

## **EXHIBIT 2**

Document Partially Redacted for Confidentiality

**Exhibit 2**

Anthem commits to pay for and implement the business practices described below for a period of three (3) years from the date of Final Approval of the Settlement Agreement (the “Settlement Term”).

1. Before the end of the Settlement Term, Anthem shall complete deployment of the following data archiving steps related to data retention in [REDACTED]:

- Retain no more than the latest [REDACTED] of data in [REDACTED]. For information from the [REDACTED] retain data for no more than [REDACTED].
- Archive [REDACTED] data older than what is retained in the [REDACTED] with strict access requirements and reviews, as described in paragraph 2. This archived information will be evaluated on an annual basis to determine what can permanently be removed from the system based on retention requirements.

2. [REDACTED] which will be located in the [REDACTED] will be subject to the following additional access controls:

- Additional levels of management approval [REDACTED] are required prior to granting access to the [REDACTED].
- Access to the [REDACTED] will require use of [REDACTED] or substantially similar technology.
- Sessions will be automatically terminated after [REDACTED].
- Access will automatically expire [REDACTED] and users must submit new access requests if access is needed beyond [REDACTED].
- [REDACTED] will not have [REDACTED]. Should the [REDACTED] require access to the [REDACTED] for a temporary period they will use the same access request procedures as other users and be subject to the same access controls;
- [REDACTED] or substantially similar technology;
- [REDACTED] will be hosted on a [REDACTED].

3. [REDACTED] Anthem shall immediately implement [REDACTED]. Anthem shall [REDACTED].

- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

4. Anthem shall [REDACTED] where feasible. Where it is infeasible and Anthem does not deploy [REDACTED] Anthem shall require the [REDACTED]
5. Anthem shall continue to keep in place its current policies for [REDACTED] in Anthem's environment. Additionally, Anthem will commit during [REDACTED] to require business record documentation that demonstrates [REDACTED]
6. Anthem shall continue feeding the logs provided to Plaintiffs on May 10, 2017, or reasonably equivalent logs, [REDACTED] for the Settlement Term.
7. Anthem shall undertake an annual IT security risk assessment using an outside third party.
8. Anthem shall spend at least [REDACTED] a year on information security. Anthem shall also increase information security spending by [REDACTED] for every additional 5,000 users if Anthem increases its users by more than 10%, whether by acquisition or growth.
9. Anthem shall remediate 85% of critical and 80% of medium/moderate risk information security audit findings within 2 years and shall remediate 95% of critical findings within 3 years.
10. Anthem shall conduct adversarial simulations at least twice per year for the Settlement Term. These simulations, performed by [REDACTED] will mimic a malicious attacker with internal access to Anthem's network. Anthem will continue its use of [REDACTED] (or a similar vendor) [REDACTED] for the Settlement Term.
11. Anthem shall continue its current practices related to [REDACTED] and remediation. Specifically, Anthem will perform [REDACTED] in the Anthem environment for the Settlement Term. As to remediation, when a [REDACTED] is found, Anthem shall adhere to the following remediation schedule: [REDACTED]
12. Anthem shall achieve 90% implementation of the [REDACTED] by the end of Q2 2019.

13. Anthem shall keep these information security practices in place for the Settlement Term:

- Completed a 6000 sq. ft. state of the art Cyber Security Operations Center (“C-SOC”) in Indianapolis, IN. The C-SOC is staffed 24x7x365 to provide comprehensive monitoring of servers and other technologies to identify improper use of data. The C-SOC’s analytic capabilities are employed to detect, analyze and respond to potential security events that threaten the security of data. Anthem shall continue to operate the C-SOC 24x7x365.
- From 2015-2016, 70 additional information security staff members were hired, including C-SOC team members. Anthem shall keep staffing in place.
- Anthem shall keep in place requirements that [REDACTED] by Anthem associates will be [REDACTED] and that all [REDACTED] are protected by [REDACTED]
- [REDACTED] is in place and will be continued to [REDACTED] [REDACTED] are required to [REDACTED]
- Information Security training is mandatory for all associates. Phishing exercises are conducted against all associates and anyone who fails is registered for additional training.
- Anthem has implemented enhanced [REDACTED] and shall keep them in place.
- Anthem has implemented [REDACTED] and shall keep it in place.
- Anthem has implemented the [REDACTED]