MEDIC EMS of Scott County
600 West Fourth Street
Davenport, Iowa 52801-1003
Office: (563) 323-6806
Fax: (563) 323-1705
https://www.medicems.com

December 12, 2023

To: Mahesh Sharma, County Administrator
From: Paul Andorf, Director

Attached is a System Access Agreement with Iowa Health System d/b/a UnityPoint Health, an Iowa nonprofit corporation. This agreement allows MEDIC EMS of Scott County to access the UnityPoint Health's Electronic Health Records to gather insurance and other information for billing patients and gather clinical data for internal QA/QI review.

The Scott County legal department has reviewed these attached agreements and found the agreements are sufficiently drafted to accomplish their intended purpose and are not in contravention of state law.

This resolution will allow the Director of MEDIC EMS of Scott County to sign such agreements on behalf of the Scott County Board of Supervisors.

System Access Agreement

This System Access Agreement ("Agreement") is effective as of the date last signed below, ("Effective Date") between Iowa Health System d/b/a UnityPoint Health, an Iowa nonprofit corporation, on behalf of itself and the UnityPoint Health Affiliated Covered Entity (collectively "UnityPoint Health"), and MEDIC EMS of Scott County, County of Scott, a County Government ("Participant") (individually a "Party" and collectively the "Parties").

Recitals

1. UnityPoint Health maintains demographic, health and account information, which is Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d to 1320d-7, and future amendments thereto and all regulations issued thereunder ("HIPAA") relating to its patients ("Confidential Information") in UnityPoint Health electronic information systems ("System") and provides access to the System to specified employees, agents, other workforce members, or business associates of certain health care entities and/or their business associates for the purpose of providing treatment, payment, or health care operations, which functions are enhanced through the timely access to necessary health information;

2. Participant desires to access data from the System for Participant's treatment, payment, or permitted health care operations of Participant, subject to the terms, conditions, and limitations of this Agreement and consistent with the provisions of HIPAA and applicable state privacy laws;

3. Parties desire for their Shared Patients (as defined below) to access all of their services seamlessly;

4. Without this Agreement, communications between Participant and UnityPoint Health related to their Shared Patients will be inefficient and sometimes slow or incomplete, which would hinder Participant's ability to effectively perform Services;

5. UnityPoint Health and Participant believe that services may be provided more safely, effectively, timely, and efficiently if certain Authorized Users (as defined below) at Participant have appropriate access to relevant Confidential Information maintained by UnityPoint Health, in accordance with relevant provisions of applicable law and the terms and conditions of this Agreement; and

6. To provide better service to UnityPoint Health patients, UnityPoint Health wishes to grant to certain Authorized Users of Participant appropriate access to certain Confidential Information contained in the System, which may or may not be through a secure, online remote access service called "EpicCare Link" (in either event referred to throughout this Agreement as the "Epic Connection"). The System, for purposes of this Agreement, includes UnityPoint Health software and technology dedicated to generating, revising, storing, or viewing patient health records (including supporting images) electronically, to the extent such software and technology is accessible to Participant.

NOW, THEREFORE, in consideration of the foregoing, and for other good and valuable consideration, the receipt and sufficiency of which are acknowledged, the Parties agree as follows:

1. **Access.** Subject to the terms and conditions of this Agreement, UnityPoint Health agrees to allow specified Authorized Users of Participant to access the System for the purposes of accessing patient data and other information for Participant's treatment, payment, or certain permitted health care operations purposes. The terms treatment, payment, and health care operations are used herein as defined in HIPAA. This Agreement specifies the Terms and Conditions of Participant's access to and use of the Confidential Information. An "Authorized User" means Participant's employees, agents, or other persons affiliated with Participant or otherwise permitted to use Participant's systems or facilities (a) who are authorized by Participant to access and use the System pursuant to this Agreement and (b) for whom access to the System has been provided pursuant to this Agreement.

