HIPAA / HITECH

Overview of Capabilities and Protected Health Information

April 2017

Rev 1.5.2

Notices

This document is provided for informational purposes only. It represents DragonFly's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of DragonFly's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from DragonFly, its affiliates, suppliers or licensors. The responsibilities and liabilities of DragonFly to its customers are controlled by DragonFly's agreements, and this document is not part of, nor does it modify, any agreement between DragonFly Athletics and its customers.

DragonFly Athletics provides a premier mobile communication platform, focused on the Student Athlete Ecosystem. DragonFly is delivered via mobile smartphones, mobile tablets, and a website. Mobile tools have become critically important in today's world. Studies show that people who leave a purse or wallet at home may not return for it. However, if a smartphone is left at home, chances are one will return for it. With so much of our lives tethered to these devices there is now a great opportunity to utilize this technology to improve Student Athlete Health.

The Student Athlete (SA) Ecosystem contains many people who work to help athletes perform at their top levels. Commonly, as part of these services, the Athletic Trainers, Coaches, and Administrators who work with athletes must treat injuries sustained on the field of play. These injuries range from insignificant bumps and bruises to, on occasion, severe medical emergencies; requiring the coordination of Emergency Technicians, Physicians, hospital staff, Physical Therapists, and many other health care professionals. Likewise, parents play an equally vital role in this process. Through timely communication, it is easier for care providers to leverage parent's inherent influence on student athletes.

The need for and complexity of communication between all parties in the SA Ecosystem has grown in recent years as Athletic Trainers have increasingly become the first points of contact, not only for sports related care, but also for a host of medical and psychological issues. Increasingly, the Athletic Trainer represents the only health professional with whom many athletes have meaningful contact.

DragonFly recognizes the many roles that various parties play in the SA Ecosystem. Oftentimes, these parties share duties and responsibilities in the care ecosystem. Some care providers may be employed by high schools or the collective school system, while others are independent third party employees, providing care on school premises. On occasion, a provider may be unrelated to the primary organization, yet provide care due to away games or tournament play. Injuries requiring even the most basic of care, such as tape or ice, are often performed in front of thousands of spectators. This public delivery of care can quickly blur lines in terms of what is considered protected health information.

From the beginning, DragonFly made the choice to build a system with the assumption that ALL information contained within would be considered Protected Health Information (PHI). At its core, DragonFly MAX strives to protect the confidentiality of health information by restricting PHI access to only those who have appropriate authorization.

DragonFly HIPAA Compliance Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a set of U.S. laws that protect the security and privacy of health information held by Covered Entities. The term

covered entity refers to three specific groups: health plans, health care clearinghouses, and healthcare providers that transmit health information electronically.

High schools are generally not considered "Covered Entities" in the context of HIPAA. However, other regulations, such as FERPA (The Family Educational Rights and Privacy Act of 1974), provide similar guidelines over Student Athlete data. Your organization should determine if it is considered a "Covered Entity". For covered entities, DragonFly offers the option to sign a Business Associates Agreement. See the DragonFly HITECH Compliance section below for more details.

DragonFly includes many features and precautions to protect PHI and assist covered entities with HIPAA related compliance. These features include:

Physical Security

DragonFly's service infrastructure is hosted in secure facilities by Amazon Web Services (AWS). AWS operates numerous state-of-the-art Data Centers around the United States, which provide military grade, physically restricted access to all infrastructure components hosting PHI. Authorized employees of the data center must pass two factor authentication to gain access to the data centers, no less than 3 separate times prior to entering.

- No PHI is stored at DragonFly offices or on the computers, smartphones, tablets or other device of DragonFly employees. All PHI is hosted inside AWS data centers.

Mobile Devices

A key DragonFly communication component is the ability to begin the care process instantly upon injury occurrence. Appropriate parties are notified immediately after care providers, typically an Athletic Trainer, initiate documentation from their smartphone. This process may even begin from the sidelines of an athletic venue.

- All data stored inside DragonFly, on smartphone and other mobile devices, is encrypted on the physical device utilizing the cryptographic components of modern smartphones using 256-bit AES encryption.

