American Pharmacists Association

For Every Pharmacist. For All of Pharmacy.

2023-2024 House of Delegates

Report of the Policy Committee

- ❖ Artificial Intelligence Use in Pharmacy Practice
- ❖ Cybersecurity in Pharmacy

Committee Members

Mary Klein, Chair
Samm Anderegg
Timothy Aungst
Dalton Fabian
Olivia Gabrick
Neelam "Nelly" Gazarian
Mary Gurney
Christopher Harlow
Cory Holland
Brian Hose
Sarah McBane

Ex Officio
Brandi Hamilton, Speaker of the House

2023-2024 APhA Policy Committee Report
Artificial Intelligence Use in Pharmacy Practice

The Committee recommends that the Association adopt the following statements:

1. APhA opposes use of artificial intelligence in place of the pharmacist's professional judgment or access to a pharmacist.
   (Refer to Summary of Discussion items: 1-21)

2. APhA calls on the profession of pharmacy and all related organizations to proactively assess and respond to the evolving role of artificial intelligence in pharmacy practice and workforce dynamics.
   (Refer to Summary of Discussion items: 1-16, 22-24)

3. APhA encourages judicious use of artificial intelligence by pharmacists and pharmacy personnel as a tool to elevate pharmacy practice and enhance patient care. (Refer to Summary of Discussion items: 1-16, 25-31)

4. APhA advocates for the integration of pharmacists into the development, design, validation, implementation, and maintenance of artificial intelligence solutions.
   (Refer to Summary of Discussion items: 1-16, 32-40)

5. APhA calls on regulatory bodies, employers, and other relevant parties to develop policies, procedures, and applicable rules for artificial intelligence to ensure patient safety, privacy, public awareness, and public protection.
   (Refer to Summary of Discussion items: 1-16, 41-48)

6. APhA calls on those providing artificial intelligence solutions to implement processes that identify and mitigate bias and misinformation in artificial intelligence.
   (Refer to Summary of Discussion items: 1-16, 49-53)

7. APhA advocates for education providers to facilitate education and training on trustworthy artificial intelligence and its lawful, ethical, and clinical use.
   (Refer to Summary of Discussion items: 1-16, 31, 54-62)

8. APhA calls on pharmacists and pharmacy personnel to seek out education and training on trustworthy artificial intelligence and its lawful, ethical, and clinical use.
   (Refer to Summary of Discussion items: 1-16, 54-62)

Summary of Discussion

Artificial Intelligence Use in Pharmacy Practice

1. The committee broadly defined artificial intelligence (AI) as a branch of computer science that deals with problem-solving with the aid of symbolic programming, and a machine's ability to perform cognitive functions associated with human minds. This definition reflects established definitions and studies from researchers of leading institutions such as Stanford University and Cambridge University. The committee discussed large language models as a type of AI potentially used by pharmacies. (1-8)
2. Following the creation of draft proposed statements, the committee referenced generative artificial intelligence programs to explore their crafted language. (1-8)
3. In addition to the proposed policy statements, topics such as academic implications, liability, and pharmaceutical industry implications were mentioned during APhA Open Forum webinars and committee discussions. The committee opted to focus the scope of these proposed policy statements on the use of AI and engagement of pharmacists for the purposes of this policy. (1-8)
4. The overarching intent of the committee when developing these proposed policy statements is to take a proactive approach to ensure AI is effectively utilized to support pharmacy practice in an ethical manner, as opposed to being reactionary. (1-8)
5. Furthermore, from a scope perspective, the committee acknowledged the expectation that given rapid evolution of artificial intelligence technology developments, policies proposed at this time will likely be foundational policy to be further reviewed and updated by future committees. (1-8)
6. The committee discussed the order of the statements to highlight the importance of APhA's stance on the appropriate use of AI. (1-8)
7. The committee worked to arrange statements from broadest to narrowest, following a similar structure as cybersecurity. In doing so, the committee opted to lead this collection of policy statements with the strong statement of opposition against pharmacists being replaced by artificial intelligence. (1-8)
8. The general order was negative / strong statement, positive statement, call to action, then education pieces. (1-8)
9. As part of the review of existing policy gaps, the committee reviewed the following relevant APhA policies, noting that topics pertaining to (1-8):
    a. 2022 - Standard of Care Regulatory Model for State Pharmacy Practice Acts ((JAPhA. 62(4):941; July 2022)
    b. 2022 - Pharmacists' Application of Professional Judgment (JAPhA. 62(4):942; July 2022)
    c. 2020 Digital Health Integration in Pharmacy (JAPhA. 60(5):e11; September/October 2020)
    d. 2004 - Automation and Technology in Pharmacy Practice (JAPhA. NS44(5):551; September/October 2004) (Reviewed 2006) (Reviewed 2008) (Reviewed 2013) (Reviewed 2014) (Reviewed 2015) (Reviewed 2019)
    e. 1998 Access and Contribution to Health Records (JAPhA. 38(4):417; July/August 1998) (Reviewed 2005) (Reviewed 2009) (Reviewed 2010) (Reviewed 2013) (Reviewed 2014) (Reviewed 2015)

