To: Elizabeth Holmes[eholmes@theranos.com]
From: David Doyle[/O=THERANOS ORGANIZATION/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DAVID DOYLE]
Sent: Wed 5/2/2012 11:56:58 PM (UTC)
Subject: Trade secret policy reminder

Elizabeth: The following is a draft of the trade secret policy you asked me to prepare. In it, I provide a basic description of how trade secrets work, why they matter, and how they can be maintained. As we discussed earlier, this is primarily intended as a summary for team leads, so it does not contain a ton of detail or specific policy prescriptions. Let me know if this is what you had in mind. Thanks.

All:

As you know, there are few things Theranos values more than its intellectual property. We vigorously pursue and enforce patent protection for our IP, wherever it makes sense to do so. But in cases where our patents are still pending, and even where they may ultimately be unavailable, trade secret laws provide another critical layer of protection for our IP. This email is a reminder of how those laws work and what your is role in protecting the many trade secrets we develop here at Theranos.

Trade secret protections derive from state law, rather than the U.S. statutes that govern patent and (most) trademark rights. Compared to those federally-granted IP rights, trade secrets are much simpler to obtain. The developer does not need to demonstrate the novelty or non-obviousness of its trade secret, or to register anything to obtain protection. In most states, including California, a trade secret is simply any information that: (a) the owner makes reasonable efforts to keep secret; and (b) has economic value because it is not generally known (to the public or a competitor). "Negative information," such as the fact that a specific method or configuration does *not* work, is equally protectable, provided these two criteria are met.

Another way trade secrets differ is that they can theoretically last indefinitely, well beyond the limited term of patent protection (currently 20 years). But this protection depends on the information remaining secret. The defining characteristic of a trade secret, in fact, is that it is <u>never</u> disclosed publicly. This distinguishes these rights from patents and trademarks, which <u>must</u> be publicly disclosed to secure protection. Provided the holder employs reasonable efforts to protect a trade secret, he or she may file suit whenever that secret is used or disclosed through "improper means." Such means include theft, bribery, misrepresentation, breach of a duty (contractual or otherwise), or industrial espionage. Reverse engineering or independent derivation of a trade secret do not qualify as improper, unless the party doing so has previously agreed to refrain from those activities.

This is where you come in. It is Theranos policy that we employ every reasonable measure we can to protect our trade secrets from improper use or disclosure. We ask that you and your team keep the following measures in mind to protect Theranos confidential information that may include trade secrets:

- Protecting the physical security of Theranos facilities and individual work stations, laboratories, and document storage spaces within them, including through the use of access controls (mandatory ID checks, selective key card access, keeping facility doors and storage cabinets locked, etc.), enforcing company policies (e.g., prohibiting unauthorized recordings), and maintaining company-wide vigilance;
- Protecting the security of Theranos's electronic records, databases, computer applications and related communications at all times, including through the use of password protections, access restrictions, automatic login time-outs, secure communications infrastructure, etc.;
- Requiring all visitors to Theranos facilities to sign a CDA on their own behalf (an "individual CDA"); and have an authorized representative sign a CDA on behalf of any entity the visitor may represent (an "entity CDA"), before entering the facility;
- Requiring all vendors and other potential business partners to sign an entity CDA prior to commencing discussion of *any* Theranos confidential information, and also including restrictions against reverse engineering or other unauthorized use or disclosure in vendor/partner agreements;
- Requiring all new and existing employees, consultants, and other team members to sign individual CDAs, as well as project-specific CDAs for particularly sensitive tasks;
- Proactively *educating* new employees, partners, and others (as appropriate) about our confidentiality expectations and the potential consequences from unauthorized disclosure of trade secret information;
- Reminding employees/vendors/partners/visitors that no longer will be doing business with Theranos of their ongoing confidentiality obligations and requesting the return/destruction of confidential information in their possession, wherever

possible; and

- Promptly notifying management of any potential security lapse or suspected misconduct, such that we may remedy the situation and assert our legal rights against any who have improperly used or disclosed our trade secrets.

We require your help with implementing and monitoring these security measures. Together, these are the steps we feel are reasonable in maintaining the secrecy of the confidential work we do here, and hence preserving the trade secret rights indefinitely.

Thank you for your continued vigilance.