This is a Model Policy and can and should be modified by the health center to align with existing governance structure, roles and responsibilities and processes. Further, the health center should revise the policy as necessary to ensure it can comply with the policy.

Model Policy for the Use of AI Technology

1. Background and Applicability

Artificial intelligence ("AI") promises to provide significant benefits to [*Insert company name*] ("[*Company Name*]") by supporting patient care delivery, improving analytics and services, reducing manual tasks and increasing our overall performance and efficiency. AI, however, if not understood, deployed improperly or not adequately overseen presents risks to the [Company] and/or its patients and may compromise our ability to comply with the law and *[our high ethical standards, Code of Conduct/Code of Ethics*]. This Policy and Procedure sets forth key AI definitions, specific prohibited and permitted uses and related considerations, requirements that all employees, contractors, vendors and Board of [*Directors/Trustees*] (collectively, referred to herein as "**Personnel**") must meet when using AI and our AI vendor and AI tool approval and governance process.

Our [*AI Governance Committee*][1] will oversee and enforce this Policy as part of its broader responsibility to promote the compliant and safe use of vetted and trustworthy AI within and by [*Company*].[2]

2. Definitions

Artificial Intelligence ("AI") means information technology that combines complex computer processing systems with large data sets to produce results that mimic human logic and learning, make recommendations and draw conclusions. Generative AI, machine learning ("ML"), deep learning, collaborative filtering and natural language processing incorporate different aspects of AI.

Generative AI means a form of AI that trains a computer program to recognize patterns within large language models. Based on human or machine inputs, the program then statistically produces new content such as text, images or videos. Generative AI tools include OpenAI (ChatGPT, GPT-4, DALL-E 3), Microsoft (Bing), Google (Bard) and Adobe (Firefly), as well as chatbots that can communicate in real time with users to provide textual responses to their questions or concerns.

[1] Note to Client: An existing committee, such as the IT Committee or Compliance Committee, can also be utilized.
[2] Note to Client: Consider creating a charter for a new committee to list by title who is on the committee, its charge and the frequency of its meetings.

Intellectual Property ("IP") means any creative work or invention protected by law, including, but not limited to, an organization's logo, trademark, software code, music, video, photo, art, manuscript or other copyrighted creative work, patented product or design or trade secret.

Confidential Information means nonpublic information about [*Company*] or its business operations, patients or vendors, including Personal Information. Confidential Information may be labeled expressly or may be implied by the sensitive and proprietary nature of the information.

Personal Information means information that could be reasonably linked to identify an individual, including, but not limited to, a person's name, street address, email address, phone number, government ID, date of birth, medical record number, financial data or health and medical information. Personal Information includes Protected Health Information.]

Protected Health Information ("PHI") means individually identifiable health information including demographic data that relates to:

- An individual's past, present, or future physical or mental health or conditions;
- The provision of health care to the individual; or
- Past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual by HIPAA Privacy Rule at 45 C.F.R. § 160.103. In general, information we have on our patients is considered PHI. [*Company may choose to reference or hyperlink to HIPAA policies and procedures here*]

3. Risks

Personnel must understand the general risks that AI presents in order to evaluate whether an AI tool is appropriate for an intended purpose and assess the benefits, consequences and shortfalls of any AI tool. Specific AI risks include, without limitation, the following:

3.1 *Reliance on Inaccurate Information*: Generative AI often learns from and relies on historical data to generate output. If the data set is incomplete, inaccurate or dated, in whole or in part, then the AI tool may produce inaccurate output (i.e., information) in response to any input (i.e., information Personnel enters into the AI tool). Similarly, if the AI tool contains errors in the algorithm, like any math problem, the AI tool will produce an inaccurate output. Additionally, AI tools can sometimes make up an answer, known as hallucinating, and the user may not know the AI tool made such an error. Unfortunately, the AI tool generally provides confident-appearing output, making it difficult to assess when the output may be inaccurate.

3.2 *Violations of Privacy*: Many AI tools ingest user prompts into their learning models and user entered information forever remains part of the learning model or data set. Thus, entering Personal Information into an AI tool not only results in a disclosure of the information to the AI vendor, but could also result in the Personal Information being disclosed, intentionally or not, to a future user of the AI tool. If Personnel enters PHI into an AI tool without patient authorization or a business associate agreement with the AI vendor, Personnel will violate

HIPAA. The *Company* may need to provide advanced notice or obtain a person's consent to enter other types (non-PHI) Personal Information.

3.3 *Breaches of Confidentiality*: Similar to the privacy risks, Personal Information of an employee or a vendor or *Company*'s Confidential Information may be required to be confidential under contracts with the vendor or the law. Personnel who enter Confidential Information (e.g., customer data, contract terms, marketing plans) into an AI tool may expose the data to the AI vendor, third parties and/or the public, potentially violating contract terms with customers, other third parties or applicable laws.

3.4 *Security:* AI tools are subject to common cybersecurity attacks, such as phishing and ransomware, and are vulnerable to unique threats, such as the "poisoning" of learning models with inaccurate information. Depending on where the AI tool is deployed, such attacks could also compromise the *Company*'s other information systems.

3.5 *Safety*: If AI tools are not appropriately vetted, deployed and/or overseen, AI tools could threaten people's physical health or safety, damage property and harm the environment.

3.6 *IP Infringement*: Using the results of an AI tool that produces results based on images, text, sounds or other items from the databases that contain legally protected works without permission could violate IP laws in the U.S. or other countries. Personnel that enter [*Company*]'s or its vendors IP into an AI tool may compromise [*Company*]'s or vendor's IP.

3.7 *No IP Protections*. Because AI tools can produce pictures or text or other content automatically, AI output may not be considered "creative" by the courts. Therefore, the AI-generated output may not be legally protected or may have little IP value to [*Company*].

3.8 *Lack of Transparency*: AI vendors may not always know exactly how their tools work, what data is relied upon in the algorithm, how the tools were tested for bias, discrimination and errors, or why a result was produced. If an AI vendor cannot provide transparency into their tool through documentation, such as model cards, then the *Company* cannot assess it for the risks enumerated above.

4. Prohibited Uses of AI

To ensure the ethical, legal, and best uses of AI within [*Company*], [*Company*] prohibits the following:

4.1 *Unlawful Activity*. Personnel may not use any AI tool to engage in fraud, deception, threats or harassment or to violate any laws, agreements or industry standards applicable to [*Company*].

4.2 *Present a Safety or Security Concern*. Personnel may not use any AI tool that have known risks to the physical health or safety of individuals, to property or IT systems and networks or to the environment and natural resources.

4.3 *Prohibited Uses of Publicly Available AI tools*.

4.3.1 Personnel may not enter Personal Information, including PHI, into any publicly available AI tools, such as ChatGPT, or publicly available chatbots. Likewise, Personnel may not allow contractors or third parties to enter Personal Information into publicly available AI tools. Entering any PHI into a publicly available AI tool likely violates HIPAA and potentially other state privacy laws, compromises the privacy and security of PHI and may result in harm to our patients. Entering Personal Information of our employees into a publicly available AI tool likely violates certain employment laws and could harm our employees.

4.3.2 Personnel may not enter Company's or its contractor's Confidential Information into publicly available AI tools.

4.4 *Prohibited Uses of Publicly Available AI Unless Prior Approval Obtained*

4.4.1 Personnel may not enter Company or third-party's IP into public AI tools unless approved in advance by [*Legal Department*].

4.4.2 Personnel may not use any images, text, song or graphics generated by an AI tool for external marketing, social media posts or other public-facing materials or presentation, unless [the Legal Department] determines that IP has been properly licensed by [*Company*] or licensure is not necessary.

5. Permitted Uses of AI

5.1 [*Consider*: Personnel may use publicly available AI tools as not expressly prohibited (i.e., no Personal or Confidential Information is entered) above to produce first drafts of:

- internal presentations;
- grant or other applications;
- patient educational materials that summarize complex general medical or medication information;
- internal or external reports;
- responses to common patient non-clinical, administrative inbound messages; and
- templates (such as templates for insurance appeals or denials or that assist patients with obtaining benefits).

All first drafts **must** be reviewed and, if necessary, revised by Personnel to ensure the final draft is accurate, uses the correct tone and tenor and is consistent with our mission and voice. [*If applicable*: Further, any drafts initially produced by AI tools must go through any pre-existing Company approval process before being finalized and/or put into use].

5.2 In addition, if Personnel do not input Confidential or Personal Information into the AI tool, they may use publicly available AI tools for low-risk and occasional internal tasks, such as to:

- Summarize or translate long written articles or documents for internal review;
- Draft outlines or initial project plans;
- Draft initial advertising ideas;
- Obtain high-level understanding of complex topics;
- Look up technical jargon and definitions; or
- Learn specific software functions and shortcuts (e.g., Excel formulas and macros).

5.3 Personnel may use approved AI tools as permitted by the approval.

6. Approved AI Tools Use.

6.1 *General*

6.1.1 [*Company*] will maintain a list of approved AI tools and for which activities the AI tools are approved.

6.1.2 Personnel may use only approved AI tools while at [*Company*] or using Company issued devices or mobile phones and only for the sole purpose(s) approved and related to their professional duties. All AI tools must be used in accordance with all other applicable Company policies, including, but not limited to, this AI Policy, [*Company*] [*Information Security Policies, Code of Conduct, Nondiscrimination Statement, HIPAA Policies, Clinical Policies and any applicable online Privacy Policy or notice or Terms of Use*].

6.1.3 Personnel must also comply with any limitations or instructions provided to the Personnel or posted with the AI approval by the [*AI Governance Committee]*.

6.1.4 Unless otherwise approved by the [*AI Governance Committee]*, all AI tools must be configured in "incognito" mode or a similar setting so the AI tool or vendor cannot track Company data inputs and outputs or ingest them into the AI tool's learning model. If the AI tool does not have an "incognito" setting and [*AI Governance Committee]*'s approval of the AI tool assumed that this an option was available, Personnel must seek a second approval before using the AI tool.

6.1.5 [*Company*] will only permit Personnel to enter PHI into an AI tool if the AI vendor has executed a HIPAA business associate agreement and the AI vendor agrees to [*Company*]'s confidentiality and security standards required for such AI vendor. *[All business associate agreements must be on* [*Company*] *template or approved by Legal and copies must be maintained [at]].*

See Section 7 below for description for how AI tools will be approved and the list of approved tools maintained.[3] **Appendix C** has additional use cases.

6.2 *Reliance or Use of AI results*. Personnel must always review the output of any AI tool to assess its accuracy, validity, completeness and reasonableness in light of the inputs and to

[3] Approved AI tools may be maintained on the intranet or appended to the policy or through another means.

assess if the results are free from biases in accordance with any legal or industry standard practices. Because it may be challenging for Personnel to discern bias from a single output, Personnel must also evaluate the collective outputs on a regular basis to assess bias. [*consider: Requiring this to be part of an existing QI or Compliance process.]* If Personnel is unsure how to assess the results, Personnel should contact [*insert contact*.]

If an AI tool is being used to support clinical decision-making, a clinician may not rely solely on the output of the AI tool but may consider the output as part of the factors and circumstances taken into account when making a clinical decision or recommendation.

6.3 *Entering Personal Information*. Before allowing Personal Information to be entered into an approved AI tool either by Personnel, a contractor or a patient, the [*AI Governance Committee*] must confirm that all necessary notices and authorizations have been obtained or contracts executed. Personnel should enter only the minimum amount of Personal Information necessary for the AI tool to produce valid, accurate and complete results.

[*Company*] may also need to update its Notice of Privacy Practices, its online Privacy Notice or Terms of Use or external disclaimers before deploying the AI tool. If AI is used in connection with an online or telephone chatbot, the chatbot must clearly and conspicuously disclose, prior to beginning a chat session, that responses are not generated by a human.

7. AI Tool Approval Process

7.1 *AI Request*. Personnel must submit an [AI Request and Impact Assessment Form], and any other requested information, to obtain approval from the [*AI Governance Committee*] before using any AI tool on behalf of their job function for [*Company*]:

- Repetitive and ongoing business analysis or operations;
- Content published for [customers, government oversight agencies, patients, providers] or the public;
- Content created for the Board or executives;
- Significant coding for software applications [e.g., if more than xx lines of code];
- Design, modification or deployment of a significant business process;
- Any project involving the input, use or processing of Confidential or Personal Information;
- Clinical Decision-Making Tools;
- Clinical Diagnostic Tools;
- Legally significant decisions affecting access to, provision of or denial of:
    - Employment;
    - Insurance;
    - Healthcare; or
    - [*social services*]
- Automated processing without human supervision, review and/or intervention.

Personnel only needs to submit one request form for ongoing and consistent use of AI for a specific purpose (e.g., creation of marketing materials).

[*Currently approved AI tools and uses are available at* [*insert hyperlink to list or location of where they can be obtained*].

7.2 *Evaluation and Composition*. The [*AI Governance Committee*] shall comprise [*insert titles of members*] and will meet as needed, but at least [weekly, monthly], to promptly review an *AI Request and Impact Assessment Form* The *AI Governance Committee* will evaluate the AI request in accordance with the NIST AI Risk Management Framework[4].

7.3 *Procurement/Contract Approvals*. When seeking approval of an AI tool that requires a separate contract, Personnel must comply with [*Company*]'s policy on [*Vendor Management*] and seek approval of any contract to use or deploy AI tools.

7.4 *AI Contracts*. When negotiating contracts with AI vendors, [*Company*] will seek to include, as appropriate:

- confidentiality requirements regarding its data;
- privacy and cybersecurity standards or controls;
- indemnification for any third-party claims of IP infringement;
- terms describing data ownership (training data, inputs and output);
- terms describing how each party may use AI inputs and outputs; and
- representations and warranties that the AI tool has been tested for its intended purpose and implicit bias.

Contracts with AI vendors must be approved by [the *Legal Department*].

8. Accountability

The [*AI Governance Committee*] will approve, reject or recommend modifications of AI request based on the risk factors and considerations described in **Appendix A**.

The *AI Governance Committee* may impose specific oversight, monitoring and auditing requirements on the Personnel using the AI tool and require period reports back to the *AI Governance Committee* on the accuracy, validity, reliability, etc. of the AI tool. These risk factors must be continuously evaluated as the accuracy, validity and/or reliability of an AI tool can change over time. Based on the results of any oversight, the *AI Governance Committee* may require the Personnel to pause or cease using the AI tool or remove the AI tool from the approved list.

The [*AI Governance Committee*] will track individual projects and will map, measure and manage the general life cycle of AI tools used within [*Company*]. This includes receiving input from Personnel and educating and training them to ensure successful adoption of trustworthy AI.

The [*AI Governance Committee*] will recommend updates to any AI training, this AI Policy and related policies and procedures.

[4]January 2023.

***

If Personnel have any questions regarding this Policy or AI use by [*Company*], they should contact the [*AI Governance Committee*/Legal Department] at [email address].

Adopted [___]
Reviewed[___]
Last Revised [___]

Appendix A: Risk Assessment

The [*AI Governance Committee*] will assess whether the requested AI tool meets the characteristics for "trustworthy AI," as set forth by the Artificial Intelligence Risk Management Framework ("AI RMF 1.0") published by the U.S. National Institute of Standards and Technology ("NIST").[5]

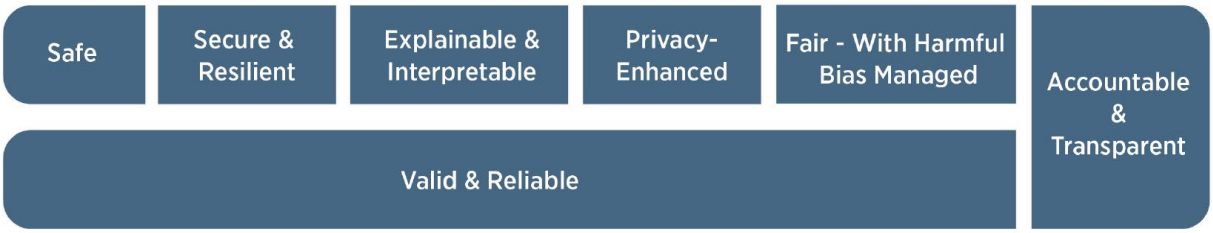

Figure 1 – NIST criteria for trustworthy AI

Using this framework and considering any laws, regulations or federal or state issued guidelines relevant to the requested AI tool, the [*AI Governance Committee*] will evaluate whether the proposed AI tool is:

