True North Patient Safety Organization

PARTICIPANT MANUAL

January 2020

Table of Contents

I. General

What is a PSO?

A PSO is a patient safety organization. A federal statute and its implementing regulations authorize the creation of PSOs to allow for the sharing of quality information outside of hospitals and across healthcare organizations, while maintaining the information's confidentiality and privilege.

State laws vary with regard to how extensively they protect the confidentiality and privilege of quality information when it is shared outside of a hospital or health system. In many states, if healthcare systems share data even within the system across or between facilities, the information loses its confidentiality and privilege. This means that the information could be subject to discovery in litigation or when requested by a patient.

A PSO can layer federal protections on top of state law protections, creating more opportunities to share information in a "safe" space. Therefore, with limited exception, Participants who join a PSO can aggregate, compare, and analyze their quality metrics and experiences with patient safety events with other Participants without fear.

What is True North PSO?

True North Patient Safety Organization, Inc. ("True North PSO") is a subsidiary of Northwell Health, which acts independently of Northwell Health. True North PSO's mission is to constantly improve patient safety and quality of care by collecting and analyzing patient safety information, sharing lessons learned to eliminate preventable harm and create knowledge-sharing opportunities around best practices. True North PSO's goal is to be recognized as a gold standard for patient safety within national health systems.

Will all of our quality information be protected if my organization joins the PSO?

No. PSOs do not protect all information held by Participants. PSOs protect information that is designated to be protected by the PSO and deemed to be patient safety work product (PSWP). PSWP can be shared by the Participant to the PSO or received from the PSO. In short, PSWP is any data, reports, records, memoranda, analyses, or written or oral statements assembled for or reported to the PSO which could improve patient safety, healthcare quality or healthcare outcomes. Section II below discusses this concept in greater detail.

II. Becoming a Participant

Sounds good; how do we join True North PSO?

A Participant joins the PSO by signing the True North PSO participation agreement. Before signing, Participants should have comprehensive internal discussions to ensure they are willing and able to undertake the responsibilities of being an active Participant. PSO participation requires time and attention, including the appointment of designated staff to:

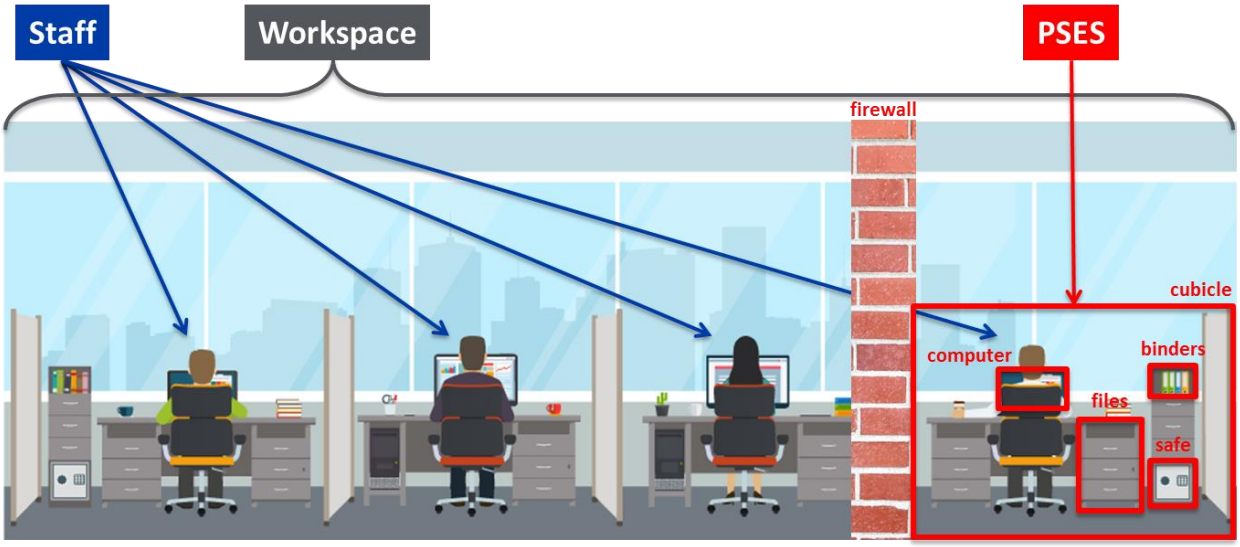
1. Learn and understand the PSO information sharing expectations and limitations
2. Manage the Participant's participation in the PSO, including collecting, preparing and submitting PSWP to the PSO and receiving PSWP from the PSO
3. Ensure any PSWP collected by the Participant for the PSO or received from the PSO or another Participant is stored and disseminated appropriately to maintain security and confidentiality
4. Participate in various PSO Safe Tables to discuss patient safety events
5. Create a patient safety evaluation system (discussed below)