2. **Conditions to Access.** Access will be provided to Participant to the Epic Connection upon completion of the following steps:
    a. **Appoint a Site Administrator.** Participant shall name two representatives who shall be responsible for and shall administer this Agreement on behalf of Participant ("Site Administrator"). The Site Administrator shall have the sole authority to request access for new Authorized Users. Such requests shall be made solely from the Site Administrator's email account on file to CareLinkRequest@unitypoint.org. Such requests may include: (a) adding Authorized Users to the Participant EpicCare Link account, (b) making changes to Authorized User email addresses, (c) deactivating Authorized User enrollment, (d) changing Authorized User or Participant physical address and telephone number or (e) other public contact information concerning Participant or Authorized Users. Once UnityPoint Health receives such request, UnityPoint Health shall make such changes as approved. UnityPoint Health reserves the right to disallow change requests, but agrees to contact the Site Administrator for clarification purposes and shall convey to the Site Administrator its reason(s) should it reject such request. Site Administrator must notify UnityPoint Health within two (2) business days of the termination of employment or contract of any Authorized User or a change in job duties such that the individual no longer meets the qualifications described in Subsection 4(c) of this Agreement, at which point the Authorized User's access to the System will be terminated.
    b. **Access Request.** Participant shall complete and submit to UnityPoint Health a Request for User Access for an Authorized User (via mail, fax or e-mail), signed by the Site Administrator listed in Exhibit A. Prior to receiving a user name and password to access the System, each such Authorized User shall be required to sign the UnityPoint Health Information Security Agreement attached as Exhibit B as may be updated from time to time with notice to Participant.
    c. **Access Training.** Participant shall complete HIPAA training for Authorized Users who have access to the System. By requesting access to the System for an Authorized User, the Site Administrator represents that the Authorized User has completed HIPAA training. Participant shall maintain documentation showing that each Authorized User for whom access to the System has been requested under this Agreement has received HIPAA training and understands the purpose and terms of this Agreement.
    d. **Access Verification.** Periodically, as requested by UnityPoint Health, Participant shall provide to UnityPoint Health a current list of Participant's Authorized Users to whom access has been granted. This is not a substitution for Participant's obligations with respect to providing notice of the termination of an Authorized User.

3. **Use and Restrictions**. Upon execution of this Agreement, Participant will be provided an Epic Connection, which may be via an EpicCare Link account to access Confidential Information related to dates of service for Shared Patients for treatment, payment, and certain health care operation purposes. No other use or right is granted under this Agreement.

4. **Scope and Terms of Access and Use.** The Parties agree to the following:

    a. **Appropriate Safeguards.** The Parties will maintain administrative, technical, and physical safeguards to protect Confidential Information in accordance with HIPAA, the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and any other applicable federal, state, or local laws, all as amended from time to time. UnityPoint Health will ensure that industry standard and HIPAA compliant security procedures are maintained for the System. Participant will also ensure that industry standard and HIPAA compliant security procedures are maintained for the computers and devices on which Authorized Users will access the System. Participant shall ensure that its Authorized Users, employees, agents, and contractors will not use or attempt to access the System by any means not specifically authorized by UnityPoint Health, including but not limited to the use of non-secure means of connection, and will ensure that no Authorized User, employee, agent, or contractor will avoid or disable any protection or security means implemented in the System or otherwise use any means to access the System without following log-in procedures specified by UnityPoint Health. Participant shall notify UnityPoint Health within 24 hours if it has information that may lead a reasonable person to believe that an Authorized User's password to the System has become known by an unauthorized third party or otherwise compromised.

    b. **Appropriate Patients.** Participant agrees that its scope of access to the System is intended for the purpose of performing Services which are for individuals (i) who have a current health care relationship with the Participant and (ii) who are or have been patients of a UnityPoint Health affiliate ("Shared Patients"). Access to or use of the Confidential Information of any individual who is not a Shared Patient is strictly prohibited and shall be considered a violation of the terms of this Agreement. Participant shall require its Authorized Users to utilize three (3) identifiers of the Shared Patients on the patient search screen as part of the query process to access Shared Patients. The Parties agree that in the event an Authorized User, in appropriately searching the System for information on a Shared Patient, inadvertently views the information of another patient, that access shall not be considered a violation of this Agreement by Participant so long as the Authorized User stops immediately viewing the information upon realizing it does not relate to a Shared Patient. Participant shall obtain and maintain any and all Shared Patients' authorizations or consents to access the Confidential Information as required by federal, state, or local laws. UnityPoint Health shall have no liability with respect to any claim arising from Participant's failure to obtain, maintain, or manage all applicable authorizations, consents, and permissions.

    c. **Appropriate Users.** Participant agrees that only those whose job duties as an employee or agent of Participant include providing Services for Shared Patients will be considered Authorized Users under this Agreement.