1. **Safe**, meaning the AI tool does not present a physical danger to human health or life, property or the environment and will be subject to appropriate testing and human oversight. While it is unlikely that AI tools requested by Personnel would be unsafe in this matter, it is nonetheless important for the *AI Governance Committee* to confirm in each instance. If the AI tool is deemed potentially unsafe, as part of their consideration, the *AI Governance Committee* will evaluate the AI Request to assess how Personnel will oversee the AI tool deployment to mitigate and report any safety risks.

2. **Secure and Resilient**, meaning the AI tool maintains the confidentiality, integrity and availability of Confidential Information and Personal Information and is capable of restoring data following attacks (such as data poisoning or exfiltration of data) or adverse events. The *AI Governance Committee* will consider the AI tools' security controls and design, including what access controls are in place, whether encryption or two factor authentication is used and that there is connectivity to other [*Company*] systems.

3. **Privacy Enhanced**, meaning whether the tool was developed with anonymity, confidentiality and control in mind. The [*AI Working Committee*] will consider whether the AI tool can comply with contracts and laws regarding the privacy and confidentiality of [*Company*]'s or vendor's Confidential Data and Personal Information. If required or best practice, the *AI Governance Committee* will assess whether the AI tool incorporate protections to Personal Information, such

[5] *See* NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

as obtaining advance notice and consent, providing necessary disclaimers on AI generated output, data minimization, anonymization or limitations on sharing.

The *AI Governance Committee* will also assess whether the AI tool is protective of other third-party's data (e.g., whether the learning data and inputs infringe on others' IP rights).

4. **Fair With Harmful Bias Managed**, meaning whether the AI tool was created with the intent to be fair and unbiased. When considering AI tools that may be used to support clinical or diagnostic decision-making, patient's access to services or benefits or employment-related decisions, the *AI Governance Committee* will request that the AI vendor explain how the training data was obtained and whether and how it was tested for bias.

5. **Ethical**, meaning whether the AI tool excluded from its learning model and was tested to ensure its outputs are free from violent, extremist, racist, sexist, visually disturbing or similarly offensive data or results. The [***AI Governance Committee***] will request the AI vendor explain how the training data was obtained, whether it excluded violent, extremist, racist, sexist, visually disturbing, or similarly offensive data from its dataset, and whether the output was assessed to confirm violent, extremist, racist, sexist, visually disturbing or similarly offensive results were not being produced.

6. **Accountable and Transparent.** Accountability presupposes transparency. Transparency reflects the extent to which information about an AI system and its outputs is available to individuals interacting with such a system – regardless of whether they are even aware that they are doing so. The role of those who use the AI should be considered when seeking accountability for the outcomes of AI systems. Measures to enhance transparency and accountability should also consider the impact of these efforts on the implementing entity, including the level of necessary resources and the need to safeguard proprietary information.

7. **Explainable** and **Interpretable.** Explainable, meaning whether the AI vendor can show documentation of the AI design, training data and logic. Interpretable, meaning the AI output is understandable by its users—it is important to determine if the AI vendor has documents to explain why the AI produces specific results. A question the *AI Governance Committee* may ask is whether the user is notified of an error or adverse outcome caused by the AI system. The *AI Governance Committee* will request that the AI vendor provide its impact assessment, design, transparency or other similar plan or report.

8. **Valid and Reliable.** Valid means fit for intended use, accurate based on testing (e.g., with known false positive/negative rates) and generalizable beyond the AI learning set (i.e., applicable to proposed project). Reliable means robust and able to perform as expected initially and over time.

