting that standard. You should determine if the software solution alone is sufficient or if additional action on your part is required. Remember: Software can never be HIPAA-compliant but it can help you become HIPAA-compliant. As with any legal topic, you should carefully review this information with a professional experienced in these matters. We're software developers, not HIPAA experts!

The Facts; Only the Facts:

Administrative Safeguards

Standards	*Sections*	*Implementation Specifications*	*Curve*	*Legacy*
Security Management Process	164.308(a)(1)	Risk Analysis [r]		
		Risk Management [r]		
		Sanction Policy [r]		
		Information System Activity Review [r]	✓	✓
Assigned Security Responsibility	164.308(a)(2)		✓	✓
Workforce Security	164.308(a)(3)	Authorization and/or Supervision		
		Workforce Clearance Procedures		
		Termination Procedures		
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions [r]		
		Access Authorization		
		Access Establishment and Modifications		
Security Awareness and Training	164.308(a)(5)	Security Reminders		
		Protection from Malicious Software		
		Log-in Monitoring	✓	✓
		Password Management	✓	✓
Security Incident Procedures	164.308(a)(6)	Response and Reporting [r]	✓	
Contingency Plan	164.308(a)(7)	Data Backup Plan [r]	✓	
		Disaster Recovery Plan [r]	✓	
		Emergency Mode Operation Plan [r]	✓	
		Testing and Revision Procedure		
		Applications and Data Criticality Analysis		
Evaluation	164.308(a)(8)			
Business Associate Contracts	164.308(b)(1)	Written Contract or Other Agreement [r]	✓	✓

Physical Safeguards

Standards	*Sections*	*Implementation Specifications*	*Curve*	*Legacy*
Facility Access Controls	164.310(a)(1)	Contigency Operations [r]	✓	
		Facility Security Plan [r]	✓	
		Access Control and Validation Procedures [r]	✓	
		Maintenance Records [r]	✓	
Workstation Use	164.310(b)		✓	
Workstation Security	164.310(c)		✓	
Device and Media Controls	164.310(d)(1)	Disposal	✓	
		Media Re-use	✓	
		Accountability [r]	✓	
		Data Backup and Storage [r]	✓	
		Access Establishment and Modifications	✓	

[r] *This is a Required specification as opposed to an Addressable specification*

The Facts; Only the Facts:

Technical Safeguards

Standards	*Sections*	*Implementation Specifications*	*Curve*	*Legacy*
Access Control	164.312(a)(1)	Unique User Identification (r)	✓	✓
		Emergency Access Procedure(r)	✓	
		Automatic Logoff	✓	✓
		Encryption and Decryption (r)	✓	✓
Audit Controls	164.312(b)		✓	
Integrity	164.312(c)(1)	Mechanism to Authenticate PHI (r)	✓	
Person or Entity Authentication	164.310(e)(1)	Integrity Controls(r)	✓	
		Encryption (r)	✓	✓

Organization Requirements

Standards	*Sections*	*Implementation Specifications*	*Curve*	*Legacy*
Business Associate Contracts and other Arrangements	164.314(a)(1)	Business Associate Contracts(r)	✓	✓
		Other Arrangements(r)		
Requirements Group Health Plans	164.314(b)(1)	Implementation Specifications (r)		

Policies and Procedures and Documentation Requirements

Standards	*Sections*	*Implementation Specifications*	*Curve*	*Legacy*
Policies and Procedures	164.316(a)			
Documentation	164.316(b)(1)	Time Limit (r)	✓	
		Availability (r)	✓	✓
		Documentation Updates (r)	✓	✓

(r)This is a Required specification as opposed to an Addressable specification

About Curve Dental

Founded in 2004, Curve Dental provides cloud-based dental software and related services to dental practices within the United States and Canada. The company is privately held, with offices in Provo, Utah, and Calgary, Alberta. The company strives to make dental software less about computers and more about user experience. Their creative thinking can be seen in the design of their software, that's easy to use and built only for the web.

curve DENTAL®

Visit us at www.curvedental.com