f. 1991 - Pharmaceutical Care and the Provision of Cognitive Services with Technologies (Am Pharm. NS32(6):515; June 1991) (Reviewed 2001) (Reviewed 2007) (Reviewed 2009) (Reviewed 2013) (Reviewed 2014) (Reviewed 2019)
g. 1991 - Emerging Technologies (Am Pharm. NS31(6):28; June 1991) (Reviewed 2004) (Reviewed 2009) (Reviewed 2014) (Reviewed 2019)
h. 1991 - Biotechnology (Am Pharm. NS31(6):29; June 1991) (Reviewed 2004) (Reviewed 2007) (Reviewed 2010) (Reviewed 2015) (Reviewed 2016) (Reviewed 2017)

10. The committee discussed ethical and equitable access to artificial intelligence patient care. However, concern was raised against inclusion of a statement to mandate utilization of AI in all delivery systems, and therefore the committee opted not to move forward with that direction at this time. (1-8)
11. The committee addressed the necessity of creating a statement of informed consent although language already exists in other government entity guidance documents. (1-8)
12. The committee reflected on an overarching workforce concern that artificial intelligence may potentially assume certain pharmacist tasks (such as prescription verification), and lead to less job security. (1-8)
13. The committee opposes AI use that would eliminate the role of the pharmacist and emphasized the importance of directly stating concerns of potential elimination of a pharmacist's clinical role through legislation or other governing bodies. Similarly, the committee was intentional to highlight pharmacists' professional judgement. (1)
14. The committee discussed whether to focus on the impact on pharmacy practice or impact on pharmacy workforce dynamics. The committee ultimately opted to focus on impacts on workforce dynamics, as it is more narrowly focuses on the impact that artificial intelligence can have on pharmacist job outlook. (1-8)
15. The committee referred to a variety of resources to inform the development of proposed policy statements, including content and concepts featured in the Washington Post's October 2023 summit, "The Futurist Summit: The Rise of AI", featuring influential policy-makers and innovative leaders shaping the future of AI. (1-8)
16. The committee noted that proposed statements aligned with current pharmacy practice literature, such as "Role of artificial intelligence in pharmacy practice: a narrative review" by authors Wong, Palisano, Elsamadisi, and Badawi, published in Journal of the American College of Clinical Pharmacology. (1-8)
17. The committee considered developing a single statement which conveyed support for certain elements of AI use and opposition of others. However, the committee was intentional to separate these points into two statements, to strengthen both statements by their own merit. (1,3)
18. The committee discussed if APhA should oppose AI in place of professional judgement entirely, or more specifically the opposition to use of AI in place of professional judgment. Ultimately from a spirit of innovation and forward-thinking, the committee supports AI use as part of pharmacy practice, so long as it does not replace the professional judgement of a pharmacist. (1)
19. The committee considered including "pharmacist's services" in addition to "professional judgment"; however, the committee wanted to ensure that pharmacist professional judgement is being used regardless of setting and the type of service being provided. (1)

