FREQUENTLY ASKED QUESTIONS:

What happened/How did this happen?

On August 4, 2020, malicious code was found on certain servers. The threat was contained and expelled, and a thorough investigation promptly commenced into this intrusion. The investigation showed that the intrusion had been active since early July 2020.

On October 28, 2020, we determined that one of the impacted servers contained data from related health studies that you may know as the Nexplanon Observational Risk Assessment (NORA) or the International Active Surveillance Study - Safety of Contraceptives: Role of Estrogens (INAS-SCORE). While we have no indication that any data related to the Study were stolen, viewed, or misused, we took the precautionary step of notifying you.

What was the "malicious code"

The malicious code referenced in our letter was a strain of ransomware, a kind of malware used to encrypt data so that the data is inaccessible in order to extort payment of a ransom to the unauthorized actor. The unauthorized actor also used other forms of malware to carry out the intrusion.

What are the Nexplanon Observational Risk Assessment (NORA) or the International Active Surveillance Study - Safety of Contraceptives: Role of Estrogens (INAS-SCORE)?

These were two related studies, at least one of which you participated in. The NORA study was designed to characterize the frequency of specific insertion-, localization- and removal-related events and clinically significant consequences among Nexplanon users in the US during routine clinical use. The INAS-SCORE study assessed the risks of short and long-term use of estradiol valerate/dienogest (EV/DNG) and of established oral contraceptives (OCs).

What specific information of mine was affected?

The personal information involved may have included your name, social security number, and medical and health information that was part of the Study.

Is my personal information publicly available?

At this time, we have no indication that any data related to the Study were stolen, viewed, or misused, and so we do not believe any such data are publicly available.

How do I know my information is now safe?

After discovery of the malicious code the threat was contained and expelled, and a thorough investigation promptly commenced. Additional protection measures were also deployed including a sophisticated endpoint protection solution with NextGen anti-virus technology.

Why wasn't I contacted sooner?

We determined that two of the servers potentially impacted contained data from two related health studies that you may know as the Nexplanon Observational Risk Assessment (NORA) or the International Active Surveillance Study - Safety of Contraceptives: Role of Estrogens (INAS-SCORE) on October 28, 2020. After making that determination, we promptly organized notification as a precaution and arranged to provide you with credit monitoring, as described in our letter to you.

How many individuals were affected?

We are not able to share that information, but please know that we have taken this matter very seriously and are notifying the appropriate individuals as a precaution.

Does this mean I am the victim of identity theft?

No. At this time, we have no indication that any data related to the Study were stolen, viewed, or misused. We notified you as a precautionary step.