The DiMe Seal

Evaluation Framework Criteria

DIGITAL MEDICINE SOCIETY

Updated XXX

Domain: Evidence

Criteria and benchmarks covering the process of producing or gathering data, information, and findings through research, clinical trials, studies, or other methods

Criteria group	Criteria
Evidence generation - Criteria covering the systematic approaches used to generate data demonstrating scientific validity and clinical evidence to support the product's claims	Patient outcomes - Attestations covering measurable effects, results, or consequences experienced by patients as a result of intervention or treatment by the product • EG 1.1 - One or more studies have been performed that show the validity, reliability, and generalizability of patient outcomes driven by the software components of your product • EG 1.2 - The study population is sufficiently diverse and/or representative of the patients for which the product intends to improve outcomes
	Comparative effectiveness - Attestations covering the evaluation of how well the product performs relative to other options in real world settings • EG 2.1 - The product's safety has been compared to other leading products/standards of care in the industry • EG 2.2 - The product's efficacy has been compared to other leading products/standards of care in the industry
Product impact - Criteria covering the effects, results, or consequences of use of the product on patients' health status, well-being, and quality of life	End user experience - Attestations covering how how users (such as healthcare professionals, patients, administrators, or caregivers) perceive and interact with the software • PI 1.1 - Potential risks associated with use of the product and their implications for the patient are clearly defined • PI 1.2 - A process is in place for patients to report risks or unintended consequences associated with using the product • PI 1.3 - Diverse stakeholders (e.g., clinicians, patients, caregivers) potentially affected by use of the product were engaged in its design, implementation, and evaluation • PI 1.4 - Behavioral analytics, including but not limited to user behavior, system activity patterns, and network traffic are captured and analyzed to identify potential impacts to end user and/or patient outcomes
	Cost measurement - Attestations covering the process of quantifying and assessing the expenses associated with the development, implementation, maintenance, and operation of the software • PI 2.1 - A cost analysis has been done for all paid products across a common baseline of direct and indirect costs

Domain: Privacy and Security

Criteria and benchmarks covering fundamental concepts that aim to protect users' data and ensure the confidentiality, integrity, and availability of software applications

Criteria group	Criteria
Continuous monitoring - Criteria covering the ongoing process of real-time surveillance, analysis, and assessment of data to detect, prevent, and respond to threats, vulnerabilities, and incidents associated with the software	Monitoring & analytics - Attestations covering practices and tools used to observe, measure, and analyze various aspects of software applications, systems, or infrastructure ● CM 1.1 - Monitoring is implemented in production environments to identify indications of a privacy breach ● CM 1.2 - Behavioral analytics, including but not limited to user behavior, system activity patterns, and network traffic are captured and analyzed to detect anomalous or suspicious activities indicative of security threats
Data governance - Criteria covering processes of gathering, storing, using, and managing health-related information while ensuring confidentiality, integrity, and privacy are in place throughout the lifecycle of the data collected by the product	Consent & authorization - Attestations covering voluntary agreements made by end users about how their data is collected, used, and distributed ● DG 1.1 - Consent is being obtained and information is provided on the data being collected, how the data will be managed and shared (including anonymization or de-identification, use for marketing purposes), how long the data will be stored, why data collection is necessary for the use of the software, and what data will be monetized ● DG 1.2 - A mechanism is in place to make users aware of updates to privacy policies, terms of service, and/or other end-user agreements. Whenever updates are made to privacy policies, terms of service, and/or other end-user agreements
	Data integrity & quality - Attestations concerned with the accuracy, reliability, and security of data as it is entered, stored, and retrieved. Additionally, the benchmarks evaluate if that data is relevant, accurate, and reliable ● DG 2.1 - There is a process for reviewing data quality and quality assurance processes are in place to ensure the accuracy, completeness, and integrity of data collected
	● Anonymization & deidentification - Attestations covering techniques and methods that purposefully break the link between data values and individuals ● DG 3.1 - Methods and reasons for anonymization, de-identification and re-identification are clear and adhere to HIPAA standards

Domain: Privacy and Security, cont.

Criteria and benchmarks covering fundamental concepts that aim to protect users' data and ensure the confidentiality, integrity, and availability of software applications

Criteria group	Criteria
Data governance - Criteria covering processes of gathering, storing, using, and managing health-related information while ensuring confidentiality, integrity, and privacy are in place throughout the lifecycle of the data collected by the product	Data retention - Attestations covering storage and maintenance of data for a specific period of time, determined by regulatory, legal, or business requirements ● DG 4.1 - All reasons for health data retention are clearly explained and no additional purposes will be allowed unless explicit consent is asked from the patient ● DG 4.2 - Users are informed of their rights regarding the retention and disposal of their data, including the right to request access, correction, or deletion of their information
	Data minimization - Attestations covering the specification of data elements necessary for providing the services associated with the use of the product ● DG 5.1 - The product only collects data elements that are necessary for performing its intended function or are reasonably associated with product monitoring or development efforts that are aligned with its intended function
	Access control - Attestations covering the process of selectively granting or denying access to data, systems, or physical locations based on the identity, role, or authorization level of the entity requesting ● DG 6.1 - Authorization mechanisms are used to determine the permissions and privileges granted to authenticated users and third party vendors based on their roles, responsibilities, and access rights ● DG 6.2 - Auditing and logging capabilities track and record access attempts, user activities, and security events
	Data encryption - Attestations covering processes and methods for ensuring sensitive information remains secure and unreadable to unauthorized users or attackers who might intercept the data ● DG 7.1 - Encryption is applied to data stored on devices, servers, databases, and other storage systems to protect it from theft, loss, or unauthorized access to physical or digital storage ● DG 7.2 - Data encryption mechanisms provide secure data transmission over networks

Domain: Privacy and Security, cont.

Criteria and benchmarks covering fundamental concepts that aim to protect users' data and ensure the confidentiality, integrity, and availability of software applications

Criteria group	Criteria
Education & awareness - Criteria covering educational initiatives and programs designed to educate product developers and other stakeholders about best practices, policies, and procedures for data security in digital health environments	Security training - Attestations covering educational programs and initiatives aimed at educating software developers, engineers, IT professionals, and other personnel involved in software development and deployment about cybersecurity best practices, principles, and procedures • EA 1.1 - Privacy and security training have been made available for all personnel with responsibilities that contribute to the development of your product, including but not limited to software and QA engineers, designers, product managers, and IT professionals
Health equity - Criteria covering the presentation of information for fair and equitable access and use of the software, regardless of socioeconomic status, academic attainment, age, or other factors	Consent - Attestations covering the permission or agreement given by a user for the collection, processing, and use of their personal data or for participating in certain activities facilitated by the product in a legally and ethically compliant manner • HE 1.1 - Privacy policy and terms of service information, including the process of collecting consent, is written at an 8th grade reading level
Secure software development lifecycle - Criteria covering a systematic approach to integrating security practices and measures throughout the software development process	Development infrastructure - Attestations covering the underlying framework, tools, and resources used to create, test, and deploy your product • SSDLC 1.1 - All forms of code – including source code, executable code, and configuration-as-code – are stored in a version controlled system based on the principle of least privilege so that only authorized personnel, tools, services, etc. have access
	Risk analysis - Attestations covering the process of identifying documenting, and validating the needs and expectations of stakeholders and the associated risks, as well as the strategies used to mitigate • SSDLC 2.1 - A risk assessment was conducted for every system (database or API, including any 3rd party services) required for the functioning of the product. These risk assessments should include, for each system profiled: Descriptions of specific vulnerabilities, Types of risk to the organization of this vulnerability is exploited, Threat sources that could take advantage of this vulnerability, Existing safeguards that reduce this risk, Likelihood of occurrence, Ownership of monitoring and addressing this risk

Domain: Privacy and Security, cont.