The *AI Governance Committee* will require the AI vendor to provide the model card, if it exists, and information regarding how the algorithm was tested, the frequency of the testing, and known accuracy issues or biases. If possible, members of the *AI Governance Committee* will test, or require the AI vendor to test, the AI tool for accuracy with a dummy dataset.

The [*AI Governance Committee*] may weigh the risks and risk-mitigations differently based on the given context of the use case.

Appendix B

Bias Types

Different types of bias in AI include the following:

- Algorithm bias occurs when there is an underlying problem or flaw with the algorithm used to deliver outputs.
- Data bias occurs when the data used to train AI systems is biased in some way. Some examples of data bias include:
  - Exclusion bias occurs when critical data point(s) are excluded from the training dataset.
  - Measurement bias occurs when there are issues with the accuracy or precision of the training data.
  - Prejudice bias occurs when the data used to train the algorithm contains prejudices or faulty societal assumptions.
  - Sample bias occurs when the data used to train the model is not representative of the population for which the tool will be used.
- Reliance bias occurs when humans over- or under-rely on AI models to inform decisions or actions.

Source: https://www.ama-assn.org/system/files/future-health-augmented-intelligence-health-care.pdf

Appendix C

Applying the Policy: Sample Use Cases

Clinical Documentation Support: Leveraging AI to support the documentation of medical charts and/or visit notes		
Considerations	Process	Oversight
Benefits: Creates efficiencies, frees up providers to see patients and reduces provider burnout. HIPAA risks: Clinical Documentation Support necessarily requires the entry of PHI into the AI tool. Reimbursement and government audit risk: Clinical documentation is the basis for coding, coverage and payment determinations. Patient care risk: Clinicians rely on medical records to make treatment decisions. If records are not accurate, then patient care could be compromised.	AI tool must be approved by the *AI Governance Committee*. AI tool must be tested and validated for the time period determined by the *AI Governance Committee* by the Company using dummy data set prior to deployment and use. The *AI Governance Committee* must evaluate the AI tool like any other vendor or software as service provider accessing, transmitting or maintaining PHI. [*Company*] must have a BAA in place with the AI vendor or obtain a patient HIPAA compliant authorization before tool is used.	[*Company*] must adopt a policy and procedure/protocol (with any revisions requested by the *AI Governance Committee*) to ensure proper clinician review of the documentation before its signed and locked. Clinicians must always review the clinical documentation draft generated by the AI tool. Clinical documentation may not be signed until reviewed by the signing clinician and, if necessary, corrections for accuracy are made. A group of clinicians should be convened to regularly review and discussed accuracy or other concerns regarding the AI tool to evaluate the continued deployment of such tool. Results should be reported to the *AI Governance Committee*. Any inaccurate documentation identified must be corrected via an amendment (per *insert relevant policy*)
Automated Patient Messaging: Leveraging AI to Generate Automatic Messages to Patients Through the Patient Portal Regarding Non-Clinical Questions (e.g., Scheduling)		
Considerations	Process	Oversight
Benefit: Reduce clinician and administrative personnel time spent providing or responding to non-clinical messages. HIPAA risks: AI tool will receive PHI. Error: AI tool may not identify a message that is clinical in nature and	AI tool must be approved by the *AI Governance Committee*. If possible, AI tool must be tested to determine if the automated messages are responding as intended (e.g., correct use of message, clinical messages are not receiving automated responses) for the time period determined by the *AI*	*Company* must develop or approve automated responses to ensure the responses are appropriate in tone, reading level, and patient population. *Company* must approve the algorithm with regard to which messages receive automated responses to ensure only

