

keep their trust

PROTECT YOUR PLAYERS' PRIVACY

PHI

protected health information

PII

personally identifiable information

ATHLETE IDENTITY THEFT AND YOU
Rate yourself on back page.



TOP 10 QUESTIONS IF YOU DO INJURY TRACKING ON THE WEB

Data breaches of PHI and PII do not happen only from hacker attacks. Those are the breaches you read about in the news. Mostly breaches come from persons authorized to work with the data who either steal the data (in order to sell it for gain), lose it or have it stolen from their possession, lose or have stolen their web access tool (mobile devices with online web/cloud logins installed), or willfully or negligently permit access by users not authorized to see the private information. Many countries have strict laws governing web PHI and PII, with serious breach penalties for those responsible for entering and maintaining the data.

If you are using the web/cloud for injury tracking, see how you score on these questions.

		Yes	No
1. Do you know where your web/cloud data is right now? (include the backup location, too)	Country	<input type="checkbox"/>	<input type="checkbox"/>
	City	<input type="checkbox"/>	<input type="checkbox"/>
	Server Center	<input type="checkbox"/>	<input type="checkbox"/>
2. Do you know what persons there have access to that web information?		<input type="checkbox"/>	<input type="checkbox"/>
3. Do your athletes/parents (customers) know you are placing their personal data and private health information online in the cloud? If so, do you have signed consent forms giving you permission to put their personal and private health information on the web where you have it?		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
4. Is your data (and backup) stored encrypted at your injury tracking cloud location?		<input type="checkbox"/>	<input type="checkbox"/>
5. Can you describe the laws that apply to you and your online PHI/PII? (include both the state where you work and the state where the data is stored)	Federal	<input type="checkbox"/>	<input type="checkbox"/>
	State	<input type="checkbox"/>	<input type="checkbox"/>
6. Have you a legally binding and financially backed letter of indemnification from your online injury tracking provider regarding liability in case of a data breach by their internal theft or negligence, or by outside hacking?		<input type="checkbox"/>	<input type="checkbox"/>
7. Have you a data breach risk assessment (written report) on file that addresses the online injury tracking services and processes you are using?		<input type="checkbox"/>	<input type="checkbox"/>
8. Do you have written authorization from management (administration / IT Dept. / Athletic Director) for placing PHI/PII on the web at the place where you have it?		<input type="checkbox"/>	<input type="checkbox"/>
9. Do you personally or does your employer have liability insurance that covers your personal risk in the event of an online data breach of PHI/PII?		<input type="checkbox"/>	<input type="checkbox"/>
10. Have you a written plan on file at your own office that spells out who is authorized from your organization to access the online private information you enter, and from what specific devices (login control)? ... emergency actions in the event of a data breach caused by you or your staff (like a lost log-in tablet or stolen password) or by your web injury tracking service (like their employee theft of identities or hacking)?		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

SCORING: Look at your answers above. If they were the answers given to you by your local bank officer about your own personal bank account information at the bank, how would you rate your bank?

1	2	3	4	5	6	7	8	9	10
not at all satisfied		not very satisfied			mostly satisfied			fully satisfied	