**Paper 1: "Federated Learning Framework for Privacy-Preserving Healthcare Applications"**  
*Link:* <https://www.sciencedirect.com/science/article/abs/pii/S0926580524002929>  
*Type:* Theoretical[medium.com+6arxiv.org+6github.com+6](https://arxiv.org/abs/2012.07183?utm_source=chatgpt.com)

**Algorithms Used:**

* Federated Learning (FL) Framework: The study proposes a privacy-preserving FL framework tailored for healthcare applications. It emphasizes secure aggregation techniques and local data retention to ensure compliance with data protection standards.
* Machine Learning Models: The framework is designed to support various machine learning models, allowing for decentralized training across multiple healthcare institutions.

**Datasets Used:**

* The paper is theoretical in nature and does not specify the use of any particular dataset. It focuses on the architectural design and privacy aspects of the proposed FL framework.

**Contribution to your project:**

* **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Provides a foundational framework emphasizing data privacy and security, crucial for handling sensitive healthcare data.
* **Objective 3 (Implement and Evaluate FL Models for Well-being Prediction):** Offers insights into implementing FL in healthcare settings, which can be adapted for employee well-being monitoring.

**Paper 2: "Privacy Preservation for Federated Learning in Health Care"**  
*Link:* <https://www.sciencedirect.com/science/article/pii/S2666389924000825>  
*Type:* Theoretical[medium.com+6arxiv.org+6github.com+6](https://arxiv.org/abs/2012.07183?utm_source=chatgpt.com)

**Algorithms Used:**

* Federated Learning (FL) Framework: The paper discusses privacy preservation strategies within FL, focusing on techniques like differential privacy and homomorphic encryption to mitigate data leakage risks.
* Security Protocols: Emphasizes the integration of advanced cryptographic methods to enhance data confidentiality during model training.

**Datasets Used:**

* As a theoretical study, it does not utilize specific datasets but discusses the applicability of privacy-preserving techniques in healthcare data scenarios.

**Contribution to your project:**

* **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Highlights advanced privacy techniques that can be incorporated into your FL framework.
* **Objective 2 (Well-being Indicators):** Provides a foundation for understanding how to protect sensitive physiological data collected from wearables.

**Paper 3: "A Survey on Federated Learning for Healthcare: Concepts, Challenges, and Applications"**  
*Link:* <https://dl.acm.org/doi/10.1145/3700838.3703679>  
*Type:* Theoretical[arxiv.org+1researchgate.net+1](https://arxiv.org/abs/2012.07183?utm_source=chatgpt.com)

**Algorithms Used:**

* Comprehensive Survey: The paper presents a survey of various FL algorithms applied in healthcare, including FedAvg, FedProx, and personalized FL approaches.
* Challenges Addressed: Discusses issues like data heterogeneity, system scalability, and regulatory compliance in FL implementations.

**Datasets Used:**

* The survey references multiple datasets used in FL research, such as MIMIC-III and PhysioNet, but does not conduct new experiments.

**Contribution to your project:**

* **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Offers a broad understanding of existing FL frameworks and their applicability to healthcare.
* **Objective 3 (Implement and Evaluate FL Models for Well-being Prediction):** Provides insights into the challenges and solutions in deploying FL models in real-world scenarios.

**Paper 4: "Federated Learning for Secure and Privacy-Preserving Medical Image Analysis in Decentralized Healthcare Systems"**  
*Link:* <https://www.researchgate.net/publication/384592561_Federated_Learning_for_Secure_and_Privacy-Preserving_Medical_Image_Analysis_in_Decentralized_Healthcare_Systems>  
*Type:* Practical

**Algorithms Used:**

* Federated Learning (FL) Framework: Implements a decentralized FL approach for medical image analysis, incorporating secure aggregation and differential privacy.
* Encryption Techniques: Utilizes advanced encryption methods to ensure data security during model training across multiple healthcare institutions.

**Datasets Used:**

* The study employs real-world medical imaging datasets from various healthcare institutions to evaluate the FL system's performance.

**Contribution to your project:**

* **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Demonstrates the practical application of FL in handling sensitive medical data securely.
* **Objective 3 (Implement and Evaluate FL Models for Well-being Prediction):** Provides a case study on deploying FL in decentralized settings, relevant for employee well-being monitoring.
* **Objective 2 (Well-being Indicators):** Highlights the use of medical imaging data, which can be analogous to physiological data from wearables.