What is a patient safety evaluation system?

A patient safety evaluation system (PSES) is the "space" within the Participant organization where PSWP is collected, maintained and submitted, and PSWP from the PSO is received. This requires designating physical space (such as a locked drawer or file cabinet) where hard copies of the Participant's PSWP will be stored, and an electronic location (such as an encrypted drive on a computer) where electronic files will be stored. The PSES will also include the means by which the Participant receives, collects or reports PSWP, such as a secure email address. Anytime PSWP is shared within the Participant organization, regardless of the type of communication, the sharing pathway will be a part of the PSES. PSWP should travel within the Participant organization only via authorized channels, which will become part of the PSES, and should be secured and monitored to ensure confidentiality.

Staff access is also part of the PSES. PSWP must be accessible only to staff members of a Participant Organization who have signed a PSO confidentiality agreement and who are working with the PSO, or for PSO purposes. Staff must be trained to make sure they observe the firewalls developed by the organization to protect the PSWP from inappropriate use or disclosure that could compromise the confidentiality and privilege protections.

True North PSO is available to assist Participants in thinking through the development of a PSES.



Tell me more; how can we ensure the PSWP is protected from unauthorized access and disclosure?

In order to protect PSWP housed within the PSES, access to the PSES must be limited, and the PSES must be protected from unauthorized access or use, including by ensuring the following:

No access will be given to any Participant employees who are not designated by the Participant to access, submit or receive PSWP ("Participant Staff").
Every staff member of the PSO team (those who create, submit or receive PSWP) will sign a confidentiality agreement and receive PSO training.
Role-based access will be developed for Participant Staff so that each individual who has access to PSWP and the Participant's PSES understands when he/she is able to access the PSES or view PSWP.

Once the Participant has its PSES defined and operationalized and its staff trained on the PSO mission, scope, tasks and confidentiality rules, the Participant is able to begin participating in the PSO.

III. Initial Participation in True North PSO

We're ready to join; what happens next?

a) Appoint a PSO liaison

When a Participant is ready to join the PSO, the Participant must sign the participation agreement and appoint someone to serve as its PSO liaison, who will be responsible for collecting PSWP within the Participant organization and transmitting and receiving patient PSWP to/from True North PSO. The PSO liaison will be the primary contact for True North PSO and will participate in or be responsible for finding the appropriate participants for PSO safe tables.

b) Develop policies and procedures

The PSO liaison should work with the additional Participant stakeholders to develop internal policy and procedures (P&Ps) for PSO participation.
These P&Ps should:

