Contract Guidelines

Overview

What revisions, if any, will M2S, the Society for Vascular Surgery Patient Safety Organization (SVS PSO), and/or the Society of NeuroInterventional Surgery (SNIS PSO) (herein referred to as the "Service Providers") consider to the agreements?

The Service Providers may, in limited circumstances, consider *modest* changes to the Service and Business Associate Agreements, provided the revisions are critical to the operation and protection of the participants' business and do not impact the Service Providers' ability to provide its standard set of services to all of their other participants. In fact, the nature of the services provided requires that the Service Providers utilize the same set of terms and conditions for all participants. For this reason, the Service Providers will not accept material changes to the risk allocation provisions, particularly the provisions regarding indemnification and limitation on damages.

Potential participants should also bear in mind that the Service Providers charge a modest amount for their services and those charges do not support the cost of extensive legal revisions or negotiations. If, once negotiations begin, it becomes clear to the parties that the contracting process may extend beyond a reasonable time and/or require intensive involvement by the parties' respective attorneys, a decision may be made either to not extend the services or to reassess the fee structure in order to account for the additional costs incurred for the prolonged negotiations.

Service Providers ask that all potential participants follow the guidelines stated herein for the negotiation of the remaining issues.

How are revisions negotiated?

The Service Provider will immediately reject wholesale changes to the documents or alternative Business Associate Agreements if the changes proposed by the Service Providers have not been incorporated. If there are revisions that meet the standards for consideration outlined herein, the potential participant should use the "track changes" feature of Microsoft Word® to insert revisions into the contract and embed a comment for each such revision explaining the business need for it.

Upon receipt of revisions from the potential participant, the Service Providers will accept those revisions that it agrees to accept, reject those that it cannot accept, and modify those revisions that are acceptable as modified. Upon receiving the revised contract from the Service Providers, the participant should then respond to the Service Providers' changes using these same "accept / reject / modify" criteria. The Service Provider will consider, after two revisions, a teleconference or meeting to advance or conclude negotiations. Prior to any such discussion, the Service Providers will require that the participant has accepted, rejected or modified the Service Providers' revisions to the contract so that the issues remaining for discussion are well-identified and understandable.

Additional terms and conditions attached or merely referenced in any of the required Agreements will not be considered. If additional terms and conditions are to be negotiated, they must be introduced into the main body of the contract and negotiated through the normal contracting process**.**

What is a PSO?

The Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act) authorized the creation of Patient Safety Organizations (PSOs) to improve the quality and safety of U.S. health care delivery. The Patient Safety Act encourages clinicians and health care organizations to voluntarily report and share quality and patient safety information without fear of legal discovery, need for patient consent or Internal Review Board (IRB) approval. To read the Patient Safety Act, go to

http://www.pso.ahrq.gov/statute/pl109-41.htm. Of course, patient consent or IRB approval may be required for studies done by contributing health care providers or the SNIS or SVS PSOs.

To implement the Patient Safety Act, the Department of Health and Human Services issued the Patient Safety and Quality Improvement final rule (Patient Safety Rule, PDF file, 760 KB. PDF Help). The Patient Safety Act and the Patient Safety Rule authorized the creation of PSOs to improve quality and safety through the collection and analysis of data on patient events.

The Patient Safety Act allows collection of patient identifiers, such as name and social security numbers, for quality improvement purposes due to the strict protections around non-identification of data. Non-identification includes compliance with the HIPAA de-identification rules by removing all patient identifiers in addition to the removal of all physician and contracting entity identifiers before any data can be released for research purposes. Internally, we use patient identifiers to match patients to the Social Security Death Index (SSDI) to update the mortality of the patients in the database. We also internally use identifiers to match to claims data for our annual validation that all procedures have been entered into the database, a requirement for participation.

What is the benefit of participating in the VQI Regional Groups?

Regional quality groups meet semi-annually to discuss variation in patient selection, process of care and outcomes with anonymous comparison among centers. They benefit from big data collected across the entire country, but promote local ownership of quality improvement projects that benefit all centers in a region. Regional groups appoint representatives to the governance and quality committees of the SVS PSO, so provide an opportunity to shape national activities. Centers that participate in regional groups receive special reports comparing centers within their region, which stimulate interesting discussion and helps individual practitioners understand the perspective of respected colleagues in their regional group.

Data Management and PSO Services Agreements

Will the Service Providers agree to revise the indemnity provisions of the agreements?

No. The current indemnity provisions are fair, reasonable and equitable for all the parties involved as they provide for mutual indemnity for damages that result from third party actions arising out of a breach by one of the Service Providers or a participant. The Service Providers will not assume the risk of not being made whole after being sued for the actions of the participant. The Service Providers are willing to insert language that states "*To the extent permitted by law*" before the indemnity provision for those participants operating under a rule of law for which there is a question as to the availability of an indemnity.

Will the Service Providers agree to revise the limitation of liability provisions of the agreements?