**Paper 5: "Privacy-Preserving Decentralized Learning Methods for Biomedical Applications"**  
*Link:* <https://pmc.ncbi.nlm.nih.gov/articles/PMC11408144/>  
*Type:* Theoretical

**Algorithms Used:**

* Decentralized Learning Frameworks: The paper reviews various decentralized learning methodologies, including federated learning, split learning, swarm learning, gossip learning, and edge learning, focusing on their applications in biomedical contexts.
* Privacy-Preserving Techniques: Discusses the integration of privacy-preserving methods within these decentralized frameworks to enhance data security.[pmc.ncbi.nlm.nih.gov+1researchgate.net+1](https://pmc.ncbi.nlm.nih.gov/articles/PMC11408144/?utm_source=chatgpt.com)

**Datasets Used:**

* As a review article, it does not utilize specific datasets but analyzes existing studies and their methodologies.

**Contribution to your project:**

* **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Provides a comprehensive overview of decentralized learning approaches, aiding in the selection of suitable frameworks for your project.
* **Objective 3 (Implement and Evaluate FL Models for Well-being Prediction):** Offers insights into the practical challenges and considerations in implementing decentralized learning in biomedical applications.
* **Objective 4 (Sustainability and Green Computing):** Discusses the efficiency and scalability of decentralized learning methods, relevant for sustainable system design.

Contribution to your project:

* + Directly informs Objective 3 (Implement and Evaluate FL Models for Well-being Prediction): This paper demonstrates the practical application of FL with real-world wearable sensor data for stress prediction, a central element of your employee well-being monitoring.
  + Supports Objective 1 (Develop a Privacy-Preserving FL Architecture): Highlights the core FL principle of keeping raw data local, crucial for protecting sensitive physiological information.
  + Informs Objective 2 (Well-being Indicators): Utilizes "biomechanical data" (e.g., EDA, movement patterns), aligning with your project's focus on physiological indicators from wearables.

**Paper 6: "Federated Learning for Privacy-Preserving Healthcare Data Analysis"**

**Link:** <https://www.researchgate.net/publication/390958370_Federated_Learning_for_Privacy-Preserving_Healthcare_Data_Analysis>  
**Type:** Practical[sciencedirect.com+32arxiv.org+32sciencedirect.com+32](https://arxiv.org/abs/2304.13360?utm_source=chatgpt.com)

* **Algorithms Used:**
  + Federated Learning (FL) Framework: Implements a decentralized learning approach to train models across multiple healthcare institutions without sharing raw data.
  + Privacy-Preserving Techniques: Incorporates differential privacy and secure aggregation methods to ensure data confidentiality during model training.[arxiv.org](https://arxiv.org/abs/2412.00687?utm_source=chatgpt.com)
* **Datasets Used:**
  + Utilizes multi-institutional medical datasets to evaluate the performance and privacy aspects of the proposed FL framework.[researchgate.net](https://www.researchgate.net/publication/390958370_Federated_Learning_for_Privacy-Preserving_Healthcare_Data_Analysis?utm_source=chatgpt.com)
* **Contribution to your project:**
  + **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Demonstrates a practical implementation of FL that maintains data privacy across institutions.
  + **Objective 3 (Implement and Evaluate FL Models for Well-being Prediction):** Provides insights into deploying FL models in real-world healthcare settings.

**Paper 7: "Federated Learning in Healthcare: Privacy-Preserving AI for Secure Medical Data Analysis"**

**Link:** <https://www.researchgate.net/publication/389216896_Federated_Learning_in_Healthcare_Privacy-Preserving_AI_for_Secure_Medical_Data_Analysis>  
**Type:** Theoretical

* **Algorithms Used:**
  + Federated Learning (FL) Framework: Discusses the theoretical underpinnings of FL in the context of healthcare data analysis.
  + Security Mechanisms: Explores various privacy-preserving techniques, including differential privacy and homomorphic encryption, within FL systems.[researchgate.net+1sciencedirect.com+1](https://www.researchgate.net/publication/390958370_Federated_Learning_for_Privacy-Preserving_Healthcare_Data_Analysis?utm_source=chatgpt.com)
* **Datasets Used:**
  + As a theoretical study, it does not utilize specific datasets but provides a comprehensive analysis of FL applications in healthcare.
* **Contribution to your project:**
  + **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Offers a foundational understanding of FL's role in secure medical data analysis.
  + **Objective 2 (Well-being Indicators):** Discusses potential applications of FL in monitoring various health indicators while preserving patient privacy.