20. The committee discussed liability concerns should AI make a medication error, noting the connection to informed patient consent when AI is being used. (1)
21. The committee discussed amending statement #1 to include "or access to" to avoid patients having limited access to a pharmacist. Considerations were made to include "pharmacy personnel" within this leading statement as well, however were ultimately opted against to specify expertise, role and responsibility of the pharmacist. (1)
22. When discussing the potential role of artificial intelligence in pharmacy practice, the committee reflected on the impacts of prior technological advancements on the pharmacy profession and workforce – such as printing and automated medication dispensing. (2)
23. The committee emphasized the necessity of a forward-thinking approach to artificial intelligence by the pharmacy profession, which encourages both proactive assessment and implementation of artificial intelligence use in pharmacy practice. In doing so, the committee was intentional to utilize language around the "evolving role of artificial intelligence", as opposed to language such as "impact of artificial intelligence", which may have a more reactionary connotation. (2)
24. The committee discussed the concept of pharmacy working groups that can be charged with reviewing research and potential solutions involving AI and the role of a pharmacist. The committee determined this recommendation was better suited as a consideration for potential implementation of artificial intelligence policy. (2)
25. The committee encourages "judicious use" of artificial intelligence, to convey the appropriate balance of consideration and precaution, while still embracing opportunities for implementation. Other adjectives such as "cautious" were considered, but opted against, because of negative and less proactive connotations. (3)
26. When discussing how AI may be used to support pharmacy practice, the committee recommended language to indicate that AI may be used "as a tool" to improve patient care. An intentional distinction was made not to include such a qualifier such in the leading opposition statement (1), so that *any* use of AI to replace pharmacist judgment was covered in the statement's opposition. (3)
27. When discussing the development and application of emerging artificial intelligence, the committee referred to existing policy, 1991 Emerging Technologies, to reaffirm the forward-thinking inclusion of pharmacists in development and application of the emerging AI technologies in the delivery of pharmaceutical care. (3)
28. The committee considered multiple verbs such as enhance, expand, and improve when describing how the practice of pharmacy may be affected by artificial intelligence use in pharmacy practice. The committee opted against "improve" or "expand", which could inadvertently imply current practices are not functional. Ultimately the committee recommended "elevate" in the spirit of aspirational language, which also captures expansion. (3)
29. The committee considered noting "scope of practice" among pharmacy practice and patient care when listing areas where AI may be applied. However, the committee opted against it in this context, as scope of practice is continually evolving and varying from state to state. (3)
30. When describing who should be using AI judiciously, the committee considered pharmacy personnel or pharmacy workforce. The committee opted for "by pharmacists and pharmacy personnel" to include all professionals in the pharmacy workforce. The

committee defines “pharmacy personnel” to include all individuals including pharmacy clerks and other non-clinical administrative roles, recognizing this definition may vary by state. (3)

31. The committee discussed the merits of “supporting” or “recommending” judicious use of AI. The committee decided that “encourages” is all-encompassing, and is a better verb to further prompt and promote pharmacy personnel to utilize AI technologies (3)
32. The committee referenced the White House Blueprint for an AI Bill of Rights in doing so. The committee decided that pharmacists should be included in the conversation and the construction of these rights. (4)
33. The committee referred to existing policy from the American Medical Association (AMA) relating to physician involvement with AI, which states that the AMA will “identify opportunities to integrate the perspective of practicing physicians into the development, design, validation and implementation of health care AI.” The committee discussed adding a statement advocating for the integration of pharmacists in the “validation of AI models”, to be consistent. (4)
34. The committee suggested APhA should advocate for pharmacist integration into AI use, as they currently may not be incorporated as extensively into artificial health intelligence. The committee raised concerns of other healthcare professionals opting to use AI tools in place of pharmacist’s services, such as patient counseling, hence emphasizing the necessity of integrating pharmacist into the development and design. (4)
35. The committee discussed that language to integrate pharmacists within AI technologies also conveys that pharmacists are innovators in development, design, validation and implementation of AI technologies. (4)
36. The committee discussed specifying “ethical use” of educational and training opportunities in its proposed language, to incorporate the concern of clinical decision-making AI replacing pharmacists. The term “its ethical use” also implies the necessity of informed consent so as not to blindside patients with the use of AI for a patient’s care. The committee discussed concepts of patient-informed consent and data use transparency, contemplating patients' potential satisfaction or dissatisfaction in utilizing artificial intelligence technology. (4,7,8)
37. The committee discussed the need for differentiation when a patient is speaking with an AI chatbot vs. a pharmacist, to ensure that patients have awareness of who they are talking to and that they can opt in or out of using talking to AI. (4)
38. The committee raised the question of what data is used to input and build artificial intelligence databases, and considerations of informed consent in this data use. (4,5)
39. The committee discussed the use of the terms “AI solutions”, “AI models”, and “AI technologies” and determined the use of “AI” is inclusive of all components of the AI lifecycle. However, the committee decided “AI solutions” serves as a final product after development and therefore was retained. (4,6)
40. The committee discussed whether to explicitly specify pharmacists' role in integrating AI into standards of care, anticipating that AI will eventually be integrated into pharmacy standards of care. Ultimately the committee opted to not include that piece, citing existing APhA policy (2020 Digital Health Integration in Pharmacy and 2022 Standard of Care Regulatory Model for State Pharmacy Practice Acts that already cover the intent of this suggestion. (4)