    d. **Appropriate Purposes.** Authorized Users will access and use the System only for

purposes of Treatment as defined by HIPAA, Payment as defined by HIPAA, and Health Care Operations as defined by paragraph (1) or paragraph (2) of the HIPAA definition of Health Care Operations of Shared Patients ("Services"), and to perform auditing and training functions that are directly related to the Services (auditing and training collectively referred to as the "Related Functions"), but only to the extent that access to and use of the System is limited to the minimum necessary to perform the Related Functions. Participant will not use or access the System for any purpose other than Services to Shared Patients and Related Functions. For clarity, but not to expand the scope described in the previous sentence, Participant will not use or access the System for any purpose for which such use of or access to Confidential Information is prohibited by applicable federal or state laws as such laws may be amended from time to time. Participant will not de-identify or otherwise anonymize Confidential Information for any purpose or use. Participant shall not distribute any Confidential Information, patient data, PHI, or other information in contravention of this Agreement. Participant acknowledges that under no circumstances shall Participant or its Authorized Users, employees, agents, or contractors use the System as a substitute for a clinician's professional skill and judgment in any instance regarding patient care.

e. **Minimum Necessary.** Participant shall ensure that Authorized Users access only the minimum amount of information necessary to perform Services to Shared Patients and Related Functions. Authorized Users shall access only information related to the condition(s) that are material to the Shared Patient's need for the Services. The Parties acknowledge that the following types of information, if related to the condition(s) that are material to a Shared Patient's need for Services, are typically relied upon to perform Services:
    i. Patient demographics
    ii. Information on history of patient (medical, surgical, family, social)
    iii. Allergies
    iv. Medications
    v. Immunization summaries
    vi. Documents, such as Health Care Directives
    vii. Scheduled office visits
    viii. Clinic & hospital progress notes
    ix. Care coordination notes/care planning
    x. ER & Urgent Care visit notes
    xi. External agency reports (home care records, hospice records, etc.)
    xii. Discharge instructions
    xiii. After visit summaries
    xiv. Face sheets
    xv. Labs and results (and ability to view over time)
    xvi. Diagnostic imaging
    xvii. Flowsheets (vital signs, labs, medications, pediatric milestones etc.)
    xviii. Documentation of co-management communication and encounters in general
    xix. Patient goals, diagnoses, care plan
    xx. Names of members of the care team

f. Authorized Users must use their professional judgment to determine which information in the System is the minimum necessary to effectively provide Services to Shared Patients. Participant represents that the information to be accessed by Authorized Users is the minimum necessary to effectively perform Services for Shared Patients and Related Functions, and UnityPoint Health is relying on this representation to allow Participant to access the System. The Parties recognize that access to information within the System other than the information described above is not necessarily prohibited in all instances, but may warrant further evaluation to determine whether such access was the minimum necessary under the circumstances.

g. **Restricted Information.** Each Party is committed to protecting the privacy and security of patient and member information and agrees to comply with applicable law in this regard. UnityPoint Health will ensure that for any Confidential Information for which UnityPoint Health is required to obtain patient consent or otherwise restrict access under applicable law, or for which UnityPoint Health determines a restriction is appropriate, UnityPoint Health will implement appropriate restrictions in the System, with the intent that Participant and Authorized Users will either be unable to access that Confidential Information or will be alerted by the UnityPoint EHR that the Confidential Information should not be accessed. If an Authorized User encounters such a system alert with regard to a record, the Authorized User will not access that record. Specifically, but not by way of limitation, the Parties acknowledge and agree that at the time this Agreement is entered into, UnityPoint Health restricts certain information via a "Break the Glass" feature within the System. Participant agrees that Authorized Users will not "Break the Glass" to view restricted information. If UnityPoint Health identifies a need to adopt other means of restricting records or information, or additional types of records or information that should be restricted, the Parties will discuss options for implementation, and if (a) no agreement is reached, (b) UnityPoint Health is unable for any reason to implement a restriction, or (c) UnityPoint Health needs time to implement a restriction, a Party may suspend access until a restriction can be implemented or terminate this Agreement in accordance with Section 12.

5. **Participant Obligations of Authorized Users**. Participant shall ensure that each of its Authorized Users:
   a. accesses the minimum amount of information on the System necessary to carry out the responsibilities of his or her employment for Participant or contract with Participant as it relates to the treatment, payment, or health care operations function being performed subject to the terms and conditions of this Agreement;
   b. does not, under any circumstances, access PHI or other data related to an individual who does not have a current health care relationship with Participant;
   c. maintains the confidentiality of patient data and all other information accessed through the System in accordance with HIPAA and the confidentiality provisions of this Agreement;
   d. safeguards, and does not disclose to any third party, his or her password to the System;
   e. does not attempt to gain access to information, computer operating systems or application areas or functions for which he or she has not been authorized by UnityPoint Health; and
   f. notifies Participant or UnityPoint Health within twenty-four (24) hours if he or she

believes that his or her password to the System has become known by a third party.