No. Because the Agreements limit the Service Providers' liability to the fees paid, the limitation of liability provision limits the Service Providers' liability to the value to which the contracting parties have agreed for the service provided. Such limitations are standard in commercial agreements of this kind. Revisions to the limitation of liability provision to have the Service Providers effectively assume unlimited liability will not be accepted as this is an unsupportable business proposition for the Service Providers. The Service Providers are willing to insert language that states "*To the extent permitted by law*" before the limitation of liability provision.

My organization has internal policies that we believe are essential to the operation of our business. Will the Service Providers agree to comply with my policies, even if that requires them to change their own procedures?

No. The Service Providers cannot agree to abide by any one participant's set of policies as each of its participants' policies may be different. Agreeing to abide by one code of conduct inevitably forces the Service Providers to court the risk of breaching another participant's policies and contract.

The Service Providers will agree, in limited circumstances, to comply with an internal policy of a participant if a) the policy is reasonable and does not impose a requirement that conflicts with the Service Providers' policies or procedures or otherwise interferes with the proper operation of the Service Provider and b) the policy's operative language to be enforced against the Service Providers is incorporated directly into the parties' agreements as an exhibit; citation references to the policy will not suffice.

We would prefer not to send patient identifiable information to the Service Providers. Why is that data included in the database?

PATHWAYS collects identifiable data for several purposes: 1) prevention of duplicate patient entry into the system at a single center; 2) association of the data with the Social Security Death Index for improved long-term survival reporting; 3) performance of an annual validation against claims data to ensure consecutive case entry into PATHWAYS (consecutive case entry is important for mitigating selection bias from the aggregate datasets); and 4) permitting the participant to download identifiable data entered for center-specific quality improvement work.

We are subject to our state's privacy laws as well as federal privacy laws. Will the Service Providers agree to change their procedures to comply with our state's laws?

No. The Service Providers' operations have an international scope. The Service Providers comply with federal privacy law but cannot agree to comply with every local jurisdiction's privacy laws. It would be inevitable that the law of one local jurisdiction would conflict or be inconsistent with that of another. The Service Providers' compliance with each conflicting provision would therefore put the Service Providers in the untenable position of courting a breach of its participant agreements.

The Service Providers will agree, in limited circumstances, to comply with a particular provision of state law if a) the law does not impose a requirement that conflicts with the Service Providers' other legal obligations or otherwise interferes with proper operation and b) the law's operative language to be enforced against the Service Providers is incorporated directly into the parties' agreements; citation references to the law will not suffice.

Why are the agreements silent as to choice of forum?

The Service Providers do not anticipate litigation. However, if there is litigation, it will likely involve participants in many states. In a suit involving multiple parties in multiple states, one participant's contractual choice of a forum would impose an injustice on all other participants. The agreements remain silent on the issue and leave the courts to choose the most appropriate forum if necessary. If a participant's own contracting guidelines require that a choice of forum must be listed, the Service Providers will agree to Delaware.

Why do the agreements automatically renew?

The Service Providers work to ensure that a participant's access to PATHWAYS is continuous and uninterrupted. The agreements must therefore be continuous and uninterrupted; the negotiation of a new set of contracts covering the same subject matter as a lapsed agreement should not suspend a participant's access to PATHWAYS.

Because the agreements permit participants to terminate the agreements without cause upon 30 days' notice at any time after the first year, the prospect of an automatic renewal is not a serious commitment.

Business Associates Agreements

We understand that our organization will continue to own all Protected Health Information that we send you. May we require you to return or destroy PHI when the contracts terminate?

Yes. All data that is entered into PATHWAYS on the M2S servers, other than that contained in the Service Providers' off-site back-up system and historical blinded datasets, will be returned or destroyed within 90 days of termination. The return or destruction of the offsite data is not feasible, therefore the Service Providers will extend the protections of the agreements to the off-site data and limit further uses and disclosures.

Do the Service Providers comply with the Red Flag Rules?

No. The Red Flag rules do not apply to PATHWAYS activities. All references to such rules in the agreements are either removed or deemed to be inapplicable.

We need to know if the Service Providers use or disclose PHI in breach of the agreements. Will the Service Providers agree to notify me in case of a breach?

Yes. 45 CFR §164.410 requires the Service Providers to report a breach to the participant no later than sixty (60) days after learning of the breach. It is important to note that the Service Provider does not act as an *agent* of the participant and therefore the participant is allowed 60 days after notification from the Service Provider. As you will see in our BAA template, we have adjusted such language to state no later than thirty (30) days. Although this point may be negotiable, it is important to understand that we cannot agree to anything less than ten (10) business days regarding notification of breach to the participant. The Service Provider will comply with that law and will reserve that legal authorization in their contracts.

We may need the Service Providers to contact a patient if the patient's PHI is used or disclosed without authorization. Will the Service Providers do that on our behalf?

