Risk Management Plan: Health-Data Privacy & Cybersecurity Safeguards

Gabrielle Holmes, Julius Miller, Mario Loyd Galvão-Wilson

1. Protected Health Information (PHI)

This project integrates continuous glucose monitoring data within EHR systems to improve chronic disease management for patients with Type I and II diabetes. The goal is to develop successful integration and develop an interface with dashboards, navigational options, and notification alerts that allow for patients and their healthcare providers to visualize, monitor, and respond promptly to changes in glucose levels.

Continuous glucose monitors, EHR systems, and our proposed project utilize protected health information (PHI). PHI according to HIPAA is any identifiable information related to the patient's health status collected, created or maintained in relation to healthcare, payment of health services, or use in health operations (1). Under this definition, this would include any information that could potentially identify the patient such as name, address, social security numbers, and date of birth. All of this information is typically associated with both EHR systems and CGMs.

HIPAA was developed in 1996 and set standards for health information privacy and security (1). The Privacy Rule established national standards for protected health information and is designed to balance the proper protection of private health information while allowing use of the health information to provide high-quality healthcare (2). On the other hand, the Security Rule establishes a set of standards of safeguards needed to secure and protect electronic health information (1). Together these two rules complement each other to define what information is

considered protected and establish rules and safeguards to keep this information private, secure and safe.

2. Health Information Exchange (HIE)

Health information exchange would be securely exchanged among users and healthcare providers within an HIE system through several established protocols. Much like many other EHRs, our project would incorporate a plan that features the best practices using a HIPAA API. [6]A HIPAA API acts as a messaging system that allows healthcare applications to request and receive information from a server over the internet. These interactions are automated and ensure secure communication without the user directly handling a third-party system. For HIPAA-compliant APIs, any data containing PHI must meet specific privacy and security requirements. PHI that has been de-identified or anonymized is exempt from these regulations, but all other healthcare data must follow HIPAA's strict guidelines.

Our plan includes robust encryption techniques, which would include encrypting data at rest and data in transit. We'd encrypt PHI during these stages to prevent unauthorized access. If the API interacts with a database containing PHI, the database would be encrypted as well. Access controls would be implemented within a HIPAA API, as only authorized personnel should be able to interact with the system. For our project, we would control this through role-based access lists. Another part of our plan would be regular security audits through audit logging. By logging every interaction with the API, healthcare providers would maintain transparency and accountability with patients. Regular review of these logs would help to prevent breaches as well. Finally, if an API interacts with an external provider or a public cloud,

it would de-identify patient data. Data de-identification would help to prevent the exposure of sensitive PHI within an HIE among care providers and healthcare systems.

To facilitate the speed and quality of patient care, we would incorporate at least two APIs that would promote interoperability between them to maximize efficiency and ultimately improve patient outcomes with our integrated CGM device. For our project, we would use a Fast Healthcare Interoperability Resources (FHIR) API and a Remote Patient Monitoring (RPM) API. FHIR APIs have become the standard for EHR exchange. They standardize data to allow easy integration across platforms. They support several healthcare applications, including patient engagement, telehealth, and HIEs. FHIR APIs work well when jointly combined with an RPM API, as the latter facilitates the exchange of real-time health data from wearable devices to healthcare providers. These help them in continuous patient monitoring outside clinical settings.

3. Compliance Plan:

Identification of a Compliance Officer: This person is responsible for monitoring regulations and standards set forth by HIPAA and is the point of contact for reports of incidents out of compliance (1). Ideally, this would be the healthcare practice's manager or administrator.

Policies Governing Routine Daily Operations:

Scheduling and Registration Policy: All electronic forms utilized for registering the patient in the EHR system and with the CGM system must be collected and stored securely. Additionally, patients will be provided with a copy of the privacy and security policies as they relate to HIPAA and consent for collection, use, and storage of data must be obtained from the patient.