Criteria and benchmarks covering fundamental concepts that aim to protect users' data and ensure the confidentiality, integrity, and availability of software applications

Criteria group	Criteria
Secure software development lifecycle - Criteria covering a systematic approach to integrating security practices and measures throughout the software development process	Third-party dependencies - Attestations covering external components, libraries, frameworks, modules, or services that are utilized within the software. ● SSDLC 3.1 - Dependency inventory, i.e., software bill of materials
	Integration testing & validation - Attestations covering any testing techniques used to verify the interactions between integrated components or modules of a software system ● SSDLC 4.1 - Integration tests are performed before major product releases to the product's end users
	Deployment & maintenance - Attestations covering the process of releasing the software application or system into a production environment and activities performed after deployment to ensure ongoing functionality, usability, and performance ● SSDLC 5.1 - Updates to security features are included in software release documentation to inform users about security considerations, where appropriate

Domain: Usability

Criteria and benchmarks covering how the product provides ways to easily and intuitively navigate interfaces, understand information, and perform tasks

Criteria group	Criteria
User experience - Criteria covering how end users perceive and interact with your product, including overall experience, satisfaction, and ability to perform necessary software functions	Task efficiency - Attestations covering the effectiveness and speed with which users can accomplish specific tasks or goals within the product • UE 1.1 - Navigational elements that appear on multiple screens generally follow the same order in each instance, unless: The user is able to customize their view, The context of the application has changed enough that the user would reasonably expect the navigation to change as well • UE 1.2 - The product's content — such as text, images, video, and interactive elements — can be fully displayed without losing any information and without requiring the user to scroll both horizontally and vertically in the same view. This does not apply to content that requires both horizontal and vertical scrolling in order to maintain functionality, such as data tables or diagrams • UE 1.3 - Elements that require user input within the product — such as form fields, buttons, and selectors — include labels that make the element's purpose clear. This includes labels that are pictographic in nature as long as the pictograph is clearly defined on the page (e.g., stars for required form fields) • UE 1.4 - Elements that require user input within the product — such as form fields, buttons, and selectors — clearly indicate when a user input error is detected and the nature of the error is described in text • UE 1.5 - Web pages and/or application screens include title elements that describe the page or screen so that users with visual, cognitive and motor disabilities, or limited short-term memory can determine where they are in the product • UE 1.6 - Links and buttons within the product allow the user to determine the purpose of the element, including changes that might occur in the product once the link or button is pressed or locations the user might be redirected to

Domain: Usability, cont.

Criteria and benchmarks covering how the product provides ways to easily and intuitively navigate interfaces, understand information, and perform tasks

Criteria group	Criteria
User experience - Criteria covering how end users perceive and interact with your product, including overall experience, satisfaction, and ability to perform necessary software functions	Accessibility - Attestations covering the ways in which a product can be accessed and used by people with disabilities • UE 2.1 - The product makes the appropriate semantic structure and elements available to the user agent to enable screen readers and other assistive devices • UE 2.2 - All functionality is operable through a keyboard interface, enabling users with alternate keyboards or input devices to successfully use the product. Exceptions to this include any product functionality that is not compatible with keyboard input, such as drawing • UE 2.3 - Text in the product can be resized without assistive technology, such as utilizing OS- or browser-provided zoom functionality. Exceptions to this include captions or images of text • UE 2.4 - Information that is required for the product's core functionality is persisted after it is entered by the user, and is auto-populated or selectable when appropriate. This includes information such as credit cards, insurance information, and user info necessary for the functionality of the product
	User testing & support - Attestations covering processes and activities aimed at gathering feedback from users, evaluating their experiences, and providing assistance to ensure effective usage of the product • UE 3.1 - A process is in place to provide the specific knowledge needed to effectively and proficiently use the product. Training is based on end-user role (e.g., patient, clinician, or administrator • UE 3.2 - Usability testing is conducted with target users, representing each end-user role, to collect feedback on task completion and user satisfaction in conditions that match the product's intended use • UE 3.3 - A process is in place to document user feedback. This includes, but is not limited to, user feedback tools that are contained within the product or easily contactable customer support via phone, email, or similar
Workflow integration - Criteria covering the incorporation of a product into existing clinical and administrative workflows within healthcare settings	Workflow integration - Attestations covering the incorporation of a product into existing clinical and administrative workflows within healthcare settings • WI 1.1 - Analysis of user roles, responsibilities, tasks, and decision points within the workflow align with product features and functionalities. • WI 1.2 - The product supports the appropriate FHIR endpoints so that it may interact with other systems, enhance patient care, and align with industry standards and regulations