No. Because direct notification of a patient would require the Service Providers to collect additional personally identifiable information for each patient and thereby increase the number of access points through which such information can be disclosed, the Service Providers' policies prohibit them from initiating direct contact with any patient. The Service Providers' legal obligations are for the benefit of the participant alone, not an individual patient.

We need to be sure the PHI we send to the Service Providers is secure. Will the Service Providers report so-called "security incidents" to us?

Yes. Because the security of a participant's data is the Service Providers' first priority, the Service Providers will report to the participant any incidents that may have put the data at risk. However, events may be considered a "security incident" under the law even though PHI is not put at risk, such as when the PHI database is "pinged" or scanned. The Service Providers will not report such instances because reporting each and every such non-substantive incident is too burdensome and offers the participant no meaningful information regarding the security of its data. All Business Associate Agreements must include the following language: "Business Associate shall report to the Covered Entity and Security Incident of which it becomes aware, excluding those that do not affect ePHI in accordance with applicable law, such as "pings" on an information system firewall; port scans; attempts to log on to an information system or enter a database with an invalid password or user

name; denial-of-service attacks that do not result in a server being taken offline; or malware (e.g. a worm or a virus) that does not result in unauthorized access, use, disclosure, modification or destruction of PHI".

We usually reserve the right to conduct an audit of our vendors' operations. Will the Service Providers agree to audits by its participants?

No, not without clear and convincing evidence that an audit is absolutely necessary. Because an audit by one participant puts all of the Service Providers' other participants' confidential data at risk of disclosure, the Service Providers do not permit any one participant to have access to their books and records. This policy also protects the Service Providers against the risk that agreeing to each of its participant's demands for audits would force them into a state of perpetual audit.

As to security audits, the Service Providers receive a monthly report about the security of their systems. The Service Providers can make that report available to any participant upon written request.

Although the services agreement contains a particular contract provision, we believe that particular provision should also be included in the BAA or vice versa. Will the Service Providers agree to address the same issue more than once?

No. Because the services agreement and the BAA are valid and enforceable contracts between the parties, there is no need to restate contract provisions in one contract that is already addressed in the other. Doing so only invites dispute as to the applicability and meaning of each such provision, especially if different language is used.

If, inadvertently or otherwise, terms are included in each contract that directly contradict each other, the terms and conditions of the services agreement will govern to the extent of the direct contradiction with the terms and conditions of the BAA. The Service Provider will accept the Business Associate Agreement being incorporated as an exhibit to the Service Agreements.

Can a potential participant propose using an alternate Business Associate Agreement?

The Service Providers will accept an alternative Business Associate Agreements as long as it complies with the requirements stated above. These changes must be included in the proposed Business Associate Agreement prior to being submitted for review.

General

What levels of insurance coverage do the Service Providers carry?

Each of the Service Providers is covered by liability insurance and other forms of insurance coverage consistent with prudent practices in its business. The limits of coverage for the principal insurable issues are as follows:

General Liability	**M2S**	**SVS PSO**	**SNIS PSO**
Each Occurrence	$1,000,000	$1,000,000	$1,000,000
General Aggregate	$2,000,000	$2,000,000	2,000,000
Excess/Umbrella Liability	**M2S**	**SVS PSO**	**SNIS PSO**
Each Occurrence	$5,000,000	$5,000,000	$5,000,000
Aggregate	$5,000,000	$5,000,000	$5,000,000

Errors & Omissions	M2S	SVS PSO	SNIS PSO
Each Occurrence	$3,000,000	$3,000,000	2,000,000
General Aggregate	$3,000,000	$3,000,000	2,000,000
Privacy Remediation Sublimit	$500,000	N/A	N/A

Can a Participant obtain evidence of the Service Providers' insurance coverage?

Yes. Insurance certificates are available upon request.

Why are participants required to sign up to six agreements?

M2S, SVS PSO, and SNIS PSO are all separate legal entities and each provides different services to the participants. Each entity therefore requires separate agreements that outline the separate and distinct services that each entity will provide to the participant. In addition, under HIPAA, each entity is a separate "Business Associate" of the participants and must sign separate BAAs with the participants.

Whom should participants contact with questions regarding the SVS PSO Agreements?

Carrie Bosela, Administrative Director, RN, CPC, CPC-I
Society for Vascular Surgery Patient Safety Organization
633 North Saint Clair Street, 22nd Floor
Chicago, IL 60611
(O) 603.298.5509 ext. 329, (C) 603-558-0163
c.bosela@svspso.org

Whom should participants contact with questions regarding the SNIS PSO Agreements?

Marie Williams, Executive Director
Society of NeuroInterventional Surgery Patient Safety Organization
3975 Fair Ridge Drive, Suite 200 North
Fairfax, Virginia 22033
(O) 703.691.2272
williams@snisonline.org

Whom should participants contact with questions regarding the M2S Agreements?

Maggie Frank, Contracts Manager, JD
M2S, Inc.
12 Commerce Avenue
West Lebanon, NH 03784
Direct: 603-298-5509 ext. 377
mfrank@m2s.com