1. *Consider the NorthChem scenario in the Appendix. Produce a report for the managing director of the company elaborating on the professional, legal and ethical issues that need to be considered and make any recommendations that you think are appropriate for development and management of the database for NorthChem.*

The concept of database design and management must be seen as a process that commences prior to initial steps in database design, and one that must be maintained rigorously and constantly once system is in production mode. Understanding the complexities of the organizational data must incorporate necessary procedures that will ensure safe, secure and optimized process for data access and storage.

As a first step, organization must ensure existence of clear procedures guiding the provision of access levels to users. The process should result in environment where users can access the minimum data needed for execution of tasks related to their type of work. This is achieved through incorporation of authentication, authorization and access level mechanisms so protecting the data from unauthorized access. Suitable username and password protection system must be designed and implemented at each system point where user interaction involves data extraction and/or manipulation. The authentication system must deliver strong protection tolls against unauthorized accesses through social engineering and/or brute force attacks. The user access level needs to be linked to data sets and entities in the database according to its role, usually including table columns, views or rows selection. One must comprehend the vastness of task in confirming the exact needs of each user within the organization and producing a correct database protocols. The process is multi-leveled and firstly incorporates clarification of roles, connection of roles to data sets and connection of roles to the organizational personnel. Once this is achieved, the system must be maintained in the environment where staff turnover, movement of personnel within the organization and shifting of responsibilities are driven by the realities of any organization.

Furthermore, the data architecture must be analyzed for any security breaches or vulnerabilities of the system. The organization must establish a thorough audit process that will scrutinize the risk potential and define the likelihood of data being breached or accessed in malicious manner. The audit process will inevitably require resources, both human and financial, in closing off the security threats. This will incorporate a number of possible tolls, such as firewalls, encryption of sensitive data, row level security (e.g. usage of SQL views), concept of access control (i.e. granting and revoking privileges), etc.

Next step is to ensure that suitable back-up facilities are available, so granting capability to organization to recover from system failures and security breaches. Such facilities must be capable to receive data repeatedly, provide safety mechanisms for data storage and ability to support operational applications in the organization without business interruptions. Both actual database system and its backup facilities need to provide audit trail and log files, so tracking down user interactions and data changes within the organization.

Organisation also needs to take into consideration the increased exposure of data through internet access and data sharing online. In such environment, security breaches can come from variety of actors and access points. As more and more databases are accessible via online-based applications, data becomes further exposed to attacks. The organization must address such weaknesses by implementing optimized web systems that reduce the risks such as SQL attacks. This will require implementation of tools for input validations, such as white and black lists, and usage of parameterized queries that ensure internally-defined parameters are confirmed when filling prepared SQL statements.

Moreover, organization must analyze data management and confirm that legal and ethical regulations are abided by through privacy measures incorporated in the system. Firstly, this needs to be established in all the interactions and data sharing with third party actors. Through data sharing, organization must be aware that control of the data and its usage is no longer control through its processes. However, that often does not result in removal of responsibility for data protection and organization will be called to burden the responsibility in acts of data mismanagement by third parties. The upcoming GDPR strengthens the measures utilized for data protection and privacy laws thus reinforcing the importance of proper data management within and between organisations. Process synchronization will entail procedures in protecting sensitive data. It will also require organization to review the contract details with third parties and ensure full acceptance of stringent data protection. The overall approach must ensure privacy ensured through correct organizational policy and system architecture.

Also, organization must address privacy concerns in relation to data mining. In the current environment, data mining techniques are very effective so being able to pierce through sanitized databases. The organization approach must have at its disposal the tools to modify the data so reducing the confidence of sensitive data sets. Another option at the disposal is data sampling that will ensure data released is opted in such way as to guarantee that any reading from the data produces a low degree of confidence.

While the above proposals list solely major areas of concern for the organization, it clearly describe a complex and resource-heavy process. The key to its successful implementation is focus on safety / privacy measures in early stages of system conceptualization and design. To deliver security and privacy of data, guiding principles for their implementation must be incorporated throughout the system development lifecycle, especially in processes dealing with concept development, analysis, design and implementation. Appropriate DBMS and application set of tools will add to overall task in ensuring compliant data management process.

**References:**

1. Bertino, E., Ji-Won B., and Ninghui L () Privacy-Preserving Database Systems, Department of Computer Science and Cerias, Purdue University. Available at: <http://people.cs.aau.dk/~simas/teaching/privacy/275agh936b763r6r.pdf> (Accessed on 27/02/2018).
2. Coy, P., S. (2008) Security Implications of the Choice of Distributed Database Management System Model: Relational vs. Object-Oriented. Available at: <https://csrc.nist.gov/csrc/media/publications/conference-paper/1996/10/22/proceedings-of-the-19th-nissc-1996/documents/paper072_073_074/sco_.pdf> (Accessed on 27/02/2018).
3. Hamed, A., A., and Helal, A., A. (2012) Security in Database Systems, *Global Journal of Computer Science and Technology Network, Web & Security*, Volume 12 Issue 17 Version 1.0. Available at:

<https://globaljournals.org/GJCST_Volume12/3-Security-in-Database-Systems.pdf> (Accessed on: 26/02/2018).

1. Hoepman, J., H. (2012) Privacy Design Strategies. Available at: <https://www.cs.ru.nl/~jhh/publications/pdp.pdf> (Accessed on: 26/02/2018).
2. Murray, M., C. (2010) Database Security: What Students Need to Know, *Journal of Information Technology Education: Innovations in Practice*, Volume 9, 2010. Available at:

<http://www.jite.org/documents/Vol9/JITEv9IIPp061-077Murray804.pdf> (Accessed on: 28/02/2018).

1. Mustafa Canim, M., and Kantarcioglu, M. (2007) Design and Analysis of Querying Encrypted Data in Relational Databases. Available at: <https://www.utdallas.edu/~muratk/publications/encdb.pdf> (Accessed on: 28/02/2018).
2. Sittig, D., F. (2011) Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3065078/> (Accessed on: 25/02/2018).
3. Swayer P., A., Jelati, G., D., Thuraisingham, B., M. (1987) Multi-level Security in Database Management Systems. Available at: <https://pdfs.semanticscholar.org/e97c/77b67796a6707a8a5e213ffbd03a6085ebd0.pdf> (Accessed on: 27/02/2018).