41. The committee discussed the use of "regulatory bodies, employers, and other relevant stakeholders" to be all-encompassing of the bodies that will develop the policies and procedures for AI. It would also include pharmacists and their involvement with development. It was discussed that "NABP" would be too specific and wouldn't necessarily encompass everything we would like stakeholders to do. (5)
42. Concepts of patient informed consent were considered and discussed in developing these statements. The committee considered explicit mention of it in a statement, however concluded that "informed consent" is encompassed by calling for public awareness and protection. The committee also recognized that principles of private patient data are covered by existing 1998 Access and Contribution to Health Records, which states "APhA supports public policies that protect the patient's privacy yet preserve access to personal health data for research when the patient has consented to such research or when the patient's identity is protected." (5)
43. The committee raised concerns of using patient data in AI, however the statement aims to address that APhA supports the transparency of the use. (5)
44. The committee discussed entities that AI implementation could affect such as medical device organizations, pharmaceutical companies, pharmacies, or regulatory bodies. (5,6)
45. The committee intentionally opted against referring to relevant parties providing artificial intelligence solutions as "stakeholders", to align with the overarching movement away from such a term, which may imply a power differential between groups and have stigmatizing connotations. (5)
46. The committee's intention was to be as broad as possible to encompass all partnerships involved in developing policies, procedures and applicable. (5)
47. The committee considered whether there is merit in addressing a subset of artificial intelligence called machine learning (ML) explicitly in the policy statement. However, the committee opted against this, as this subset is already captured by the broader term of AI. (5)
48. The committee referenced the National Institute of Health's definition of what is or is not considered PHI in AI technology. 1) De-identified health information, as described in the Privacy Rule, is not PHI, and thus is not protected by the Privacy Rule. 2) PHI may be used and disclosed for research with an individual's written permission in the form of an Authorization. 3) PHI may be used and disclosed for research without an Authorization in limited circumstances: Under a waiver of the Authorization requirement, as a limited data set with a data use agreement, preparatory to research, and for research on decedents' information. (5)
49. When discussing the policy language for bias, the committee utilized the American Academy of Family Physician's policy on Ethical Application of AI, which states that companies providing AI/ML solutions must address implicit bias in their design. We understand implicit bias cannot always be completely eliminated. Still, the company should have standard processes in place to identify implicit bias and to mitigate the AI/ML models from learning those same biases. In addition, when applicable, companies should have processes for monitoring for differential outcomes, particularly those that affect vulnerable patient populations." (6)
50. The committee noted potential biases and implications to principles of diversity, equity, inclusion, and belonging – particularly as it relates to algorithmic bias. (6)

51. When discussing parties which provide AI solutions, the committee deliberated whether to refer to these as "companies" or "entities". While "entities" may be more all-encompassing, the use of the term "companies" puts the responsibility on those that use and produce the AI. The committee decided to change "companies" to call on "those providing AI" to encompass individuals outside of companies who may develop AI tools. (6)
52. The committee recognizes bias in data sets, and therefore calls on those providing AI solutions to implement processes that identify and mitigate bias in AI models. They considered whether it would be necessary to explicitly recognize these biases in the statement itself, however determined that this is implied by calling on parties to mitigate bias. Furthermore, while the committee discussed both implicit and explicit bias the use of "bias" alone encompasses all forms. (6)
53. The committee discussed the use of "training data" vs. "data sets" vs. "all data sets"; In their discussions, the committee defined data sets as requiring training, testing, and validation. The committee discussed having a diverse data set and capturing the diversity of patient populations when addressing bias therefore "increase diversity" was included. However, by acknowledging that bias exists, the committee ultimately decided that this was not necessary to include. (6)
54. The committee recognizes the existence of both trustworthy and non-trustworthy artificial intelligence, and the importance of distinguishing the two. The committee defines "trustworthy artificial intelligence" according to the Trade and Technology Council (TTC)'s definition, which notes that Trustworthy AI has three components: (1) it should be lawful, ensuring compliance with all applicable laws and regulations (2) it should be ethical, demonstrating respect for, and ensure adherence to, ethical principles and values and (3) it should be robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm. Global principles have not been established, and the use of "principles" in the statement was intended to keep the policy evergreen.(7,8)
55. By defining trustworthy artificial intelligence, the committee discussed when it would be appropriate to specify "trustworthy" artificial intelligence among the proposed statements. The committee opted to specify trustworthiness when advocating for which forms to include in effective education or implantation of artificial intelligence solutions. (7,8)
56. The committee referenced the GAO global report, which spotlights public health concerns and AI practices within health care. These cover clinical applications such as supporting population health management, monitoring patients, guiding surgical care, predicting health trajectories and administrative applications such as automating laborious tasks, recording digital clinical notes, and optimizing operational processes. This report supports the committee's intention to advocate for training around clinical use. (7,8)
57. The committee considered creating a single statement encompassing learner-driven and provider-driven education pertaining to trustworthy artificial intelligence. However, the committee ultimately decided to create two statements (one focused on learners and one focused on providers) to note their distinctions. (7,8)

58. The committee discussed appropriate subject-verbs to be consistent with the cybersecurity statement, when considering "integrate principles of trustworthy artificial intelligence and its ethical use into education and training programs". The committee then opted for the verb facilitate (7)
59. The committee discussed that use of both "ethical use" and "trustworthy" may be redundant, as the Trade and Technology Council definition of trustworthy artificial intelligence includes ethics as criteria. (7)
60. The committee discussed the need to include "education providers" and development of education and training, from the question of whether this pushes the profession ahead or retreats to being more passive. The use of "education providers" aims to encompass not only those who provide education in academia but includes organizations who may provide continuing education. (7)
61. The committee discussed the inclusion of "lawful, ethical, and clinical use" to encompass all aspects relating to the development and use of AI. There was further discussion on what happens after the product has been built and ensuring that once it is implemented, anyone using the technology is using it appropriately. (7,8)
62. The committee discussed whether the policy statements shall call on pharmacists and pharmacy personnel to educate themselves, in addition to calling on education bodies, to take a less passive approach. The committee noted responsibility should be upon the learner to seek out the knowledge to understand and apply the AI tools recognizing that there is not much training available at this time of its use in health care. (7,8)
    The committee discussed the merits of including pharmacists, interns, and technicians as individuals needing to seek out education and training. (8)

2023–2024 APhA Policy Committee Report
Cybersecurity in Pharmacy

The Committee recommends that the Association adopt the following statements:

1. APhA advocates for implementation and maintenance of cybersecurity systems, safeguards, and response mechanisms to mitigate risk and minimize harm or disruption for all pharmacies and related parties who manage or access electronic health and business information.
   (Refer to Summary of Discussion items: 1-15)

2. APhA advocates for all pharmacies and related business entities responsible for electronic health and business information to have cyber liability insurance or an equivalent self-funded plan to protect all relevant parties in the event of a cyberattack and data breach.
   (Refer to Summary of Discussion items: 1-6, 13-20)

3. APhA advocates for education providers to integrate cybersecurity laws, regulations, and best practices on protection of electronic health and business information into their education and training programs.
   (Refer to Summary of Discussion items: 1-6, 13, 20-26)

4. APhA calls for the pharmacy workforce to seek out education and training on cybersecurity laws, regulations, and best practices on protection of electronic health and business information.
   (Refer to Summary of Discussion items: 1-6, 26)

Summary of Discussion

Cybersecurity in Pharmacy

1. The committee broadly defined cybersecurity as referring to measures taken to protect a computer or computer system against unauthorized access or attack, based on relevant authorities on the subject such as the CURES Act. (1-4)
2. As part of the review of existing policy gaps, the committee reviewed the following relevant policies (1-4):
    a. 2022 - Data Security in Pharmacy Practice (JAPhA. 62(4):941; July 2022)
    b. 2022 - Data Use and Access Rights in Pharmacy Practice (JAPhA. 62(4):941; July 2022)
    c. 2010 - Personal Health Records (JAPhA. NS40(4):471; July/August 2010) (Reviewed 2013) (Reviewed 2014) (Reviewed 2015) (Reviewed 2019)
    d. 2005, 2004, 1999 - Telemedicine/Telehealth/Telepharmacy (JAPhA. 39(4):447; July/August 1999) (JAPhA. NS44(5):551; September/October 2004) (JAPhA. NS45(5):559; September/October 2005) (Reviewed 2009) (Reviewed 2012) (Reviewed 2014) (Reviewed 2019)
    e. 2004 - Automation and Technology in Pharmacy Practice (JAPhA. NS41(5)(suppl 1):S8; September/October 2001) (Reviewed 2004) (Reviewed 2007) (Reviewed 2008) (Reviewed 2013) (Reviewed 2015)
3. The committee reviewed the following additional background references when developing statements on this topic:
    a. Defining EHI and the Designated Record Set in an Electronic World. American Medical Informatics Association; Electronic Health Record Association, American Health Information Management Association. https://www.ahima.org/media/ztqh1h2q/final-ehi-task-force-report.pdf 2021
    b. ONC's CURES Act Final Rule. The Office of the National Coordinator for Health Information Technology. https://www.healthit.gov/topic/oncs-cures-act-final-rule August 2022
    c. Health IT Regulation Resources. The Office of the National Coordinator for Health Information Technology. https://www.healthit.gov/topic/laws-regulation-and-policy/health-it-regulation-resources September 2023.
    d. FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy. The White House Office of the National Cyber Director. https://www.whitehouse.gov/oncd/ March 2023 (1-4)
4. When describing relevant data in this policy, the committee utilizes the terminology "data record set", which is derived by the 21st Century CURES Act. This terminology encompasses personal health information, medical records, billing records, insurance information, and information used in case management. (1-4)
5. The committee considered cybersecurity implications of the drug supply chain and upcoming implementation of the Drug Supply Chain Security Act (DSCSA) (https://www.pharmacytimes.com/view/fda-announces-delayed-enforcement-of-dscsa-to-2024) on pharmacies and wholesalers in November 2024.

The committee also acknowledged that all relevant entities are making efforts to fully implement DSCSA by the November 2024 deadline and therefore, reaffirming DSCSA standards or development of a specific proposed statements on this subject is not necessary at this time. (1-4)