- Any mobile device can be remote wiped, such that the data on the device is permanently erased.

- Only data associated with the individual who is authorized on the mobile device is stored.

Technical Security

DragonFly implements various policies and procedures to ensure access to the system is restricted to only authorized parties.

- Users must be added to the system and receive private authentication credentials known only to that specified user. For most users, physical access to mobile devices must be available when installing the system for the first time.

- DragonFly user sessions automatically time out after a certain amount of idle time, requiring the user to login to their device again.

- Users are required to pass "two-factor authentication" prior to gaining access to DragonFly.

- Each user account must be configured with a specific set of security parameters. For instance, Coaches are only allowed access to athletes associated with the sport he or she instructs. Athletic Trainers only have access to specific teams, for which they provide care. Parents have access only to their individual athlete.

- All access to any service in the DragonFly infrastructure is audit logged, providing a record of the requestor. These access logs are proactively monitored to detect unauthorized activity.

- Notifications sent via Text or In-App notification never contain PHI.

- All PHI is redundantly backed up daily. Multiple encrypted copies are maintained in geo-redundant availability zones of AWS data centers to protect against accidental destruction.

Data Encryption

All PHI transmitted in DragonFly is secured while in motion with TLS 1.2 security. Often, the term SSL is utilized to imply secure communications. However, SSL is being phased out industry wide, in favor of TLS.

All PHI stored within DragonFly is encrypted utilizing 256-bit AES encryption when sitting on storage media, such as hard drives and backup devices.

When infrastructure components are replaced, DragonFly utilizes procedures to destroy the devices and all data contained on the devices.

Firewalls

All infrastructure components in the DragonFly system are protected by extensive firewalls. These firewalls are placed in multiple layers at points in our infrastructure to isolate our internal data processing systems from the components of our infrastructure, which communicate with end users. Firewalls are configured to be maximally restrictive.

Administrative Policy

Only Employees needing access to PHI are granted access, and only to the minimum extent necessary to complete their tasks. This access is only for the operation and maintenance of the DragonFly infrastructure by Engineering staff.

All employees who may typically come into contact with PHI are required by DragonFly to sign confidentiality agreements and Non-Disclosure Agreements.

Employees must participate in HIPAA awareness training concerning how DragonFly protects sensitive data.

Access to all DragonFly Infrastructure within AWS is logged. Employees, when required and necessary, use Secure Shell tools implementing TLS 1.2 encryption to access infrastructure components at the AWS data center.

Peer-review of activity is required for employees of DragonFly. When work is being performed there is a minimum of two individuals providing peer oversight.

DragonFly HITECH Compliance Summary

The Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the American Recovery and Reinvestment Act of 2009 (ARRA) confer additional responsibilities to Business Associates who have access to Covered Entities' Protected Health Information.

Business Associates Agreement

In some cases, DragonFly may qualify as a Business Associate. At the customer's request (if the customer is a covered entity), DragonFly will sign a Business Associate Agreement, acknowledging that:

1. DragonFly will act as the custodian of the customer's PHI data (because DragonFly manages the hosting infrastructure)

2. Certain DragonFly employees have access to the data on an as-needed and Minimum Necessary basis
3. DragonFly will protect the privacy, confidentiality, integrity, and availability of that data, and will safeguard the PHI from unauthorized access and disclosure

DragonFly Infrastructure Partner – Amazon Web Services

DragonFly has chosen Amazon Web Services as our partner in providing a secure, managed infrastructure for our back end systems, which permits the delivery of the DragonFly system. DragonFly has entered into a Business Associates Agreement with Amazon Web Services, providing certified HIPAA compliant and capable infrastructure components.

Amazon provides “Security of the Cloud”, which ensures that the services we utilize under our BAA agreement protect all PHI transmitted and processed through their infrastructure.

More about the extensive details of AWS HIPAA certifications may be found at the following resources.

https://aws.amazon.com/compliance/hipaa-compliance/
https://aws.amazon.com/compliance/shared-responsibility-model/
https://d0.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf