American Pharmacists Association

For Every Pharmacist. For All of Pharmacy.

2021-2022 House of Delegates

Report of the Policy Committee

- ❖ Standard of Care Regulatory Model for State Pharmacy Practice Acts
- ❖ Data Security in Pharmacy Practice
- ❖ Data Use and Access Rights in Pharmacy Practice

Committee Members

Alison Knutson, Chair
Jennifer Adams
Dalton Fabian
Aliyah Horton
Sara McElroy
Dallas Moore
Daniel Robinson
Ryan Waldschmidt
Lorri Walmsley
Suzy Wise

Ex Officio
Missy Skelton Duke, Speaker of the House

2021-22 APhA Policy Committee Report

Standard of Care Regulatory Model for State Pharmacy Practice Acts

The Committee recommends that the Association adopt the following statements:

1. APhA requests that state boards of pharmacy and legislative bodies regulate pharmacy practice using a standard of care regulatory model similar to other health professions' regulatory models, thereby allowing pharmacists to practice at the level consistent with their individual education, training, experience, and practice setting.
   [Refer to Summary of Discussion Items 1-16, and 21]

2. To support implementation of a standard of care regulatory model, APhA reaffirms 2002 policy that encourages states to provide pharmacy boards with the following: (a) adequate resources; (b) independent authority, including autonomy from other agencies; and (c) assistance in meeting their mission to protect the public health and safety of consumers.
   [Refer to Summary of Discussion Items 1-10]

3. APhA encourages NABP as well as state and national pharmacy associations to support and collaborate with state boards of pharmacy in adopting and implementing a standard of care regulatory model.
   [Refer to Summary of Discussion Items 1-10, 17, and 18]

4. APhA and other pharmacy stakeholders should provide educational programs, information, and resources regarding the standard of care regulatory model and its impact on pharmacy practice.
   [Refer to Summary of Discussion Items 1-9 and 19-22]

Summary of Discussion

1. Standard of care is a regulatory model that is defined as the care that would be provided in a similar practice setting by a reasonable and prudent practitioner with similar education, training, and experience. This regulatory model may include standards of practice as defined by other entities. Standard of care is also used by medicine and nursing, and those professions' standard of care regulations were used as models for the Committee's discussions. (1-4)
2. The Committee discussed the definition of bright-line regulatory model and agreed that a bright-line rule (or bright-line test) is a clearly defined rule or standard, composed of objective factors, which leave little or no room for varying interpretation. The purpose of a bright-line rule is to produce predictable and consistent results in its application. The term "bright-line" in this sense generally occurs in a legal context. (1-4)
3. The Committee discussed the application of standard of care regulatory models compared to bright-line regulatory models related to the dispensing process and clinical care. Continuing education requirements are an example of bright-line regulation in which a defined number of hours are required to be completed within a specific timeframe. Additionally, statewide protocols are an example of bright-line regulations. Therapeutic substitution, as an additional example, would be allowed in a standard of care regulatory model, but may be blocked or more difficult to implement within a bright-line regulatory model. An additional example is prescription adaptation, in which pharmacists can make certain changes to prescriptions based on their professional judgment without provider approval, such as extending refills or changing dosage forms (e.g., a pediatric patient cannot swallow a capsule and the pharmacist dispenses an equivalent dose via a liquid formulation). (1-4)
4. The Committee discussed that advantages of a standard of care regulatory model include (1-4)
    a. Utilizing full competence and ability of the health professional
    b. Determined by education, training, and experience.
    c. Recognizes professional heterogeneity
    d. Advances with new education, technology, science, and practice standards
    e. Avoids tying fixed regulations to an entire class of health professional
    f. Avoids lengthy statutory and regulatory changes as practice and health care evolve
5. The Committee discussed and recognized that a standard of care regulatory model does not prevent the usage or development of bright-line regulations. In the medical model, a standard of care regulatory model is used extensively, but still includes pieces of bright-line regulation, such as continuing education requirements. (1-4)
6. The Committee discussed how standard of care regulatory models consider an individual's level of clinical ability by noting that clinical ability is defined based on their level of education, training, experience, and practice setting. Clinical ability determines what level of service that individual should be providing. (1-4)
7. The Committee reviewed the following additional background references when developing statements on this topic (1-4):