provide an inaccurate response and/or delay patient access to care or information. Patient dissatisfaction: AI tool response may not be responsive to patient.	*Governance Committee* using dummy data set prior to deployment and use. Accuracy of output (test) must be evaluated and the *AI Governance Committee* should determine an acceptable accuracy threshold. The *AI Governance Committee* must evaluate the AI tool like any other vendor or software as service provider accessing, transmitting or maintaining PHI. [*Company*] must have a BAA in place with the AI vendor. [*Company*] may consider disclosing (or could be required to disclose) the use of AI to generate the response and provide a mechanism for the patient to follow-up if the response is not responsive or if additional support is needed.	appropriate messages receive automated responses. *Company* must convene a team to audit the automated message responses [*monthly*] to assess whether the responses are consistent with the algorithm and are responsive to the inquiry. [*Consider whether a sample of messages should be reviewed daily]* Results of the audits must be reported to the *AI Governance Committee* at a defined cadence.
Automated Patient Messaging: Leveraging AI to Generate Draft Messages to Patients Through the Patient Portal		
Considerations	Process	Oversight
Benefit: Reduce clinician and time spent providing or responding to portal and email messages. HIPAA risks: AI tool will receive PHI. Error: AI tool may not prepare an accurate response and clinician's review may not identify the inaccuracy. Patient satisfaction: Patients may receive quicker responses to their messages, leading to patient satisfaction.	AI tool must be approved by the *AI Governance Committee*. The Personnel submitting the request must provide a draft policy and procedure/protocol for how messages will be reviewed by clinicians and revised before being sent to a patient. If possible, AI tool should be tested to assess the reliability and accuracy of the draft messages for the time period determined by the *AI Governance Committee* using dummy data set prior to deployment and use. This will assist in [*Company*] determining whether the AI tool truly adds value and reduces clinician's time spent on messaging. The *AI Governance Committee* must evaluate the AI tool like any other vendor or software as service provider	*Company* must adopt a policy and procedure/protocol (with any revisions requested by the *AI Governance Committee*) to ensure proper clinician review of each message before it is sent to a patient. Clinicians must always review the draft message before it is sent. *Company* must develop a process to assess clinician compliance with the policy, which must include an audit of a sample of messages every [*month]*. Any inaccurate or incomplete messages identified must be corrected and errors in AI tool's drafts tracked. Results of the audits must be reported to the *AI Governance Committee* at a defined cadence.

	accessing, transmitting or maintaining PHI. [*Company*] must have a BAA in place with the AI vendor.	
Analytics of Patient Data to Produce Aggregated, De-Identified Reports		
Considerations	Process	Oversight
Benefits: Reduce administrative time in manually aggregating and/or de-identifying data; may be less costly than traditional vendors. HIPAA risks: AI tool will receive large amounts of PHI. Errors: May be more challenging to confirm the accuracy of the output.	AI tool must be approved by the *AI Governance Committee*. To the extent that the AI vendor can demonstrate its accuracy with the use of dummy data sets that can be easily assessed, the *AI Governance Committee* should require such demonstration. The *AI Governance Committee* must evaluate the AI tool like any other vendor or software as service provided accessing, transmitting or maintaining PHI. Privacy and security may need to be more heavily weighted. [*Company]* must have a BAA in place with the AI vendor.	Personnel using the AI tool should assess each output for reasonability based on the data set inputted. Concerns regarding output need to be reported to the *AI Governance Committee* and AI tool vendor promptly.
AI-Enabled Diabetic Retinopathy Screening		
Considerations	Process	Oversight
Benefits: Enables at-scale screening for diabetic retinopathy in a primary care context. HIPAA risks: AI tool will receive PHI. Errors: May be concerns about accuracy which can be mitigated by using an FDA-cleared device.	Screening tool must be approved by the *AI Governance Committee*. If possible, the *AI Governance Committee* should require AI tool to be tested to assess the reliability and accuracy of the screening tool using existing images that can be easily accessed. The *AI Governance Committee* must have a process in place for monitoring the AI tool for drift over time. The *AI Governance Committee* must evaluate the AI tool like any other vendor or software as service provided accessing, transmitting or maintaining	Personnel using the AI tool should assess each output for reasonability based on the data set inputted. Personnel using the AI tool should receive specific training on the tools use and failure modes. Concerns regarding output need to be reported to the *AI Governance Committee* and AI tool vendor promptly.

	PHI. Privacy and security may need to be more heavily weighted. [*Company]* must have a BAA in place with the AI vendor.	