**Paper 8: "Federated Learning for Privacy-Preserving Medical Data Sharing in Drug Development"**

**Link:** <https://www.researchgate.net/publication/385144298_Federated_Learning_for_Privacy-Preserving_Medical_Data_Sharing_in_Drug_Development>  
**Type:** Practical[sciencedirect.com+32arxiv.org+32sciencedirect.com+32](https://arxiv.org/abs/2304.13360?utm_source=chatgpt.com)

* **Algorithms Used:**
  + Federated Learning (FL) Framework: Applies FL to facilitate collaborative model training across pharmaceutical institutions without sharing raw data.
  + Privacy-Preserving Techniques: Utilizes differential privacy and secure multi-party computation to protect sensitive drug development data.[researchgate.net+1dl.acm.org+1](https://www.researchgate.net/publication/384592561_Federated_Learning_for_Secure_and_Privacy-Preserving_Medical_Image_Analysis_in_Decentralized_Healthcare_Systems?utm_source=chatgpt.com)[arxiv.org+1researchgate.net+1](https://arxiv.org/abs/2412.00687?utm_source=chatgpt.com)
* **Datasets Used:**
  + Employs proprietary datasets from various pharmaceutical companies to evaluate the efficacy of the FL approach in drug development.
* **Contribution to your project:**
  + **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Demonstrates the application of FL in a sensitive data-sharing environment.
  + **Objective 3 (Implement and Evaluate FL Models for Well-being Prediction):** Provides a case study on deploying FL in a real-world, privacy-sensitive domain.

**Paper 9: "Federated Learning with Differential Privacy for Breast Cancer Diagnosis: Enabling Secure Data Sharing and Model Integrity"**

**Link:** <https://www.researchgate.net/publication/390838080_Federated_learning_with_differential_privacy_for_breast_cancer_diagnosis_enabling_secure_data_sharing_and_model_integrity>  
**Type:** Practical[dl.acm.org+26sciencedirect.com+26sciencedirect.com+26](https://www.sciencedirect.com/science/article/pii/S2001037024000382?utm_source=chatgpt.com)

* **Algorithms Used:**
  + Federated Learning (FL) Framework: Implements FL to train models for breast cancer diagnosis across multiple institutions.
  + Differential Privacy: Integrates differential privacy mechanisms to ensure patient data confidentiality during model training.
* **Datasets Used:**
  + Utilizes breast cancer datasets from various medical institutions to validate the FL approach's effectiveness and privacy preservation.
* **Contribution to your project:**
  + **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Provides a practical example of FL application in sensitive medical diagnostics.
  + **Objective 3 (Implement and Evaluate FL Models for Well-being Prediction):** Offers insights into deploying FL models for disease prediction while maintaining data privacy.

**Paper 10: "Privacy-Preserving Edge Federated Learning for Intelligent Mobile-Health Systems"**

**Link:** <https://arxiv.org/abs/2405.05611>  
**Type:** Practical[researchgate.net+1researchgate.net+1](https://www.researchgate.net/publication/389216896_Federated_Learning_in_Healthcare_Privacy-Preserving_AI_for_Secure_Medical_Data_Analysis?utm_source=chatgpt.com)

* **Algorithms Used:**
  + Edge Federated Learning (FL) Framework: Proposes an FL approach tailored for resource-constrained mobile health (mHealth) devices.
  + Privacy-Preserving Techniques: Incorporates lightweight encryption and secure aggregation methods suitable for edge devices.[arxiv.org+1sciencedirect.com+1](https://arxiv.org/abs/2405.05611?utm_source=chatgpt.com)
* **Datasets Used:**
  + Employs real-world mHealth datasets, including wearable sensor data, to evaluate the proposed FL framework's performance and privacy aspects.
* **Contribution to your project:**
  + **Objective 1 (Develop a Privacy-Preserving FL Architecture):** Demonstrates the feasibility of implementing FL on edge devices with limited resources.
  + **Objective 3 (Implement and Evaluate FL Models for Well-being Prediction):** Provides a practical framework for deploying FL in mobile health applications, relevant for employee well-being monitoring.