Michael Kohronas
iSeeU EyeCare

1. **Using the Function column in the NIST Privacy Framework CORE document (Identify-P, Govern-P, Control-P, Communicate-P, and the Protect-P), describe how each selected function can add value and benefits to your company's specific situation.**

- Identity-P:
    - Developing a detailed understanding of how data is processed across various systems (front desk, examination rooms, fitting area, servers) is crucial for managing privacy risks effectively. This function can help iSeeU Eyecare inventory and map data processing activities, ensuring that privacy risks are identified and managed proactively.
- Govern-P:
    - Implementing a robust governance structure is key to ensuring that privacy risks are managed in alignment with the company's privacy values, regulatory requirements, and business objectives. This will help iSeeU Eyecare develop and maintain privacy policies and procedures that are crucial for the franchise model and for ensuring consistent privacy practices across locations.
- Control-P:
    - Establishing appropriate data processing policies and procedures will enable iSeeU Eyecare to manage data with sufficient granularity. This is particularly important for managing patient information, processing payments securely, and ensuring the confidentiality and integrity of patient records.
- Communicate-P:
    - Enhancing transparency and communication around data processing practices can build trust with patients and stakeholders. This function is essential for iSeeU Eyecare to effectively communicate its privacy practices and manage privacy-related inquiries and complaints.
- Protect-P:
    - Implementing strong data protection measures is essential for safeguarding sensitive patient data and ensuring the resilience of iSeeU Eyecare's IT infrastructure. This function addresses the need for robust security controls, such as access controls, data encryption, and incident response capabilities.

2. **Using the Category column in the document, select one category for each function that offers the most benefit to your company. You should have a total of five of the most beneficial categories listed for your company. Describe how each of the selected categories can add value to your company's privacy.**

- Identity-P:
    - Inventory and Mapping (ID.IM-P) can help iSeeU Eyecare understand and map all data processing activities, crucial for managing privacy risks across its operations.

- Govern-P:
    - Governance Policies, Processes, and Procedures (GV.PO-P) are essential for establishing a privacy governance framework that aligns with iSeeU Eyecare's business model and compliance requirements.
- Control-P:
    - Data Processing Policies, Processes, and Procedures (CT.PO-P) ensure that all data processing activities are conducted in accordance with established privacy policies and regulatory requirements.
- Communicate-P:
    - Communication Policies, Processes, and Procedures (CM.PO-P) are critical for maintaining transparency about iSeeU Eyecare's data processing practices and privacy risks.
- Protect-P:
    - Identity Management, Authentication, and Access Control (PR.AC-P) is crucial for ensuring that only authorized individuals can access sensitive patient data, thereby protecting against unauthorized access and breaches.

3. **Using the Subcategory column in the document, select one subcategory for each category you selected in item 2 above that offers the most benefit to your company. You should have a total of five of the most beneficial subcategories listed for your company. Describe how each of the selected subcategories can add value to your company's privacy.**

- ID.IM-P8: Implementing a comprehensive data mapping solution that illustrates all data actions and interactions, enhancing the management of privacy risks.
- GV.PO-P5: Developing a privacy training program for employees and contractors to ensure they understand legal and regulatory requirements related to privacy.
- CT.PO-P4: Integrating data life cycle management with the system development life cycle to enhance data privacy throughout the data's life span.
- CM.PO-P1: Establishing a patient privacy notice that clearly communicates data processing purposes, practices, and privacy risks.
- PR.AC-P4: Deploying a role-based access control system to manage access permissions and enforce the principle of least privilege.

4. **For each of the items, you selected in item 3 above, describe a security control (policy, procedure, hardware, or software) that could be used to help with your company's privacy.**

- Risk Assessment (ID.RA-P4): Prioritizing privacy risks based on the likelihood and impact of problematic data actions can guide iSeeU Eyecare in implementing targeted risk mitigation strategies.
- Data Security (PR.DS-P1): Protecting data-at-rest through encryption can prevent unauthorized access to patient information stored on servers and devices.

- Awareness and Training (GV.AT-P1): Informing the workforce about their privacy responsibilities is essential for ensuring that all employees contribute to the privacy posture of iSeeU Eyecare.
- Monitoring and Review (GV.MT-P1): Continuously re-evaluating privacy risks and adapting privacy practices can help iSeeU Eyecare maintain an effective privacy program, especially as the business expands and technology evolves.

5. **Using the Subcategory column in the document, select four other subcategories that offer the most benefit to your company. Describe how each of these additional subcategories can add value to your company's privacy.**

- Risk Assessment (ID.RA-P4): Evaluating problematic data actions and their impacts helps iSeeU prioritize privacy risks, ensuring resources are allocated effectively to mitigate the most critical vulnerabilities.
- Data Security (PR.DS-P1): Protecting data-at-rest through encryption safeguards patient information against unauthorized access, enhancing the confidentiality and integrity of sensitive data.
- Awareness and Training (GV.AT-P1): Providing privacy awareness education to the workforce empowers employees to handle personal information responsibly, reducing the risk of data breaches.
- Monitoring and Review (GV.MT-P1): Continuous monitoring and periodic reviews of the privacy posture enable iSeeU to adapt to new threats and regulatory changes, maintaining a robust privacy program.

6. **Using the Category column in the document, select one category for each function that offers the least benefit to your company. You should have a total of five of the least beneficial categories listed for your company. Describe why each of the selected categories adds the least amount of value to your company's privacy.**

- Identify-P: For iSeeU Eyecare, a category like Business Environment (ID.BE-P) might offer less immediate value because the primary focus is on patient data processing and security, rather than broader business strategy discussions.
- Govern-P: Awareness and Training (GV.AT-P) might be seen as less critical in a small, specialized context where training can be more direct and informal, though it's important to note that awareness and training are critical for privacy.
- Control-P: Disassociated Processing (CT.DP-P) might be less applicable if iSeeU Eyecare does not engage in complex data processing that requires advanced disassociation techniques.
- Communicate-P: Data Processing Awareness (CM.AW-P) could be perceived as less beneficial if there's already a high level of transparency and direct communication with patients.

- Protect-P: Maintenance (PR.MA-P) might be less critical compared to other categories if the company outsources IT maintenance and focuses more on proactive security measures.

7. **Using the Subcategory column in the document, select one subcategory for each category you selected in 2, that offers the least benefit to your company. You should have a total of five of the least beneficial subcategories listed for your company. Describe how each of the selected subcategories adds the least amount of value to your company's privacy**

- ID.BE-P3: Identifying systems/products/services that support organizational priorities might be less beneficial if iSeeU Eyecare's technology needs are straightforward and stable.
- GV.AT-P4: Understanding roles and responsibilities for third parties might be deemed less critical if iSeeU Eyecare operates with a small, trusted network of vendors and partners.
- CT.DP-P5: Substitute attribute references for attribute values could be less beneficial if iSeeU Eyecare already minimizes data collection and processing to essential elements only.
- CM.AW-P7: Notifying impacted individuals and organizations about a privacy breach is crucial, but it might be considered less beneficial if iSeeU Eyecare has robust preventative measures in place.
- PR.MA-P2: Remote maintenance of organizational assets being approved and logged might be less critical if most IT support and maintenance are performed on-site.