1. Identify Participant Staff. Every member of the Participant Staff should sign a confidentiality agreement (a model of which is attached to this manual).
2. Define both the physical and electronic attributes of the Participant's PSES, including where the Participant's PSWP will be stored.
3. Explain the safeguards the Participant will use to ensure no one outside the Participant Staff is able or permitted to access PSO materials.
4. Confirm the data that will be collected by the Participant for submission to the True North PSO, as required by the PSO.
5. Explain how data and information collected for the purpose of submission to True North PSO will be identified as such (this is required for confidentiality protection to apply, as discussed further in Section IV). While the Participant is permitted to develop any labels determined appropriate by the Participant, True North PSO provides suggested language in Section IV below.
6. List Participant Staff's responsibilities to ensure that data is submitted to True North PSO in compliance with True North PSO's requirements, True North PSO's Safe Tables are attended by the Participant, and PSO-produced analysis and reports are reviewed and utilized by the Participant.
7. Ensure that the Participant also complies with HIPAA when submitting and receiving PSWP.
8. Explain that the Participant will not take adverse employment action against an individual based on the fact that the individual, in good faith, reported information

directly to True North PSO or someone within the Participant organization for the purpose of having the information reported to the PSO.

9. Develop an internal record retention policy which, at a minimum, records what PSWP has been disclosed to the PSO, the date of the disclosure and the specific information that was disclosed.

c) Conduct staff training

The Participant must provide Participant Staff training. The training must include the goals of participating in the PSO, the responsibilities of participating, the confidentiality of PSWP, the importance of maintaining PSWP within the PSES and the importance of limiting access to PSWP to the Participant Staff. The training should culminate with the signing of a confidentiality agreement, similar to that attached to this manual, which should be updated annually.

Questions on PSO and PSWP training can be directed to Kristin McOlvin, True North PSO Administrator, at **Kmcolvin1@truenorthpso.org.**

d) Share PSWP with PSO

Participants will share PSWP with True North PSO. In order to share certain quality data with True North PSO, the Participant must follow technical guidance to be provided by True North PSO. Participants will be expected to transmit different data types at different frequencies. More information from True North PSO will be forthcoming.

e) Begin collecting PSWP in PSES, for submission to PSO

A Participant's PSWP includes any data, reports, records, memoranda, analyses (such as root cause analyses) or written or oral statements (or copies of any of this material) which could improve patient safety, healthcare quality or healthcare outcomes, and which:

1. Are assembled or developed *for* reporting to a PSO and reported to a PSO, including information that indicates it was prepared for submission to True North PSO (explained in more detail below)
2. Identify or constitute the deliberations or analysis of a PSES, or pertain to reporting to a PSES

PSWP *does not* include:

1. *Original* medical records, billing and discharge information, or any other original patient or provider information; copies of selected parts of original provider records may become PSWP

2. Information that is collected, maintained or developed separately, or exists separately, from the PSES

To ensure PSWP within the PSES is protected even before it is submitted to the PSO, the Participant should clarify that the PSWP is intended for reporting or submission to True North PSO.

Therefore, when PSWP is collected, best practice is to label the PSWP with an identifying watermark, header or the like, in order to clearly demarcate the day the PSWP was entered into the PSES and that the PSWP is intended to be reported to the PSO.

Draft Document Disclaimer:

"Prepared/Compiled for submission to True North PSO on [Date]"

"Submitted to True North PSO [on Date]"

"Protected under the Patient Safety and Quality Improvement Act of 2005"

Draft Email Disclaimer:

This email transmission, and any documents, files or previous email messages attached to it, contains information that was prepared for submission to or has been received from True North Patient Safety Organization, Inc., and the information contained is intended to be confidential and privileged and afforded all protections under the Patient Safety and Quality Improvement Act of 2005.

Once the Participant has segregated PSWP for the purpose of reporting to the PSO, and "placed it" in the PSES, the PSWP becomes privileged and confidential.[1]

f) Oops, we included information in our PSES that should not have been PSWP. Can the information be removed?

Yes. If a Participant collects, develops or assembles data or information with the intent of submitting it to the PSO, but later determines the PSWP is not appropriate for the PSO, PSWP can be removed from a PSES and no longer considered PSWP if (1) the information has not yet been reported to a PSO and (2) the Participant documents the act and date of removal of such information from the PSES.