a. Adams AJ, Weaver K. Pharmacists' patient care process: A state "scope of practice" perspective. Innov Pharm. 2019;10(2):1–8. DOI: https://doi.org/10.24926/iip.v10i2.1389
b. Adams AJ, Frost T, Weaver K. Pharmacy Regulatory Innovation Index: Benchmarking the regulatory environment in 10 western states. J Am Pharm Assoc. 2021;61(5):e84–e89. DOI: https://doi.org/10.1016/j.japh.2021.05.003
c. Adams AJ. Transitioning pharmacy to "standard of care" regulation: Analyzing how pharmacy regulates relative to medicine and nursing. Res Social Adm Pharm. 2019;15(10):1230–5. DOI: https://doi.org/10.1016/j.sapharm.2018.10.008
d. Cooke BK, Worsham E, Reisfield GM. The elusive standard of care. J Am Acad Psychiatry Law. 2017;45(3):358–64. https://pubmed.ncbi.nlm.nih.gov/28939735/

8. When considering this policy topic, the Committee referenced the work of NABP's Task Force to Develop Regulations Based on Standards of Care, completed in 2018 (https://nabp.pharmacy/wp-content/uploads/2018/12/Task-Force-to-Develop-Regulations-Based-on-Standards-of-Care-December-2018.pdf), and the NABP Model Pharmacy Act/Rules (https://nabp.pharmacy/resources/model-pharmacy-act/). (1-4)
9. The Committee discussed examples of standard of care regulatory models used by other health professions' regulatory boards. For example, nowhere in regulation does it say a surgeon should remove every sponge before closing a patient, but if they do not they could be disciplined based on them harming a patient by not meeting the standard of care. Another example would be that a dermatologist should not perform neurosurgery because it is outside their clinical ability. (1-4)
10. In some states, there are other entities (Board of Medicine, Dept Public Health, etc.) that may play a role in regulating pharmacy, and the Committee discussed the importance for the Board of Pharmacy to have autonomy. The Committee reviewed existing policy statements in **2002 National Framework for Practice Regulation.** Statement 2 specifically calls for states to provide boards of pharmacy with a) adequate resources, (b) independent authority, including autonomy from other agencies, and (c) assistance in meeting their mission to protect the public health and safety of consumers. The Committee noted the importance for boards of pharmacy to have necessary resources to complete the transition to a standard of care regulatory model and felt that reaffirming the existing policy would be the best approach for this topic, as stakeholders would receive this messaging again if the reaffirmation passes in the House. (1,2,3)
11. The Committee discussed the inclusion of both "state boards of pharmacy" and "legislative bodies" within the statement. It was determined that since some states require approval from the legislature to change rules, it would be most appropriate to include both entities within the language. The Committee noted that some states may require a statute change to implement a standard of care regulatory model. (1)
12. The Committee discussed how there is a fine line regarding the inclusion of educational materials in the policy statement and felt it was necessary to explain, in part, what a standard of care regulatory model is within the statement because many pharmacists and regulators are not yet aware of this type of model. (1)

13. The Committee discussed how there will potentially be some concern surrounding liability for malpractice within a standard of care model, as current regulatory models have bright-line language describing exactly what discipline will occur and for which violations. The Committee agreed that if pharmacists desire enhanced practice opportunities, then pharmacists would need to assume some level of liability. As pharmacist are pursuing recognition as a provider within the Social Security Act, pharmacists need to be prepared to accept accountability for the care they provide and its related outcomes. (1)
14. The Committee discussed potential inclusion of language acknowledging "professional judgment" within the policy statements. The Committee determined that an individual's professional judgment is influenced by their education, training, experience, and practice setting, and opted to leave "professional judgment" out of the language. (1)
15. The Committee agreed that when discussing "pharmacy practice" in statement 1, this would apply to clinical care delivery, dispensing, and facilities. (1)
16. The Committee considered multiple options for the action verb in the first policy statement. "Advocates" was initially used, but the Committee wanted to use a stronger, more actionable word than "advocates" or "encourages." The Committee ultimately determined that "requests" fulfilled these qualifications. (1)
17. The Committee discussed how not all state governments operate the same. Some states would need statutory modifications for the implementation of a standard of care regulatory model, which would need additional engagement from other stakeholders beyond just the board of pharmacy for proper implementation. (3)
18. The Committee considered the different roles of NABP, national pharmacy associations, state boards of pharmacy, and state pharmacy associations when advocating for, enacting, and implementing new regulatory models. The Committee agreed that a collaborative approach is the best way to increase the likelihood of adoption and streamlined implementation. The Committee acknowledged that state boards of pharmacy will be critical for implementation of regulatory model changes and focused the statement to have support and collaboration from NABP and state pharmacy associations. (3)
19. The Committee discussed the need for continuous education efforts to advance standard of care and collaboration on implementation so pharmacists understand what they legally can and cannot do and how they approach care in a practice setting. (4)
20. The stakeholders intended within statement 4 include but are not limited to schools and colleges of pharmacy, state and national pharmacy associations, boards of pharmacy, legislators, employers, and pharmacy managers, etc. (4)
21. The Committee intends for APhA, in collaboration with other stakeholders, to create and make available a Continuing Pharmacy Education course describing what a standard of care regulatory model is, how it applies to various practice settings, and what it means for individual pharmacy practitioners. (1,4)
22. The Committee acknowledged the unconventional structure of statement 4, and feels the statement is appropriate as written to convey the necessary collaboration. (4)

