IMPACT
Virtual First Medical Practice Collaboration

Hosted by the Digital Medicine Society (DiMe) and the American Telemedicine Association (ATA), IMPACT is a pre-competitive collaboration of leading digital health companies, investors, payers, and consultants dedicated to supporting virtual first care (V1C) organizations and their commitment to patient-centric care.

Terms used throughout this resource are defined in the Glossary of Terms.

Contract Exhibit: Data

This exhibit covers what project-related data each party will collect, what data will be shared between parties, file standards for sharing, and security mechanisms in place to protect data. Data sharing is always guided by the question of whether data is being shared for use in Treatment, Payment, or Operations (TPO) of the payer's organization or the virtual first care (V1C) service, and therefore whether that data exchange is a part of each party's Health Insurance Portability and Accountability Act (HIPAA)-covered status. Where data is not covered under a party's TPO or where the recipient of participant data is not a HIPAA covered entity (e.g. fully insured employers), additional documentation around appropriate permissions to access, security practices, and other agreements (such as a business associate agreement (BAA) or patient consent) may be necessary.

Data use is a primary focus of this section. Generally, data use falls into these categories and the contracting parties will need to discuss if and how data will be exchanged in each instance:

Data Type	Data Use	Sample Data Flow
Outreach	To invite members to join a V1C service	Payer copy of member name, email, address, and/or phone will be used by payer for outreach or shared with V1C service to conduct outreach. Data sharing with V1C solution ideally excludes member numbers for security purposes. This data may be collected again by a V1C service in the onboarding process.
Member Eligibility	To support ongoing checks of member eligibility for coverage of care by the payer at the start and for the duration of an individuals participation on a V1C service	Payer houses member name, number, and eligibility status. Data is made available to V1C service either through a platform that can be accessed by V1C service to determine real time eligibility (through a 270 ping) or through a monthly eligibility report transmitted to

		the V1C service. Data on the result of the eligibility check (271 response) is owned by the V1C service, as it is with any provider.
Program Delivery	To support care coordination and payer benefit personalization	Payers may share claims data and other clinical information they store about V1C participant-related medical care provided outside of a V1C solution. V1C services store personal health information (PHI) in their Electronic Health Record (EHR), including clinical, test results or other information about a participant and the care being provided by the V1C service.
Program Participation & Outcomes	To measure enrollment, engagement, and health outcomes	Payers may share claims data and other clinical information about a V1C participant related to medical care provided outside of a V1C solution as part of program outcome analyses. V1C services may share enrollment data, EHR data (de-identified as required by the HIPAA coverage status of the receiving entity), and engagement data. Sharing of this data doesn't change ownership of PHI or proprietary nature of the data.
Program Evaluation	To measure non-clinical outcome variables of V1C performance, such as costs and member satisfaction	Payers may share claims data or member satisfaction data. V1C services may share EHR data, participant engagement, or satisfaction data. Again, ownership resides with the originating party and any publication or Intellectual Property (IP) would be assigned according to data originating from a single party or shared by both parties. Identifiability of data disclosed is defined by HIPAA rules.

Where data will be exchanged, how it will be shared, what the rights are of each party to use another party's data, and data security requirements will all be covered in this section. Finally, this section will include agreements on continuity of TPO data availability following contract termination.

V1C CONSIDERATION: **Data**

Since both parties are covered entities, requests for data sharing from both parties should be respected where that data (including PHI) is deemed necessary and appropriate for the conduct of each of their TPO, consistent with:

- Guidance from Office for Civil Rights (OCR) on exchange of PHI for the other party's health care operations, and
- The Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS) rules and standards for exchange (for example, the data available in the U. S. Core Data for Interoperability standards for certified EHRs and to payers).
  V1C owns payer member data generated on their platform since V1C platform is a medical record and the provider is obligated to own and manage that.

IDEAL ★★★	TO AVOID ☆☆☆
General	
Security requirements should follow traditional provider security expectations — System and Organization Control (SOC) 2 Type II Report or HITRUST should suffice for non-TPO data Agreements and projects should proceed if V1C service is still in process of obtaining security certifications, as long as good faith effort and progress are being made Usage of Fast Healthcare Interoperability Resources (FHIR) standards for seamless Application Programming Interface (API) integration	Additional security requirements mandated by payer beyond SOC 2 and HITRUST — exposure to member information is low and given V1C is a covered entity they should be trusted Requests/requirements to provide a SOC 1 (either Type I or Type II) report. A SOC 1 is related to financial controls for publicly traded companies. Unless a V1C service is part of a publicly traded company, this should not be required Payer ownership of V1C data — V1Cs are providers and like all doctor's offices, and therefore are the "owner" of all data acquired from patients and stored in Electronic Medical Record (EMR) upon establishing a care relationship. (Payer retains ownership of marketing data since this is prior to establishment of care relationship.) Data blocking — data should be allowed to flow bi-directionally when legitimate TPO justification exists
Program Evaluation	
Where the V1C-payer is undertaking activities that are primarily intended to	Arbitrary assumption that consent is/is not needed. OCR/ONC fact sheet on

contribute to general knowledge, beyond TPO, routine treatment, and internal use of V1C service data for analyses, consent from V1C participants for research uses of data will be needed. Examples include where activities, tests, and assessments in addition to the routine care provided by a V1C solution are being asked of patients to support research goals; engaging external parties (such as researchers, or research institutions) to conduct studies, etc.	exchange of data, and the OCR FAQ on what research is should be considered

..... *Phase 1* .....>	..... *Phase 2* .....>
If vision for phase 2 is that the V1C service is performing non-TPO activities, include details for initiating necessary security assessments and processes to setup phase 2	If V1C service is performing non-TPO activities, SOC 2/HITRUST security assessment in process or completed should be contemplated

QUICK LINKS: GUIDE TO PAYER - VIRTUAL FIRST CARE (V1C) CONTRACTING

Overview

Payer-V1C Contract Fundamentals

How To Use The Guide to Payer-V1C Contracting

Glossary of Terms

Contract Body

- Termination Rights
- Assignment of Agreement or Obligations
- Business Associate Agreement
- Publicity
- Payment

Contract Exhibits

- Data
- Subcontractors
- Credentialing/Certification & Licenses
- Audits
- Publication Rights
- Statement of Work