[1] If a Participant fails to document this information, the Department of Health & Human Services will presume the intent to report information in the PSES to the PSO is present, absent evidence to the contrary.

IV. Understanding the Confidentiality and Privilege Protections Afforded to PSWP

PSWP is privileged and confidential. This means that it generally cannot be required to be produced in response to a discovery request, a subpoena or an order, or admitted as evidence in a court or a professional disciplinary proceeding.

There are some exceptions to this general rule. PSWP is no longer privileged and may be disclosed:

1. In a criminal proceeding, after an in-camera review and determination that the PSWP contains evidence of a criminal act, is material to the proceeding and is not reasonably available from any other source
2. To the extent required to ensure equitable relief for persons who reported the PSWP, if the court considering such PSWP has issued a protective order to protect the confidentiality of the PSWP
3. When authorized by each of the identified Participants or providers
4. When the PSWP is nonidentifiable

a) Disclosing deidentified or nonidentifiable PSWP

Identifiable PSWP is PSWP that (1) is presented in a form and manner that allows the identification of any provider that is a subject of the work product, or any providers that participate in, or are responsible for, activities that are a subject of the work product; (2) constitutes individually identifiable health information as that term is defined in the HIPAA Privacy Rule at 45 CFR 160.103; or (3) is presented in a form or manner that allows the identification of an individual who in good faith reported information directly to a PSO or to a provider with the intention of having the information reported to a PSO.

Deidentified PSWP is PSWP that has had all the direct identifiers removed.

Nonidentifiable PSWP is deidentified PSWP *after* it has undergone the removal of all direct identifiers *and* (a) all geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code and equivalent geocodes, except for the initial three digits of a ZIP code if, according to the current data publicly available from the United States Census Bureau, the geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; (b) all elements of dates (except year) for dates directly related to a patient safety incident or event; and (c) any other unique identifying number, characteristic or code except as permitted for re-identification.

PSWP is confidential and should not be disclosed, except that it can be disclosed when permitted above, as well as:

1. For research authorized, funded, certified or otherwise sanctioned by rule or other means by the Secretary of Health and Human Services
2. To the U.S. Food and Drug Administration (FDA) and entities required to report to the FDA
3. In a voluntary disclosure to an accrediting body
4. For business operations to attorneys, accountants and other professionals by the PSO or a provider
5. To law enforcement, if the discloser reasonably believes the PSWP disclosure is necessary for criminal law enforcement
6. For other purposes authorized under 42 CFR §3.206

Direct Identifiers of Participants/Provider Include:

1. Names
2. Postal address information, other than town or city, state, and ZIP code
3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social Security numbers or taxpayer identification numbers
7. Provider or practitioner credentialing or DEA numbers
8. National provider identification numbers
9. Certificate/license numbers
10. Web Universal Resource Locators (URLs)
11. Internet Protocol (IP) address numbers
12. Biometric identifiers, including finger- and voiceprints
13. Full-face photographic images and any comparable images

In cases where a Participant's PSWP is sought by agencies investigating the Participant or its providers, or by litigants in cases where the Participant or its providers are parties, the Participant or its providers maintain primary responsibility for defending against attempts to access the Participant's PSWP. True North PSO will cooperate as necessary to protect the Participant's PSWP. In the event True North PSO receives a request, subpoena, or other attempt of an outside party or agency to access confidential PSWP provided by a Participant, it will assert all applicable privileges and will notify the affected Participants.

b) Receiving PSWP from the PSO

Participants also receive PSWP from True North PSO. True North PSO will send Participants PSWP by a protected exchange processes that will be determined by True North PSO.

V. Ongoing Participation in the PSO

a) Staff trainings

The Participant must train Participant Staff on an annual basis.

b) PSES security evaluations

The Participant should develop a schedule for regularly evaluating the safety and security of the Participant's PSES. This will include monitoring access to the PSES, ensuring firewalls and security measures are successful at limiting access to PSWP by any individuals outside the Participant organization, or within the Participant organization who are not on the PSO team. The Participant should record PSES security evaluations, the results of the evaluation, any potential or actual breaches, and steps taken to correct potential or actual breaches.