2021–22 APhA Policy Committee Report

Data Security in Pharmacy Practice

The Committee recommends that the Association adopt the following statements:

1. APhA advocates that all organizations and healthcare providers adopt best practices in data security to ensure ongoing protection of patient data from loss, alteration, and all forms of cybercrime.
   [Refer to Summary of Discussion Items 1-7]

2. APhA recommends that organizations understand the flow of information, both internally and externally, to apply and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy and identity of their patients.
   [Refer to Summary of Discussion Items 1-3, and 5-8]

3. APhA calls on organizations to provide ongoing employee education and training regarding patient data protection, best practices, and cybersecurity standards.
   [Refer to Summary of Discussion Items 1-3, 5, 6, and 9]

Summary of Discussion

1. This topic was separated out from the original proposed policy topic, "Data Ownership Rights and Responsibility of Pharmacists and Pharmacy Practices to Secure Data." The Committee discussed how the intent of the original policy topic was focused on patient data to address issues on electronic data use/access and data security. After much discussion, the Committee acknowledged that to best address specific issues captured through open-forum webinars and from members, it would be best to separate these issues into 2 distinct policy topics. (1-3)
2. The Committee referenced general cybersecurity best practice recommendations from the Healthcare Information and Management Systems Society (HIMSS), https://www.himss.org/resources/cybersecurity-healthcare. (1-3)
3. The Committee focused these statements on the security of electronic data—as opposed to physical records such as prescription records or paper medical charts—because existing APhA policy already cover security of physical property at a pharmacy site. Existing APhA policies **2010 Personal Health Records** and **1971 Prescription Department Security** relate to the physical security of pharmacy departments or physical health records located within a pharmacy, and therefore the Committee decided not to develop a new policy topic focused on physical security of pharmacy records. Statement 2 does include the terminology of "physical safeguards" as it relates to the security of electronic storage of data (e.g., stolen laptop). (1-3)
4. The Committee considered different terminology related to cyber-related activities. The Committee agreed that cybercrime was the broadest term that includes cyberattack and cybercrime and used this to capture broader cyber related activities. (1)
5. When the term "patient data" is used in the proposed statements, the Committee's intent was that it included protected health information (PHI) and personally identifiable information (PII). (1-3)
6. Within these statements the Committee refers to "organization." The Committee intends for this to cover any organization which provide care to patients, including pharmacies and other healthcare sites that may or may not be an entity covered by HIPAA. (1-3)
7. The Committee discussed the concept of least-privilege access in relation to administrative, technical, and physical safeguards and protection from cybercrime. Least-privilege access refers to a process that limits the number of users who have access to data and the length of time for access to data, monitors how users access data, and tracks how users can modify or edit data. The intent is to carefully delegate access rights in order to reduce unnecessary levels of access to patient data. The Committee referenced content provided by the Cybersecurity & Infrastructure Security Agenda (CISA), https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege. Additionally, the Committee agreed that organizations should adopt policies and procedures to secure data as part of their administrative safeguards. (1,2)
8. An additional safeguard discussed by the Committee was the concept of attack-surface minimization to lessen the vulnerability of an attack and minimize risk of cybersecurity vulnerabilities. Attack-surface minimization may consist of not giving wireless printing access to computers that do not need access. (2)

9. The Committee considered various definitions for cybersecurity and referenced the National Institute of Standards and Technology's definition, which is "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." (https://csrc.nist.gov/glossary/term/cybersecurity) (3)

2021–22 APhA Policy Committee Report

Data Use and Access Rights in Pharmacy Practice

The Committee recommends that the Association adopt the following statements:

1. APhA supports an organization's and patient care provider's rights to use patient data for improvement of patient outcomes and enhancement of patient care delivery processes in accordance with ethical practices and industry standards regarding data privacy and transparency.
   [Refer to Summary of Discussion Items 1-3, and 8]

2. APhA urges ongoing transparent, accessible, and comprehensible disclosure to patients by all HIPAA-covered and non-covered entities as to how personally identifiable information may be utilized.
   [Refer to Summary of Discussion Items 1, 2, and 4-8]

3. APhA calls for all entities with access to patient health data, including those with digital applications, to be required to adhere to established standards for patient data use.
   [Refer to Summary of Discussion Items 1, 2, and 8-10]

4. APhA supports the right of patients to have timely access to their personal health data from all entities.
   [Refer to Summary of Discussion Items 1, 2, and 10-12]

Summary of Discussion

1. This topic was separated out from the original proposed policy topic, "Data Ownership Rights and Responsibility of Pharmacists and Pharmacy Practices to Secure Data". The Committee discussed how the intent of the original policy topic was focused on patient data to address issues on electronic data use/access and data security. After much discussion, the Committee acknowledged that to best address specific issues captured through open-forum webinars and from members, it would be best to separate these issues into 2 distinct policy topics. (1-4)
2. The Committee considered including a statement that discussed patients' ability to opt-in or opt-out of policies related to the use of personally identifiable health information, and ultimately decided to exclude such a statement. (1-4)
3. The Committee was intentional in not including the word "ownership" within policy statement 1, noting that it can be a nuanced term. (1)
4. The Committee specifically used the term "personally identified information (PII)," as this was broader than protected health information (PHI). Some forms of PII could be used to gain access to an individual's personal health records or PHI, and as such the Committee wanted to ensure the statement covered situations like this. (2)
5. The Committee reviewed existing policy statements in **1996 Confidentiality of Patient Data**. The Committee noted some overlap in subject matter but sought to address the need for non-covered entities to adhere to personal health data protection standards and determined that an additional policy statement is necessary to fully cover this intention. (2)
6. The Committee discussed the application of informed consent, using examples of patients with disabilities which make it impossible to read through and comprehend disclosure documents, and noted that the purpose of informed consent is to ensure the individual clearly understands what they are consenting to. (2)
7. The Committee additionally discussed that the intention of statement 2 is to ensure notification of disclosure of data use is conducted similarly to receiving informed consent, and determined that the terms "transparent, accessible, and comprehensible" fulfilled this intention. (2)
8. The Committee discussed examples of when patient data is given to HIPAA non-covered entities, such as when a patient signs up for GoodRx, health and wellness apps, ancestry.com, etc. (1,2,3)
9. The Committee discussed multiple aspects of HIPAA as established standards for patient data use, including what classifies as personal identifiable information (PII) and who is and is not included as a covered entity. The Committee intended to not duplicate what already exists in federal law related to these concepts within the policy statements. (3)
10. The Committee noted that the language "all entities" in statements 3 and 4 is intended to capture any entity, regardless of if they are included within HIPAA. According to HHS, "Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information" Furthermore, covered entities are defined in the HIPAA rules as "(1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted

standards." The Committee intends to capture any entity that interfaces with a pharmacy or pharmacy practice. (3, 4)

11. The Committee referenced the 21st Century Cures Act: "Beginning April 5, 2021, the program rule on Interoperability, Information Blocking, and ONC Health IT Certification, which implements the 21st Century Cures Act, requires that healthcare providers give patients access without charge to all the health information in their electronic medical records without delay." A critical purpose of statement 4 is to ensure that patients also have access to their data from entities that are not encompassed within the 21st Century Cures Act. (4)
12. The Committee also referenced how HIPAA cites the timeliness of providing access to patient information within 30 days. The Committee noted that patients should request access to patient information through proper methods and that sometimes "timely access" cannot be an instant process. The citation below from HHS notes some instances through usage of health information technology that may speed up this process. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (4)
    a. Timeliness in Providing Access
    "In providing access to the individual, a covered entity must provide access to the PHI requested, in whole, or in part (if certain access may be denied as explained below), no later than 30 calendar days from receiving the individual's request. See 45 CFR 164.524(b)(2). **The 30 calendar days is an outer limit and covered entities are encouraged to respond as soon as possible.** Indeed, a covered entity may have the capacity to provide individuals with almost instantaneous or very prompt electronic access to the PHI requested through personal health records, web portals, or similar electronic means. Further, individuals may reasonably expect a covered entity to be able to respond in a much faster timeframe when the covered entity is using health information technology in its day-to-day operations."