6. **Indemnification.** Each Party (referred to as "Responsible Party" when an indemnification claim is being made against it) will indemnify, defend and hold harmless the other Party (referred to as "Claiming Party" when claiming indemnification) and any related entity, including any entity that controls a Party, is controlled by a Party, or is controlled by an entity that also controls a Party, and each of their directors, officers, agents, and employees ("Indemnified Parties" and each an "Indemnified Party") from and against any and all third-party liability, loss, damage, claim, and expense, including but not limited to reasonable attorneys' fees and interest, which any of them at any time sustain or incur arising from (i) any intentional or negligent act or omission of the Responsible Party, its directors, officers, agents, employees, contractors, Authorized Users, or subcontractors under this Agreement, or (ii) any breach or default of a Responsible Party under this Agreement. Notwithstanding the foregoing, unless otherwise specifically set forth herein, no Party will be liable for special, indirect, consequential, incidental, or punitive damages of any kind (including, without limitation, lost profits, loss of use, or goodwill), even if any such damages are reasonably foreseeable or the Party has been advised of the possibility of such damages.

7. **Notification of Breach**. During the term of this Agreement, Participant shall notify UnityPoint Health within twenty-four (24) hours of discovery of an actual or suspected breach of security, intrusion, or unauthorized use or disclosure of Confidential Information from the System by Participant; any of its Authorized Users, employees, agents, or contractors; or any other individuals who access the System or data from the System by means of the rights granted to Participant under this Agreement in violation of this Agreement or any applicable federal or state laws or regulations. Participant shall cooperate with UnityPoint Health to take prompt corrective action to mitigate any harm with respect to the actions of Participant Authorized Users; employees, agents, contractors; or other individuals who access the System or data from the System by means of the rights granted to Participant under this Agreement.

8. **Responsibility for Breach**. Participant shall be solely responsible for any and all breaches of this Agreement, including breaches of privacy or confidentiality, by Participant, its Authorized Users, employees, contractors, and all other individuals who access the System or data from the System by means of the rights granted to Participant under this Agreement. Participant shall be solely responsible for any and all damages, liabilities and other penalties that may arise from such a breach ("Expenses"), in addition to being solely responsible for any actions required by law or this Agreement that arise from such a breach. Such Expenses include, but are not limited to, reasonable attorney's fees, costs of third party services necessary for investigation of the Breach, costs of legally required notification of individuals and the media, credit monitoring, and other mitigating actions if reasonably determined necessary by UnityPoint Health.

9. **Response to Confidentiality Concerns**. Whenever UnityPoint Health in its sole judgment and discretion believes that an Authorized User, employee, agent, contractor, or subcontractor of Participant has obtained unauthorized access to Confidential Information, has disclosed Confidential Information inappropriately or in violation of federal or state laws or regulations, has violated the UnityPoint Health Information Security Agreement, or has violated any material provisions of this Agreement, UnityPoint Health shall be entitled to

take any or all of the following actions immediately, as it reasonably determines to be appropriate:

a. Notify Participant's Privacy Officer of the Authorized User's conduct and require Participant to educate and/or discipline the Authorized User;
b. Suspend or terminate the Authorized User's remote access to the System temporarily or permanently;
c. Comply with any mandatory reporting and disclosure requirements;
d. Terminate this Agreement; or
e. Bring legal action to enforce this Agreement.