Any breaches of the Participant's PSES, and a description of PSWP affected, should be reported to True North PSO within three business days of discovery.

c) Safe Table participation

The PSO will hold periodic Safe Table discussions to serve as a forum for PSO Participants to share patient safety and risk management strategies. If a Participant Staff member wants to attend Safe Table calls or meetings, he or she must first execute a Safe Table Authorization Form in a format substantially similar to the example attached at the end of this manual, and submit this form to True North PSO.

d) Participant contract renewal

A Participant must renew its contract to participant in the PSO according to the terms of the contract.

If you have questions, contact Kristin McOlvin, True North PSO Administrator, at Kmcolvin1@truenorthpso.org.

VI. True North PSO Who's Who

Executive Director
Mark Jarrett, MD, MBA, MS
Mjarrett@truenorthpso.org

Mark Jarrett, MD, is the deputy chief medical officer, senior vice president, and chief quality officer for Northwell Health. He has lead Northwell on a journey to strengthen patient safety efforts and developed strategies aligned with the national healthcare agenda. He is an expert in health care cybersecurity and serves on several national and regional committees focused on how to address threat to IT infrastructure in healthcare. As Executive Director of True North PSO Dr. Jarrett oversees PSO activity and will serve as PSO liaison to the Northwell Health parent entity.

Quality Director
Karen Nelson, RN, MBA, CPHQ
KNelson14@ truenorthpso.org

Karen Nelson, RN, is the deputy chief quality officer for Northwell Health. She leads the Institute for Clinical Excellence and Quality overseeing clinical strategy and development as well as accreditation and regulatory affairs. In addition she teaches science education at the Donald and Barbara Zucker School of Medicine at Hofstra/Northwell and is on the faculty of the Center for Learning Innovations Physician Leadership Development Program. As Quality Director of True North PSO Karen reviews and analyzes the monthly data and creates feedback for each participant with input from any pertinent subject matter experts.

Chief Counsel
Alexandra Trinkoff, Esq.
ATrinkof1@ truenorthpso.org

Alexandra (Alex) Trinkoff is a Vice President in the Office of Legal Affairs for Northwell Health. Alex specializes in all areas of health care law providing counsel to Northwell' s Managed Care and Health Insurance management team, the Office of Academic Affairs and Graduate Medical Education and to the Feinstein Institute for Medical Research on research compliance issues. As Chief Counsel for True North PSO Alex ensures compliance with the Patient Safety Act, addresses any legal concerns and sits on the board of directors.

Administrator
Kristin McOlvin, MS, CPHQ
Kmcolvin1@ truenorthpso.org

Kristin McOlvin is an Assistant Director for Performance Improvement for Northwell Health's Institute for Clinical Excellence and Quality. Her focus is on establishing and overseeing processes for the Northwell core measures abstraction team, interpreting and providing education on various quality measures, and analyzing and displaying data in meaningful ways. She also supports the Behavioral Health Service Line in their performance improvement efforts. As the Administrator of True North PSO Kristin coordinates PSO routine operations including responding to provider inquiries, coordinating provider reporting and managing the reporting process and scheduling and planning Safe Tables.

PSWP CONFIDENTIALITY AGREEMENT

As a condition of being given responsibilities on behalf of _____ ("Participant") related to Participant's role in the True North Patient Safety Organization, Inc. (PSO), a patient safety organization established under the Patient Safety Act, I agree with the following:

1. Definition of PSWP. As used in this Agreement, patient safety work product (PSWP) means any data, reports, records, memoranda, analyses (such as root cause analyses), or written or oral statements which could improve patient safety, healthcare quality or healthcare outcomes and which (i) are assembled or developed by a provider by which I am not employed that is participating in PSO for reporting to PSO and are reported to PSO; or (ii) are developed by PSO for the conduct of patient safety activities; or (iii) identify or constitute the deliberations or analysis of, or identify the fact of reporting pursuant to, a patient safety evaluation system.