System Access Policy: Access to computers, data collected by CGMs, EHR systems, and related equipment is restricted based on job descriptions, allowing only the necessary functions to complete daily tasks. Keeping credentials confidential, including log-in ID and password, is a requirement for all staff members. Failure to comply with these requirements will result in disciplinary action.

Release of Patient Information:

Patients must be informed about the protected health information that is collected by CGMs and stored within the CGM database, as well as the data shared between the CGM database and EHR systems. Patients must provide written authorization confirming that they authorize health data to be integrated from their CGM into their electronic health record. Only relevant information may be shared and only on a need-to-know basis. There are exceptions for this, including emergent treatment, public health purposes, or legal orders.

Breach of Confidentiality:

Breaches of confidentiality are any violations of set privacy and security standards and rules regarding protected health information set forth by HIPAA. It is required that any breach or suspected breach in confidentiality be reported immediately to the compliance officer. Any reported breach must be thoroughly documented and investigated by the compliance officer. Any patients impacted are informed regarding the breach as set forth by HIPAA's Breach Notification Rule. Disciplinary action for breaches are enforced based upon the severity of violations. Internal breaches, such as sharing password information with coworkers, could result in unauthorized access and breach of confidentiality. On the other hand, external breaches, sending patient data to an

unauthorized party, result in violation of a patient's privacy as well as HIPAA privacy laws.

Security Breaches:

Security breaches include any attack upon the electronic healthcare information. A proactive approach will be taken first to prevent security breaches by ensuring proper safeguards are taken to protect protected health data. In the event of a security breach, the compliance officer must be notified immediately, and an investigation will be launched. Mitigation strategies will be utilized to minimize the impact of the breach, including isolating impacted devices, revoking access, and halting the interface that integrates the CGM to EHR. All impacted patients will be promptly informed as mandated by HIPAA's Breach Notification Rule.

Coding and Billing

Billing and coding will be the responsibility of the providers and the billing/coding team at the healthcare facility, and these individuals must utilize ICD-10, CPT and HCPCS codes to remain in compliance with HIPAA. It is imperative that the healthcare providers are documenting accurate medical records in order to support medical necessity, ensure chart completeness and correctness and avoid fraudulent or abusive billing practices. The compliance officer is responsible for overseeing and ensuring compliant billing and coding practices.

Consequences for Breaking Compliance:

Incidents of noncompliance vary depending on severity and findings from the compliance officers' investigation of the incident. Incidents with minimal impact on privacy and security may result in re-education of policies and procedures. There may be fines or

legal consequences associated with more serious violations of compliance. Fines may range from $100 per single unintentional violation up to a maximum of $1.5 million per year (1).

4. EHR Integration Considerations:

The goal of this project is to create an interface that integrates CGM data into a patient's electronic health record. Selection of the EHR system will be a decision for the healthcare facility and should be tailored to the intent, needs and wants for the healthcare providers who may be utilizing our interface.

Intent of EHR:

There are pros and cons associated with selecting an EHR system that stands alone versus one that is integrated with PM software. For our project, the CGM and EHR systems stand alone, and our interface allows for seamless integration of data from the CGM system into the EHR system. PM integration is not a necessary feature in order for our interface to work, so ultimately this is a decision for the healthcare facility to make based on their wants and needs for PM functions.

Needs:

For our project to be successful, it will need to be easily implemented into various EHR systems to meet the needs of various healthcare facilities. Prior to implementation, we will need to assess all needs of the healthcare facility including existing clinical and administrative workflows in order for our interface to be seamlessly integrated.

Budget:

Healthcare facilities must consider the budget when selecting an EHR system, as well as when considering implementing new interfaces. As established in our feasibility analysis and requirements specification, it is believed that our proposed interface has cost-saving benefits that outweigh costs. Our interface serves as an opportunity to reduce healthcare costs associated with chronic disease management. Additionally, this project promotes interoperability that has the potential to improve the quality and efficiency of patient care. Thereby, potentially allowing for healthcare facilities to be eligible for incentives associated with the Promoting Interoperability Program, aka Meaningful Use, (1).

