Risk assessment of a local clinical Matchmaker Exchange implementation: A route to regulatory approval

Sharmini Alagaratnam[1], Tor Solli-Nowlan[2], Tony Håndstad[2]
[1] Precision Medicine programme, Group Technology and Research, DNV GL, 1363 Høvik, Norway
[2] Department of Medical Genetics, Oslo University Hospital, 0424 Oslo, Norway

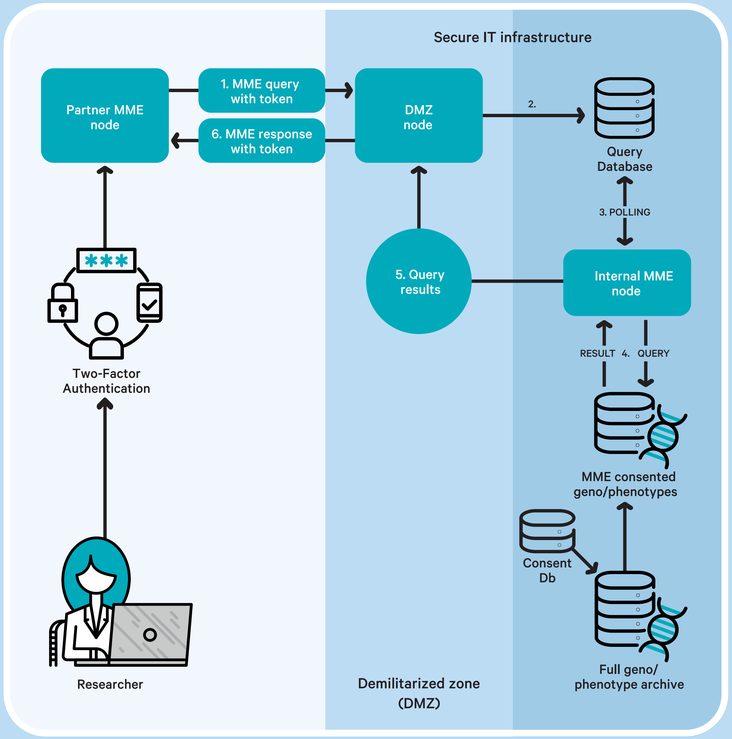
sharmini.alagaratnam@dnvgl.com

Motivation The Matchmaker Exchange (MME) federated network allows participating nodes to send queries detailing a genotype and accompanying phenotype to each other using standardized APIs, with the aim of identifying similar or matched cases to aid diagnosis of rare diseases.

MME has recently been implemented for consented samples at Oslo University Hospital (OUS) in Norway, in the first instance by connecting with one other partner node. A condition of this service going live is approval by the OUS Information Security Officer, using a **risk assessment** approach.

This poster describes the methodology applied and the subsequent risks uncovered associated with this MME implementation, as well as the mitigating measures proposed.

Implementation MME queries and responses are split in this implementation of MME as the secure IT infrastructure does not allow querying and response in a single session for security reasons.



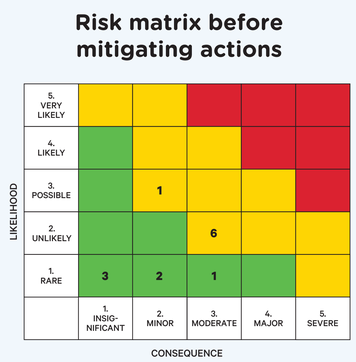
Methodology

Risks identification and analysis A total of 13 risks were identified, 7 in the intermediate risk area and 6 in the low risk area of the matrix, while none were identified in the high risk area. The 13 risks could be categorized as follows:

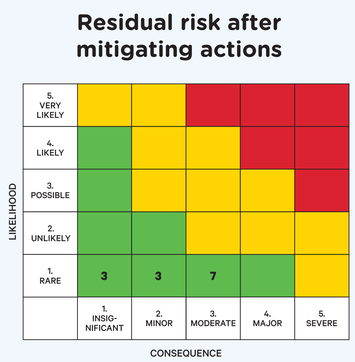
- 2 Access and authorization to the secure IT infrastructure
- 5 Organizational and architectural issues, segregation of duties
- 5 Access and authorization within the secure IT infrastructure
- 1 Access and authorization at partner node

Mitigating actions were identified for intermediate risks, after which risks were reassessed. All risks then mapped to the low risk area. Mitigating actions were assigned to specific individuals based on their role for implementation.

Risk matrix before mitigating actions



Residual risk after mitigating actions



MME-specific conclusions

Data available for MME is limited automatically by electronic consent, ensuring that patient preferences are quickly acted upon and only consented data is available for MME.

The higher risks identified map to the access interface between the secure MME database and partner nodes, and organizational and architectural issues.

The lower risks map almost exclusively to internal access and authorization issues.

Clear segregation of duties between the clinical unit implementing MME and the secure IT infrastructure hosting it facilitates best practice in testing, deployment and production.

General conclusions

The implementation of a solution developed for research into a clinical setting imposes regulatory requirements which may be challenging to fulfill due to continuing development of the research solution.

This is exacerbated by the often complex infrastructural landscape between research and clinic in which the solution will be implemented, with varying security and architectural needs.

Despite this, the risk assessment approach is accepted and can be applied as a route for gaining approval for similar services within healthcare settings.

Periodic risk reassessment may potentially overcome the dynamic nature of the service implemented.