2. Confidentiality. I will maintain in confidence and will not disclose, disseminate or use any PSWP belonging to Participant or PSO or compiled for the purpose of reporting to PSO unless such disclosure, dissemination or use is expressly permitted under the Patient Safety Act and Quality Improvement Act of 2005 and its implementing regulations, PSO policies and procedures, or Participant policies and procedures. I agree to exercise reasonable care to protect PSWP as confidential information. This will include compliance with all Participant and PSO security measures, and taking additional personal measures to ensure no PSWP accessible by me can be inappropriately accessed or viewed or is inadvertently disclosed.

3. Access to and use of PSWP. I agree to limit access to and use of PSWP to occasions in which I am accessing and utilizing PSWP for performance of the Participant's PSO-related functions. I will not electively view, copy, disperse, analyze, share or disclose any PSWP outside of official responsibilities on behalf of Participant. Participant employees not involved in PSO will not have access to PSWP, and I acknowledge that I should not share PSWP with other employees at any time, unless expressly authorized to do so. Similarly, I agree not to access PSWP when I am performing functions for Participant that are not related to PSO. I will not use PSWP in, or allow PSWP to influence, my unrelated employment activities.

4. Term of obligations. I agree that my obligations under this Agreement shall continue in effect after termination of my responsibilities for Participant, regardless of the reason or reasons for termination, and whether such termination is voluntary or involuntary on my part.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Safe Table Authorization Form

Information shared by Participants in the True North PSO during Safe Table is considered patient safety work product and is permitted by exceptions to confidentiality requirements of the Patient Safety and Quality Improvement Act of 2005, set forth at 42 C.F.R. § 3.206(b)(3) and (4). PSO Participants present during Safe Table calls or meetings are not required to disclose the identity of their facilities or their agents and employees, and should not disclose the following information of any specific providers or patients as required by 42 C.F.R. § 3.206(b)(4) and (5):

The following direct identifiers of any providers, affiliated organizations, corporate parents, subsidiaries, practice partners, employers or members of the workforce of such providers should not be disclosed:	**The following direct identifiers of a patient or relatives, employers or household members of the patient should not be disclosed:**
1. Names 2. Postal address information, other than town or city, state, and ZIP code 3. Telephone numbers 4. Fax numbers 5. Electronic mail addresses 6. Social Security numbers or taxpayer identification numbers 7. Provider or practitioner credentialing or DEA numbers 8. National provider identification numbers 9. Certificate or license numbers 10. Web Uniform Resource Locators (URLs) 11. Internet Protocol (IP) address 12. Biometric identifiers, including finger- and voiceprints 13. Full-face photographic images or comparable images	1. Names 2. Postal address information, other than town or city, state, and ZIP code 3. Telephone numbers 4. Fax numbers 5. Electronic mail addresses 6. Social Security numbers 7. Medical record numbers 8. Health plan beneficiary numbers 9. Account numbers 10. Certificate or license numbers 11. Vehicle identifier and serial numbers, including license plate numbers 12. Device identifiers and serial numbers 13. Web Uniform Resource Locators (URLs) 14. Internet Protocol (IP) address 15. Biometric identifiers, including finger- and voiceprints 16. Full-face photographic images or comparable images

By signing below, Participant hereby authorizes identification of their facilities or their agents or employees during a Safe Table, as is required for such disclosures by 42 C.F.R. § 3.206(b)(3) and (4). Further, Participant agrees to maintain, and ensure that their agents and employees maintain, the confidentiality of any PSWP that may be disclosed by other PSO Participants during a Safe Table.

Participant Name:	
Liaison Printed Name:	
Liaison Title:	
Signature:	
Date:	