Staffing and Training:

Upon initial implementation of our project, all staff members of the healthcare facility will need to undergo an initial training course regarding use of our interface. We would like two individuals of the healthcare facility to be chosen to undergo additional training and serve as point of contact within the facility for any questions or concerns regarding usage of our system. Additionally, a yearly reeducation course will be provided to address any questions and receive feedback from users regarding usability and functionality.

5. Data Integrity

As our project will deal with sensitive patient health information, it's paramount that our project uphold a patient's data integrity. When dealing with a continuous glucose monitoring (CGM) device, data integrity ensures the accuracy, completeness, and reliability of the glucose data that has been collected, stored, and transmitted. These metrics are crucial for effective diabetes management.

CGMs need to have several error detection mechanisms to ensure accurate readings, and our project will have the same as well. These include built-in software checks, user-driven verification, and calibration protocols. Internal checks and controls are necessary to alert users of potential issues. Our project will rely on established algorithms to flag errors like unusual trends or inconsistencies in glucose level readings. It'll also incorporate internal tests to verify sensor functionality and to ensure it's working within established parameters as it's properly calibrated and integrated with the EHR.

Data validation checks play a role in ensuring the accuracy and reliability of patient data, which together uphold data integrity for better diabetes management. The FDA requirements for Integrated CGM devices stipulate that [3]at least 95% of measured glucose values should be within either ±15 mg/dL of the averaged comparison values at glucose concentrations <100 mg/dL or within ±15% at glucose concentrations ≥100 mg/dL. CGM devices have their own established metrics for consistency and reliability for monitoring glucose levels, which our project will also adopt. [4]These metrics are time in range (TIR), time in hypoglycemia (TIHypo), and time in hyperglycemia (TIHyper), which represent the complications from the extremes of patient glucose levels. The agreed-upon default TIR (from a CGM data standardization consensus conference) is 70–180 mg/dL, with the understanding that there may be circumstances in which the clinician or patient wants to set an alternative target TIR (e.g., 70–140 mg/dL during the night for patients on hybrid closed-loop therapy). For TIHypo, there are two CGM-defined cut points to define TIHypo and one clinically defined hypoglycemia level.

- Level 1: Glucose <70 mg/dL and ≥54 mg/dL, or 54–69 mg/dL
    - › Hypoglycemia alert level/low/need to monitor the situation
- Level 2: Glucose <54 mg/dL

› Clinically significant/very low/immediate action required

- Level 3. Severe hypoglycemia

› Altered mental and/or physical status requiring assistance

Levels <70 mg/dL are referred to as an alert for hypoglycemia, and those <54 mg/dL indicate a higher risk for individuals with known cardiovascular disease and are often associated with cognitive impairment.

For TIHyper, there are two CGM-defined cut points to define TIHyper and one clinically defined hyperglycemia level.

- Level 1: Glucose >180 mg/dL and ≤250 mg/dL, or 181–250 mg/dL

› Elevated or high glucose/need to monitor the situation

- Level 2: Glucose >250 mg/dL

› Clinically significant/very high/action required; consider correction of insulin bolus, check insulin pump infusion set, increase hydration, address illness or excess stress if present, and consider checking urine or fingerstick ketones if persistent.

- Level 3: Diabetic ketoacidosis

› Ketones, acidosis, and usually hyperglycemia

There isn't a single metric of time in range (TIR, TIHyper, or TIHypo) that can adequately characterize glucose control, but an ideal CGM target is to maximize TIR with minimal TIHypo.

6. Permissions Granting Plan

Permission Levels:

- **Administrative level:** IT administrators and compliance officers with full system access, including configuration tools and security controls. This level can create, modify, and revoke user accounts and permissions.
- **Provider level:** physicians, nurses, and PAs who are involved in care and require complete access to patient glucose data, analytics, and alerts. This level can set patient-specific glucose thresholds for alerts, access historical data, and have permissions for updating treatment plans.
- **Front office:** general staff and receptionists with limited access to patient demographic data for scheduling. This level has no access to CGM data or any treatment information.
- **Patient level:** for patients to access their own glucose data through the patient portal which allows access to personal glucose data, trends, and provider recommendations.