10. **Disclaimer.** Participant understands and agrees that remote access to the System involves (1) technological risks, including possible introduction of errors, data corruption, and artifacts that may not be present on original versions of the health record document and (2) additional risks may include compromises to the integrity and security of data, including but not limited to spyware, hacker access, viruses, worms, and other harmful software (collectively referred to as "Remote Access Risks"). UnityPoint Health will not be responsible for any losses or damages related to Remote Access Risks. Participant understands that documents accessed remotely may not have the same degree of clarity as documents viewed on-site. PARTICIPANT AGREES THAT UNITYPOINT HEALTH WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR OTHER DAMAGES INCURRED BY PARTICIPANT, ITS AUTHORIZED USERS, OR ALL OTHER INDIVIDUALS WHO ACCESS THE SYSTEM OR DATA FROM THE SYSTEM BY MEANS OF THE RIGHTS GRANTED TO PARTICIPANT UNDER THIS AGREEMENT ARISING OUT OF THE USE OF EPICCARE LINK, EPIC CONNECTION, OR THE SYSTEM. UNITYPOINT HEALTH DOES NOT GUARANTEE OR WARRANT THE TIMELINESS, ACCURACY, COMPLETENESS AND AVAILABILITY OF REMOTE ACCESS TO THE SYSTEM VIA EPICCARE LINK, EPIC CONNECTION, OR THE CONTENT OF THE SYSTEM. WITHOUT LIMITING THE FOREGOING, UNITYPOINT HEALTH MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE ACCESS PROVIDED HEREUNDER, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. EXCEPT WHEN OTHERWISE STATED IN WRITING, UNITYPOINT HEALTH PROVIDES ACCESS TO THE SYSTEM "AS IS" WITHOUT WARRANTY OF ANY KIND. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SYSTEM IS WITH PARTICIPANT. SHOULD THE SYSTEM PROVE DEFECTIVE. PARTICIPANT HAS NO OBLIGATION TO UNDERTAKE TO CORRECT OR OTHERWISE ADDRESS SUCH DEFECTS, AND THE TERMS OF ANY SUCH UNDERTAKING MUST BE MUTUALLY AGREED BY THE PARTIES. HOWEVER, IN NO EVENT SHALL UNITYPOINT HEALTH BE OBLIGATED BY THIS AGREEMENT TO PAY FOR THE COST OF ANY SERVICING, REPAIR OR CORRECTION THAT IS NECESSARY TO PROVIDE OR MAINTAIN PARTICIPANT'S AND ITS AUTHORIZED USER'S ACCESS TO THE SYSTEM UNDER THIS AGREEMENT.

11. UnityPoint Health understands and agrees that Participant is not obligated to perform any services under this Agreement and that by entering into this Agreement, Participant is not making any guarantee or warranty, express or implied, with respect to any services performed

by Participant for or on behalf of UnityPoint Health.

12. **Auditing.** The Parties agree to comply with an auditing plan to ensure that Authorized Users are only accessing the patient related information needed for the performance of their duties and responsibilities as outlined in the Agreement. The Participant must conduct a monthly audit to ensure that verification will be made when all of the following is true: the patient being accessed was appropriate for the Authorized User; the timeframe of the access was appropriate; and the information accessed regarding the patient was appropriate. The Parties may modify the requirements of the above audit by mutual agreement of the Parties. Failure to enter into good faith negotiations in modifying the auditing plan is considered a material breach of this Agreement. In addition, Participant agrees that UnityPoint Health may audit any Authorized User's access at any time to determine Participant's compliance with this Agreement. To the extent Participant participation in the audit process is required, the time, place, duration, frequency and scope of the audits or monitoring will be reasonable and agreed to in advance. Furthermore, UnityPoint Health may participate in all of Participant's internal investigations regarding access to the System and the use of patient data and other information accessed through the System, and Participant shall share the results of all such investigations with UnityPoint Health.

13. **Term and Termination.**

    a. This Agreement and Participant's access to UnityPoint Health's EHR shall commence as of the Effective Date of this Agreement. The initial term of this Agreement shall be one (1) year, commencing on the Effective Date (the "Initial Term"). Following the Initial Term, this Agreement shall automatically renew for additional one-year terms unless otherwise terminated as provided herein.

    b. Termination by UnityPoint Health. UnityPoint Health may, in its sole discretion, immediately terminate this Agreement, or any individual Authorized User's access to the System, at any time, with or without cause or notice.

    c. Termination by Participant. Participant may terminate this Agreement without cause upon thirty (30) days' prior written notice to UnityPoint Health. Participant's access to the System shall terminate on the effective date of Participant's termination.

    d. Termination Based on Supervening Law. This Agreement may be terminated by either party, upon written notice to the other party specifying the date on which termination will become effective, in the event of any action or threatened action by local, state or federal governmental or accrediting bodies, or any opinion by legal counsel to the effect that any provision of state or federal law or regulation creates a serious risk of assessment, sanction, penalty or other significant consequence to the party giving such notice. The parties acknowledge that this Agreement is being entered into at a time of significant change in state and federal law regarding the delivery and financing of health care services and agree to negotiate in good faith to reform or modify this Agreement in the event of supervening law as defined herein prior to terminating this Agreement, unless termination is reasonably necessary to prevent imminent adverse legal consequence.

