IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MASSACHUSETTS

TEVA PHARMACEUTICALS INTERNATIONAL GMBH and TEVA PHARMACEUTICALS USA, INC.,

Plaintiffs,

v.

ELI LILLY AND COMPANY,

Defendant.

Civil Action No. 1:18-cv-12029-ADB

JOINT STIPULATED PROTOCOL GOVERNING ELECTRONICALLY STORED INFORMATION

The Parties, through their counsel, hereby stipulate and agree to this Joint Stipulated Protocol Governing Electronically Stored Information (the "Protocol"). All Parties are bound by and subject to the terms of this Order. By stipulating to this Protocol, no Party is waiving any objection that could otherwise be made in response to a discovery request, including any objections to the production, discoverability, admissibility, or confidentiality of documents. No Party shall be required to undertake preservation, collection, or search measures beyond the scope of this Protocol unless the Parties agree in advance and in writing or the Protocol is modified by the Court. All document productions shall be subject to the Parties' forthcoming Stipulated Protective Order (the "Protective Order"), which shall be filed with the Court no later than May 26, 2020.



1. General Provisions

- a. Definitions. The Parties incorporate by reference the Definitions set forth in Rule26.5(c) of the Local Rules of the United States District Court for the District of Massachusetts.
- b. Cooperation. The Parties shall conduct discovery in a cooperative manner, including without limitation by reasonably drafting discovery requests and responses in accordance with Fed. R. Civ. P. 1 and 26(g)(1); and producing Electronically Stored Information ("ESI") in accordance with Fed. R. Civ. P. 34; and by meeting and conferring in good faith on topics such as the identification of custodians, potentially relevant data sources, and search terms, and such other issues as may arise during the course of discovery.
- c. Proportionality. The proportionality standard set forth in Fed R. Civ. P. 26(b)(1) shall be applied in all matters related to discovery of ESI, including without limitation the preservation, collection, and production of such information. To further the application of the proportionality standard, requests for production of ESI and related responses shall be stated with reasonable particularity and specificity.
- d. Preservation of Discoverable Information. The Parties recognize their obligation to take reasonable and proportional steps to preserve discoverable information in their possession, custody, or control.
- i. Absent a showing of good cause by the party requesting information (the "Requesting Party"), the Parties shall not be required to modify, on a going-forward basis, the procedures used by them in the ordinary course of business to back up and archive data; provided, however, that the Parties shall preserve the non-duplicative discoverable information currently in their possession, custody, or control.



- **ii.** Absent a showing of good cause by the Requesting Party, the following categories of ESI need not be preserved:
 - 1. Deleted, slack, fragmented, or other data only accessible by forensics;
 - 2. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;
 - 3. On-line access data such as temporary internet files, history, cache, cookies, and the like;
 - 4. Data in metadata fields that are frequently updated automatically, such as "last opened" dates;
 - 5. Back-up data that are substantially duplicative of data that are more accessible elsewhere;
 - 6. Voice messages;
 - 7. Instant messages that are not ordinarily printed or maintained in a server dedicated to instant messaging;
 - 8. Electronic mail or pin-to-pin messages sent to or from mobile devices (e.g., iPhone and Blackberry devices), provided that a copy of such mail is routinely saved elsewhere;
 - 9. Other electronic data stored on a mobile device, such as calendar or contact data or notes, provided that a copy of such information is routinely saved elsewhere;
 - 10. Logs of calls made from mobile devices;
 - 11. Server, system, or network logs;
 - 12. Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as part of a laboratory report; and
 - 13. Data remaining from systems no longer in use that is unintelligible on the systems in use.



e. Privilege.

- i. The Parties shall confer on the nature and scope of privilege logs for the case, including whether categories of information may be excluded from any logging requirements and whether alternatives to document-by-document logs can be exchanged.
- ii. With respect to information generated after the filing of the Complaint on Sept. 27, 2018, the Parties are not required to include any such information in privilege logs.
- iii. Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).
- iv. This Protocol is subject to, and does not modify, the Fed. R. Evid. 502 non-waiver provision of the Protective Order.
 - **f. Rolling Productions:** The Parties shall produce documents on a rolling basis.
- 2. Initial ESI Disclosures. No later than thirty (30) days after entry of this Protocol, each Party shall disclose:
- a. Custodians. A list of the 10 custodians most likely to have discoverable information in their possession, custody, or control. The custodians shall be identified by name, title, role in the instant dispute, and the subject matter of the information.
- **b. Non-custodial data sources.**¹ A list of the non-custodial data sources that are most likely to contain non-duplicative discoverable information for preservation and production consideration, from the most likely to the least likely.
 - **c. Notice.** The Parties shall identify any issues relating to:

¹ As used herein, the term "non-custodial data source" means a system or container that stores ESI, but over which an individual custodian does not organize, manage, or maintain the ESI in the system or container (e.g., an enterprise system or database).



- i. Any ESI (by type, date, custodian, electronic system, or other criteria) that a Party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(C)(i).
- **ii.** Third-party discovery under Fed. R. Civ. P. 45 and otherwise, including the timing and sequencing of such discovery.
- **iii.** Production of information subject to privacy protections, including information that may need to be produced from outside of the United States and subject to foreign laws.

3. Specific E-Discovery Issues.

- a. On-site inspection of electronic media. Such an inspection shall not be permitted absent a demonstration by the Requesting Party of specific need and good cause.
- b. Search methodology. No later than thirty (30) days after entry of this Protocol, the Producing Party shall disclose to the Requesting Party the search terms it intends to use to locate potentially responsive ESI. Absent a showing of good cause, a Requesting Party may request no more than 10 additional terms to be used in connection with the electronic search. Focused terms, rather than over-broad terms (e.g., product and company names), shall be employed. The Producing Party shall search (i) the non-custodial data sources identified in accordance with paragraph 2(b); and (ii) emails and other ESI maintained by the custodians identified in accordance with paragraph 2(a).
- c. **De-Duplication.** The Parties shall make reasonable efforts to de-duplicate ESI. ESI may be de-duplicated vertically within each custodian or horizontally across custodians. To the extent a party deduplicates horizontally across all custodians, the party shall identify all custodians of the document in the metadata field "Duplicate Custodian." All ESI will be deduplicated using MD5 or SHA1 Hash values. All files bearing an identical MD5 or SHA1 Hash



DOCKET

Explore Litigation Insights



Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time** alerts and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