Approval Process:

The process for granting permissions within our CGM-EHR system:

1. **Initial Request:** Department managers submit formal access requests with the required access level based on job responsibilities. Documentation of staff credentials must accompany requests.
2. **Verification and Review:** A compliance officer reviews the access request against the job description and verifies that the necessary training has been completed.
3. **Approval Authority:** The appropriate authority approves access based on role level:

- Administrator level: Requires approval from the compliance officer and the IT director
- Provider level: Requires approval from the medical director and the compliance officer
- Front office level: Requires approval from the office manager
- Patient level: Automated process after identity verification

4. **Provisioning and Documentation:** IT staff provides access with documentation and permissions are recorded and timestamped.
5. **Periodic Review:** Quarterly audits to verify the continued necessity of all user permissions.

Revocation Procedures:

- **Termination of Employment:** Immediate removal of all system access immediately upon termination.
- **Role Change:** Review and adjustment of permissions to match new responsibilities, once requested.
- **Inappropriate Use:** Immediate suspension of non-vital permissions upon detection of suspicious activity, with investigation suggested to compliance.
- **Inactivity:** Review of accounts inactive for 30+ days with suspension after 90 days.

7. Security Audit

As our project will integrate an EHR for continuous glucose monitoring, audit findings are necessary to illustrate any security issues that may exist within the workflow for both the EHR and the wearable device. To properly plan for any vulnerabilities that may exist would require several methods to prevent a breach from occurring. First, our project will mandate secure access protocols to prevent unauthorized access from third parties. Only patients themselves and their healthcare providers actively involved in the long-term management of their diabetes should have access to patient data. These secure access protocols will involve robust encryption (for both data at rest and data in transit) and multi-factor authentication to enhance CGM device security.

After an audit is performed, to improve the security of the integrated CGM device, an audit trail analysis has to be performed. Through an audit trail analysis, we'll be able to identify and correct any gaps or weaknesses in our integrated CGM device. [5]For our risk management plan, we would adopt a risk-based approach to prioritize and focus on the most sensitive data and activities. We'd incorporate automated and integrated tools that would help to streamline the process, and use standardized templates to record and report results. Furthermore, we can incorporate benchmarks that measure the security of the integrated CGM device. Lastly, after the audit trail analysis has been completed, we would factor in the feedback that we've received periodically to enhance the security protocols and ensure that these updates are compliant with HIPAA's security rule. Regarding the last point, healthcare providers must comply with HIPAA to ensure patient data is secure and confidentiality is maintained.

8. Safeguarding Computer Hardware and Software Systems

Strict Vetting of Potential Employees:

To ensure trustworthiness of personnel with access to sensitive diabetes monitoring data, we plan to conduct criminal background checks and verify credentials for all staff with access. Staff must demonstrate understanding of data privacy regulations and HIPAA requirements. Additionally, mandatory security awareness training with a specific focus on diabetes data sensitivity is required for all employees.

Handling Sensitive and Restricted Access:

For role-based access controls and need-to-know information management, see item 6. We implement monitoring of data access patterns with automated flagging for any unusual

behavior. Security is further enhanced through multi-factor authentication for all system access and automatic session timeouts to prevent unauthorized usage.

Restrict Computer Access and Locations:

Our security approach includes secure server rooms with controlled access and entry badge requirements. Clinical areas are equipped with privacy screens and automatic locks to prevent unauthorized access. All remote connections require a VPN with device verification for added protection. We intend to separate clinical networks from administrative networks, with strong firewall protection between networks to prevent unauthorized data access.

Data Encryption and Employee Tracking:

All CGM data is protected through end-to-end encryption during transmission and at-rest encryption for stored information. The system assigns unique user IDs and maintains logs of all system interactions. Preventive measures include systems to block unauthorized data exports and email filtering to prevent PHI transmission.