14. **No Requirement or Inducement of Referrals**

a. Nothing in this Agreement shall in any way be construed to require or induce either party to admit, refer, or recommend admission or referral of patients to another party, it being the intent that such admissions, referrals, and recommendations be made by each party and its respective medical staff in their best professional judgment and in the patient's best medical interests.

b. Both parties hereby represent and warrant that they are not currently, and at no time have been, excluded from participation in any federally funded health care program, including Medicare and Medicaid. Each party hereby agrees to immediately notify the other party of any threatened, proposed, or actual exclusion from any federally funded health care program, including Medicare and Medicaid. In the event that either party is excluded from any federally funded health care program during the term of this Agreement or, if at any time after the effective date of this Agreement, it is determined that either party is in breach of this section, this Agreement shall, as of the effective date of such exclusion or breach, be automatically terminated.

15. **Contractors and Subcontractors.** The Parties agree that Participant intends to perform Services itself and/or through the use of contractors and/or subcontractors and that the access to the System that is granted to Participant under this Agreement will also be available to Participant's contractors or subcontractors. As such, Participant agrees that it shall obtain written agreement from its contractors and subcontractors who need access to the System to perform services on behalf of Participant to abide by all requirements and perform all obligations of Participant set forth in this Agreement, unless such requirements and obligations are identified herein as not applicable to the contractor or subcontractor, prior to granting Authorized Users of such contractor or subcontractor access to the System under this Agreement. Additionally, Participant will require its contractors and subcontractors to enter into Business Associate Agreements (as defined by HIPAA) or equivalent agreements prior to requesting access to the System under this Agreement. The Parties understand and agree that access to the System will not be granted to any contractors or subcontractors with operations outside the United States.

16. **Notice.** Any notice required to be given by this Agreement shall be in writing and deemed given when personally delivered, faxed, or when deposited in the United States mail, certified or registered mail with return receipt requested, to the following persons (unless otherwise specified in the Agreement):

As to Participant: MEDIC EMS of Scott County
600 West 4th Street
Davenport, IA 52801-1030

As to UnityPoint Health: UnityPoint Health Law Department
1776 West Lakes Parkway, Suite
400 West Des Moines, Iowa 50266-
8239 Fax: (515) 241-4656

17. **Miscellaneous**.

a. **Assignment.** Except as otherwise provided in this Agreement with respect to

contractors and subcontractors of Participant, the rights and obligations of the Parties to this Agreement may not be assigned or subcontracted unless such assignment or subcontract is in writing and consented to by the Parties hereto. Any assignment not in accordance with this Agreement shall be null and void.

b. **Amendment.** This Agreement and the Exhibits attached hereto constitute the entire agreement between the Parties hereto pertaining to the subject matter hereof and supersede all negotiations, preliminary agreements and all prior and contemporaneous discussions and understandings of the Parties in connection with the subject matter hereof. Except as provided in Section 9.b. of this Agreement, no amendment, change or modification of any of the terms, provisions or conditions of this Agreement shall be effective unless made in writing and signed or initialed by all Parties.

c. **Definitions.** Capitalized terms not otherwise defined in this Agreement shall have the meanings given to them in HIPAA.

d. **Waiver.** Waiver of any provision of this Agreement shall not be deemed a waiver of future compliance therewith and such provision shall remain in full force and effect. In the event any provision of this Agreement is held invalid, illegal, or unenforceable, in whole or in part, the remaining provisions of this Agreement shall not be affected thereby and shall continue to be valid and enforceable.

e. **Third Party Beneficiaries.** This Agreement shall be binding upon and shall inure to the benefit of the Parties hereto and their respective legal representatives, successors and permitted assigns. Nothing in this Agreement, express or implied, is intended to confer upon any party, other than the Parties hereto (and their respective heirs, legal representatives, successors and permitted assigns), any rights, remedies, obligations, or liabilities under or by reason of this Agreement.

f. **Choice of Law and Jurisdiction.** This Agreement shall be governed by and construed in accordance with the laws of the State of Iowa without regard to conflicts of law principles. In the event of any dispute, each of the Parties hereby irrevocably submits to the exclusive jurisdiction of any United States Federal Court or Iowa District Court sitting in Polk County, Iowa in any action or proceeding arising out of or relating to this Agreement, and each Party hereby agrees that all claims in respect of such action or proceeding may be heard and determined in such court.

