Security Incidents at Study Sites

Statement date 07-Jun-2023

Medidata is aware of the recent series of cybersecurity incidents at sites which are supporting clinical trials being conducted on our Platform. Due to privacy concerns those sites will not be identified here, but the statement below applies to all known incidents.

Proactively, Medidata/Dassault Systemes continuously monitors all access across our suite of services. Activity which is determined to be potentially malicious is blocked at levels ranging from network (IP addresses) to User accounts. These blocks are only lifted once the activity or account is determined to be safe. This is done continuously, not just when an external security incident is reported.

While confidentiality laws and Study Site policies may prevent Medidata from knowing the specific details of an incident at a Study Site, the preventive and response controls that Medidata has implemented to minimize associated risk are compliant with internationally recognized standards.

Medidata remains poised to respond/restrict access if any potentially malicious activity is detected, or if Medidata is notified of any user credentials which are known to be compromised.

Keep in mind that one of the major risks associated with a site compromise is if a full set of credentials (user ID and password) have been compromised during the incident - AND multi-factor authentication has not been required of the User. In these cases malicious activity would be harder to detect, as detection is then based on behavioral analytics.

For this reason Medidata does request that our customers remain vigilant in the administration of access to their data from these and any other sites. If any client believes that a user with access to a study has had their credentials compromised, the follow actions should be taken immediately:

- **Remove the users from the sites** - This will temporarily disable the site's ability to log into iMedidata and access Rave. Be careful to understand whether any valid work for active (or soon to be active patients) will potentially be impacted before taking action.
- **Remove any unnecessary users** - Only allow access to essential users that need to remain active in Rave. If their primary email is no longer accessible, then they will need to provide an alternative email address.
- **Require multi-factor authentication for any access**

Access should only be restored when the customer is confident that a user account is no longer compromised, and they are working from a secure workstation.

Security Incidents at Study Sites

Statement date 16-Mar-2023

Medidata is aware of the recent series of cybersecurity incidents at sites which are supporting clinical trials being conducted on our Platform.

Specifically:

- Hospital Clínic de Barcelona (incident on 05-Mar-2023)
- CHRU Brest (incident on 11-Mar-2023)
- Dr. De Wit (incident reported on 16-Mar-2023)

Proactively, Medidata/Dassault Systemes has conducted a review of the access to our customer's data, including any access that has been granted to personnel at these sites, with no anomalies noted.

Medidata remains poised to respond/restrict access if any potentially malicious activity is detected, or if Medidata is notified of any user credentials which are known to be compromised.

Medidata has neither identified malicious activity related to these breaches, nor has Medidata been notified of specific compromises outside of our network which impact Medidata.

Medidata does request that our customers remain vigilant in the administration of access to their data from these and any other sites. If any client believes that a user with access to a study has had their credentials compromised, the follow actions should be taken immediately:

- **Remove the users from the sites** - This will temporarily disable the site's ability to log into iMedidata and access Rave. Be careful to understand whether any valid work for active (or soon to be active patients) will potentially be impacted before taking action.
- **Remove any unnecessary users** - Only allow access to essential users that need to remain active in Rave. If their primary email is no longer accessible, then they will need to provide an alternative email address.
- **Require multi-factor authentication for any access**

Access should only be restored when the customer is confident that a user account is no longer compromised, and they are working from a secure workstation.

Statement date 10-Mar-2023

Medidata's Information Security team is aware of the security incident at the Hospital Clínic de Barcelona on 05-Mar-2023.

Medidata continuously monitors User activity and access to our hosted services.
A review of all Users associated with the Hospital Clínic de Barcelona is currently underway and will include the analysis of all activity for potentially malicious actions.

To date Medidata has identified no cases of undue access to our hosted services using credentials which may have been compromised during this security incident.

If any client believes that a User with access to a study has had their credentials compromised, the follow actions should be taken immediately:

- **Remove the users from the sites**. This will temporarily disable the site's ability to log into Rave. Be careful to understand whether any valid work for active (or soon to be active patients) will potentially be impacted before taking action.
- **Remove any unnecessary users from Rave** and add back in essential users that would need to remain active in Rave with an alternative email address that they would need to provide.