Mobile Learning System (MLS) is facing new challenges in terms of privacy, such as data collection, storage, and sharing because of the core infrastructure and network that enables cloud computing services. Most of the data exchange in Mobile Learning System (MLS) require mandatory authorisation to allow access to the learners’ information in the MLS. Therefore, this article attempts to rank learners' sensitive attributes stored in MLS. Thus, concerns about privacy breaches motivated this paper to adopt an attributes partitioning strategy into the sensitive attributes to enforce privacy during learners’ profile information access. The article adopted the informed consent phenomenon to determine and formulate learners’ data privacy attributes sensitivity using the Fuzzy Analytic Hierarchy Process (FAHP) Algorithm. Results from the implemented Learners’ Privacy Preserving (LPP) Algorithm determined normalized weights of top-five rank-selected learners’ sensitive data to include: Browsing History (1ST, Ranked), Geolocation Data (2ND, Ranked), IP Address (3RD, Ranked), web Browser (4TH, Ranked), Medical Records (5TH, Ranked) and CGPA (10TH, Ranked) respectively. This indicates that these five most sensitive features are at risk and require protection to prevent privacy breaches, thus ensuring privacy preservation that prevents unauthorised access to learners’ sensitive data in the mobile learning system environment. The ranking of sensitive data in this paper could serve as inspiration for future research work on mobile learning security to improve the privacy of sensitive attributes in MLS environment