g. **Survival.** In addition to any other terms and conditions of this Agreement that by their nature survive its expiration or termination, all provisions of this Agreement related to privacy, security, confidentiality, limitations of liability, indemnification, notice or governing law shall survive the expiration or termination of this Agreement.

h. **Provisions are Severable.** If any provision of this Agreement is held to be invalid or unenforceable by any judgment of a court of competent jurisdiction, the remainder of this Agreement shall not be affected by such judgment, and the Agreement shall be carried out as nearly as possible according to its original terms and intent.

i. **Authority.** Each individual signing this Agreement warrants and represents that he

or she has full authority to execute this Agreement on behalf of the party for whom he or she has signed.

In witness whereof, the parties have executed this Agreement in duplicate on the dates set below their respective names.

UnityPoint Health	**Participant**
By: _____	By: _____
Title: _____	Title: Director _____
Date: _____	Date: _____

EXHIBIT A

PARTICIPANT SITE ADMINISTRATORS (Require Two)

Name: _____ **Title:** _____

Business Address: _____

Phone #: _____ **Fax #:** _____

Email Address: _____

Name: _____ **Title:** _____

Business Address: _____

Phone #: _____ **Fax #:** _____

Email Address: _____

THIS DOCUMENT IS A SAMPLE OF WHAT EACH USER WILL BE SENT WHEN INDIVIDUAL ACCESS IS REQUESTED.

Exhibit B

UnityPoint Health
INFORMATION SECURITY AGREEMENT (1/21)

Patient, financial, and other business-related information in any form, electronic or printed, is a valuable asset, and is considered private and sensitive. Employees, physicians, physician office staff, consultants, vendors, contracted agency staff, nursing home staff, students, and other authorized users may have access to confidential information in the performance of their duties. Those charged with this responsibility must comply with information confidentiality/security policies in effect at UnityPoint Health (UPH) and its affiliates. This agreement applies regardless of the method of access used.

In consideration of being allowed access to UnityPoint Health information systems, I, the undersigned, hereby agree to the following provisions:

1. I agree to abide by all confidentiality/security policies and procedures for UPH and its affiliates. Updates to state and federal regulations and/or risk mitigation concerns will prompt policy changes from time to time, and I understand it is always my responsibility to abide by the then-current UPH policies. I understand that such policies and procedures are available on the Intranet or will be provided to me upon request.
2. I will not operate or attempt to operate UPH computer equipment without specific authorization.
3. I will not demonstrate the operation of UPH computer equipment or applications to anyone without specific authorization.
4. I will not install or use software that is not licensed by UPH (or that is otherwise unlawful to use) on any UPH information systems, computer equipment, devices, or networks. I understand that unauthorized software may pose security risks and will be removed by UPH.
5. I agree to maintain a unique password, known only to myself, to access the system to read, edit and authenticate data. I understand that my unique password constitutes my electronic signature and that it should be treated as confidential information. I agree not to share my password with any other individual or allow any other individual to use the system once I have accessed it. I understand that I may change my password at any time, and it is my responsibility to reset my password immediately if I suspect it has been compromised.
6. I agree only to access the patient, financial, and/or other UPH business-related information needed for the performance of my duties and responsibilities. I understand that accessing my own patient record or the patient records of my family members is only appropriate to do via the Patient Portal or through the Release of Medical Information process. I agree that I will not use my access granted to me for my job role to look at my record or the records of my family members or others, unless it is in accordance with my professional job duties and responsibilities.
7. I will contact my supervisor, the affiliate compliance officer or Information Security Officer (ISO), or the IT department if I have reason to believe the confidentiality and security of my account has been compromised.
8. I will not disclose any portion of the computerized systems to any unauthorized individuals. This includes, but is not limited to, the design, programming techniques, flow charts, source code, screens, and documentation created by employees, outside resources, or third parties.
9. I will not disclose any portion of the patient's record except to a recipient designated by the patient or to a recipient authorized by UPH who has a "need to know" in order to provide continuing care of the patient.
10. I understand that applications are available outside of the UPH network via various remote access methods (i.e. VPN, Citrix, and/or Web), and I agree to abide by the following when accessing UPH computer systems from remote locations:
    a. I will only access UPH computer systems from remote locations if I am authorized to do so and from only locations in the United States unless I have received prior approval from UPH.
    b. I will use discretion in choosing when and where to access UPH computer systems remotely in order to prevent inadvertent or intentional viewing of displayed or printed information by unauthorized individuals.
    c. I will use proper disposal procedures for all printed materials containing confidential or sensitive information.
    d. I understand that if I choose to use my personal equipment to access UPH computer systems remotely, it is my responsibility to provide internet connectivity, configure firewall and virus protection appropriately,

properly maintain security patches, and to install any necessary software/hardware. UPH is not responsible if the installation of software necessary for accessing UPH computer systems remotely interferes or disrupts the performance of other software/hardware on my personal equipment. UPH will restrict personal devices from connecting to UPH information systems if security posture checks do not pass.