Identify Threats and Safeguard Measures:

Our system safeguards against common cybersecurity threats, including malware, phishing, and man-in-the-middle attacks. We implement preventive measures like advanced endpoint protection and vulnerability scanning. Protection is enhanced through a multi-layer firewall and close monitoring. Password security includes complex password requirements, multi-factor authentication for any system access, as well as immediate account deactivation upon staff changes.

File Back-up Procedures:

Ideally, we can create backup procedures with real-time replication of critical CGM data with daily full backups. However, due to the consistency of the data stream, a cutoff will likely

be more reasonable from a technical standpoint. Our approach includes on-site, off-site, and encrypted cloud backup storage to ensure data safety. It is important to note that many continuous glucose monitoring devices utilize their manufacturer-provided cloud storage, which we intend to integrate alongside our backup strategy while maintaining our backup systems. All archives are retained for at least 6 years after their from the date they were last in effect, as required by HIPAA (7), ensuring compliance while maintaining a complete data history for patient care.

Disaster Recovery Plan:

Our disaster recovery plan encompasses critical components for operational continuity during a system failure. We maintain a comprehensive electronic functions inventory, including patient registration, CGM data collection, and clinical documentation. Our hardware and software inventory catalogs all servers, any connected workstations, the network infrastructure, our integration middleware, and the patient portals. Backup specifications detail multiple storage locations (on-site, off-site, and encrypted cloud storage), formats (encrypted database dumps and file backups), and schedules (daily complete backups). Our restoration procedures follow a step-by-step approach from team activation through hardware preparation, software restoration, data recovery, validation of system integrity, and end with system testing. All staff should undergo comprehensive security training, including annual refreshers, quarterly drills, and role-specific instruction for compliance purposes.

Evaluation Criteria:

We evaluate security through metrics including threat detection rates and incident response times. Regular compliance measurements should be conducted through both internal reviews and external audits to ensure regulations are followed and industry standards are met.

Additionally, we carefully balance security requirements with usability by monitoring how security controls impact workflows and analyzing authentication success rates.

9. Individual Contributions

Our team, consisting of Gabrielle, Julius, and Mario, has remained in contact regarding our project despite busy schedules and time zone differences. For this Risk Management Plan, Gabrielle completed the discussion of PHI, development of a compliance plan, and EHR considerations. Julius has completed sections discussing health information exchange, data integrity, and security audit. Finally, Mario completed sections discussing safeguards for both hardware and software as well as our plan for granting permissions. We will continue to work together in the next stage as we complete the wireframes and prototype for our project.

References:

1. *Integrated Electronic Health Records (Textbook with Connect), 4th Edition.* Shanholtzer/Ensign. McGraw-Hill Education. ISBN 978-1-260-08226-5

2. HHS. (2022). *Summary of the HIPAA privacy rule*. HHS.gov; U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

3. Freckmann, G., Pleus, S., Grady, M., Setford, S., & Levy, B. (2018). Measures of Accuracy for Continuous Glucose Monitoring and Blood Glucose Monitoring Devices. *Journal of Diabetes Science and Technology*, *13*(3), 575–583. https://doi.org/10.1177/1932296818812062

4. Bergenstal, R. M. (2018). *Understanding Continuous Glucose Monitoring Data*. PubMed; American Diabetes Association. https://www.ncbi.nlm.nih.gov/books/NBK538967/

5. *How do you monitor and audit EHR access and activity?* (n.d.). Www.linkedin.com. https://www.linkedin.com/advice/3/how-do-you-monitor-audit-ehr-access

6. Peremore, K. (2023). Why healthcare organizations should maintain both paper and digital records. *Paubox.com*. https://doi.org/1098040/CLEAN-6-1-theme_child

7. HIPAA Journal. (n.d.). HIPAA retention requirements. HIPAA Journal. Retrieved April 8, 2025, from https://www.hipaajournal.com/hipaa-retention-requirements/