

Green LA, White LL, Barry HC, Nease DE, Jr, Hudson BL. Infrastructure requirements for practice-based research networks. *Ann Fam Med*. 2005;3(Suppl 1):S5-S11.

http://www.annfammed.org/cgi/content/full/3/suppl_1/S5

Supplemental Appendix. Example of HIPAA-Compliant Business Agency Agreement

(Used in GRIN, approved by University of Michigan Health Systems Attorney's Office, developed from an agreement created by OKNet, and approved by the University of Oklahoma)

THIS AGREEMENT, effective the <> day of <>, <> by and between the Board of Regents of the University of Michigan (hereinafter referred to as "University") on behalf of the Department of Family Medicine (hereinafter referred to as "Department") and <name of practice> (hereinafter referred to as "Site").

Under this agreement, the Department will act as the information systems operator to provide the ClinfoTracker patient problem list and clinical reminder system to <name of practice>. <name of practice> will use ClinfoTracker services for its quality improvement efforts, with support from the Department. In exchange, <name of practice> will permit the Department faculty who develop and maintain ClinfoTracker to use HIPAA-compliant de-identified summary data to explore scientific questions, and will give due consideration to sharing identifiable information for specific research projects on a case-by-case basis subject to institutional review board (IRB) approval and patient informed consent as applicable.

Confidentiality of Protected Health Information. To the extent the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is applicable to this agreement, each party, its officers and employees, agree as follows. Each party acknowledges that it may have or obtain access to confidential protected health information (PHI), including but not limited to individually identifiable health information. Each party may use PHI solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Each party acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or by law. Specifically, each party agrees it will:

- (a) not use or further disclose PHI except as permitted in this Agreement or as required by law, and in such case, disclose only the minimum necessary;
- (b) protect and safeguard from any oral and written disclosure all confidential information, regardless of the types of media on which it is stored, with which it may come in contact;
- (c) use appropriate safeguards to prevent use or disclosure of PHI other than as permitted by this Agreement or as required by law;
- (d) require that all of its subcontractors, vendors, and agents to whom it provides PHI pursuant to the terms of this Agreement shall agree to all of the same restrictions and conditions to which it is bound;
- (e) report to the other any unauthorized use or disclosure immediately upon becoming aware of it and mitigate any harmful effects known to it of a use or disclosure it makes in violation of this Agreement;
- (f) to the extent allowed by law, indemnify and hold the other party harmless from all claims, liabilities, costs, and damages arising out of or in any manner related to the disclosure by the indemnifying party of any PHI or to the breach by the indemnifying party of any obligation related to PHI;

Online Supplementary Data

- (g) make PHI available to the other in accordance with 45 CFR §164.524; (h) make PHI available for amendment and incorporate any amendments to PHI in accordance with 45 CFR §164.526;
- (i) make the information required to provide an accounting of disclosures available in accordance with 45 CFR §164.528; (j) make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by one party on behalf of the other available to the Secretary of Health and Human Services, governmental officers and agencies, and the other for the purpose of determining compliance with 45 CFR §§164.500- 534;
- (k) upon termination of this Agreement, return or destroy all PHI, if feasible, received from or created or received by it on behalf of the other which it maintains in any form, and retain no copies of such information. If such return or destruction is not feasible, it will extend the precautions of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
- (l) comply with all applicable laws and regulations specifically including, but not limited to, HIPAA.

Each party recognizes that any breach of confidentiality or misuse of information may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' Agreement. Unauthorized disclosure may cause irreparable injury to the patient or to the owner of such information and, accordingly, the patient or the owner of such information may pursue legal remedies against it.

Except as otherwise limited in this Agreement, each party may use or disclose PHI to perform the functions, activities, and services for, or on behalf of, the other as specified in this Agreement, provided that such use or disclosure would not violate applicable HIPAA provisions if done by the other.

When and to the extent required to do so, each party will make its Privacy Notice available to the other.

Agreed upon by:

<name of authorized signer for UM>
<title of signer>

Date

<name of authorized signer for practice>
<name of practice>

Date