e. I understand that by using my personal equipment to access UPH computer systems that my computer is a de facto extension of the UPH network while connected, and as such is subject to the same rules and regulations that apply to UPH owned equipment.

11. If I will be using a mobile device to access the UPH network or network services (through a personally-owned or UPH-owned device) that include, but is not limited to, email, VPN, or other remote access capabilities, I will allow UPH limited control of my mobile device for the protection of UPH data and its assets. For this context a mobile device is currently identified as a mobile phone, tablet, or other miniaturized computing system. This limited control can include the enforcement of a password/pin and/or remote wiping of the mobile device in the event of loss or theft or other factors that may present a risk of harm to the UPH network, its data, or applications.
    a. I understand using the talk-to-text feature built into the mobile device, like Siri, is not HIPAA-compliant, and I agree to avoid using talk-to-text features if patient information is included unless the talk-to-text tool has been specifically approved by UPH IT.
    b. In the event of loss or theft of my personal device, I agree to the remote wiping of all content on my mobile device, including any personal information I may have stored on the device, such as, but not limited to, photos, videos, and other content stored on the hard drive of the device.
    c. In the event of an investigation or inquiry by the internal compliance department at UPH or the government, or in the event of litigation, I agree to provide UPH and/or its affiliate(s) with access to my device to copy and retain information related to the investigation, inquiry, or litigation. I understand that UPH will take reasonable steps to limit access to personal information, such as using key word searches to identify relevant material.
12. I understand the UPH computer systems are intended to be used for business purposes with limited personal use, such as saving a family picture or my resume, is permitted. If I chose to save my personal files or emails on UPH computer systems, I will save them in a folder clearly marked “personal”. I understand that upon my departure with the organization, all business-related emails and files that are not clearly saved in my “personal” folder may be transferred to my manager or their designee in order to continue business operations.
13. I understand that UPH regularly audits access to UPH computer equipment, applications, and the data contained in these systems. I agree to cooperate with UPH regarding these audits or other inspections of equipment and data, including UPH inquiries that arise as a result of such audits.
14. I agree to report any activity which is contrary to UPH policies or the terms of this agreement to my supervisor, the affiliate compliance officer, or to the IT Service Center at **800-681-2060.**

I understand that I must sign this Agreement as a precondition to issuance of a computer password for access to the UPH network and/or patient information and that failure to comply with the preceding provisions will result in formal disciplinary action, which may include, but will not be limited to, termination of access, termination of employment in the case of employees, termination of agreements in the case of contractors, or revocation of clinical privileges in the case of medical staff members, taken in accordance with applicable medical staff by-laws, rules and regulations.

PRINT NAME_____

SIGNATURE_____ DATE_____

DEPARTMENT_____

COMPANY_____

PLEASE SCAN SIGNED FORM AND SEND VIA E-MAIL WITH EXCEL SPREADSHEET TO

THE COUNTY AUDITOR'S SIGNATURE CERTIFIES THAT THIS RESOLUTION HAS BEEN FORMALLY APPROVED BY THE BOARD OF SUPERVISORS ON _____.
DATE

SCOTT COUNTY AUDITOR

R E S O L U T I O N

SCOTT COUNTY BOARD OF SUPERVISORS

DECEMBER 19, 2023

APPROVING SYSTEM ACCESS AGREEMENT BETWEEN MEDIC EMS OF SCOTT COUNTY AND IOWA HEALTH SYSTEM D/B/A UNITYPOINT HEALTH.

BE IT RESOLVED BY the Scott County Board of Supervisors as follows:

Section 1. This agreement provides MEDIC EMS of Scott County access to the UnityPoint Health Electronic Health Records to gather necessary information for billing patients and to conduct clinical outcome data gathering.

Section 2. That the Director of MEDIC EMS of Scott County is hereby authorized to sign said agreements on behalf of the Board.

Section 3: This resolution shall take effect immediately.