6. When discussing the topics overall, the committee considered pharmacists and pharmacy personnel in diverse practice settings, such as the community pharmacy setting, health systems, and consultants, who may have access to relevant data record sets. (1-4)
7. The committee introduced the term "threat assessment" to address the recent hacks on health care and hospital systems. The committee considered using "continuous threat assessment" to ensure that entities are conducting these processes not only when an attack occurs but using a more proactive approach. The committee shared thoughts that threat assessments could be included in disaster plans but debated whether or not they should be explicitly stated in the statement. The committee suggested the use of "threat assessment" vs. "action plan". Ultimately, this language was replaced with cybersecurity systems and safeguards. (1)
8. The committee considered using "cybersecurity framework" when describing appropriate safeguards and ultimately used the phrase "cybersecurity systems and safeguards" to encompass system backups, threat or continuous threat assessments, and disaster plans/incident responses. The committee discussed changing "cybersecurity disaster plan" to "cybersecurity incident response" to better capture that the "plan" addresses recovery and response to an attack; whereas "incidence response" refers to an attack that has already happened. This is the language used by CISA. The committee discussed incorporating "(e.g., incident response plans)" into the statement in such a way to be both proactive (maintaining and implementing systems and safeguards) and reactive (having a response plan). (1)
9. The committee initially considered if it was necessary to specify whether safeguards for mitigating risk apply only to "patients". The term patients were removed to ensure all persons who may be harmed or experience disruption by a cybersecurity attack are not overlooked. (1)
10. The committee agreed that the verbiage to "advocate" is most appropriate given that there are laws and regulations that already require pharmacies and business entities to develop these systems and safeguards. (1)
11. The committee discussed using the terms establishment, development, adoption, maintenance, or implementation when describing the use of cybersecurity systems, and ultimately decided that the term implementation covers both the terms development and adoption of cybersecurity systems. The retention of maintenance is essential to ensure that these systems are still reviewed consistently. (1)
12. The committee discussed the necessity of using the term "appropriate" and noted that its inclusion could eliminate concerns of implementing inappropriate cybersecurity systems but was ultimately unnecessary. (1) The committee discussed the need to include both harm and disruption, or if these two words addressed the same thing. It was decided that

disruption does *not* equate to harm. Disruption *can* be harmful but is not always harmful. (1)

13. The committee opted for the verb "advocates" as opposed to "encourages" for these statements. This implies that APhA holds these statements to the same importance. "Advocates" is listed as a strong verb and "encourages" is a medium verb. (1,2,3)
14. The committee originally discussed using the term "stakeholders" and agreed to recommend usage of "all relevant parties" because stakeholders can be a stigmatizing term for some communities. The term "stakeholder" may imply a power differential between groups and could imply a violent connotation for some tribes and tribal members. The two words were deemed interchangeable in intent. (1, 2)
15. The committee used the term "related business entities" to encompass any entity that could have access to data record sets. (1,2)
16. The committee questioned the difference between cyber liability insurance and equivalent self-funded plan. It was explained that some companies may not have a specific liability insurance policy, and just have the funds or means to cover a data breach event. The committee decided to leave in both terms. (2)
17. The committee discussed what insurance plans cover to protect patients; an example was given where liability insurance plans can provide credit monitoring systems to protect patients who are potentially impacted by a data breach. (2)
18. The committee discussed the need to include any other groups/individuals that could be affected by data breaches. The committee decided to be all-expansive and say "all relevant stakeholders" rather than "patients" to encompass any person or persons that could be protected by insurance/self-funded plans. (2)
19. The committee discussed the correct verbiage to use for the relationship between "pharmacies and relevant business entities" and "cyber liability insurance and equivalent self-funded plans". The committee recommended a word change from "utilize" to" have" the insurance or an equivalent self-funded plan", to simplify language and make it clear the ask is just to *have* the insurance plan. The committee considered the verbs "maintain" and "use" when addressing cybersecurity responsibilities. The committee opted for "have" as it implies that the pharmacies and business entities will also utilize and maintain the insurance or plan. (2)
20. The committee discussed using the terms "recommends", "advocates", or "should", to determine how strong of a stance APhA should take on the impact on pharmacy curriculum. The Committee agreed that "advocates" is the best term to provide a stronger stance and highlight the importance of having education provided on this topic. (2,3)
21. The committee deliberated on whether proposed statements should make recommendations around information-sharing, referencing a possible repository of information about cyber-attacks that occur to be shared and inform others of how the attack was handled. The Committee confirmed that despite there not being a single, national cyber-attack repository, the FTC provides information on what should be done

in the event of a data breach titled Data Breach Response: A Guide for Business. The committee further reviewed the FTC's health breach notification rule and noted there are several organizations that must be notified of a data breach. Due to these existing processes, the Committee felt a specific statement on information sharing is not necessary at this time. (3)

22. The committee agreed that the term "educational providers" would include any person or persons that could be involved in educating pharmacists on cybersecurity and data record sets and would encompass all education – not just CE. (3)
23. When advocating for education related to cybersecurity and protection of the data record set, the committee discussed whether "best practices" or "policies" is most appropriate. While the broad pattern among existing APhA policy language is to opt for "policies" in such a list, the committee prefers "best practices" in this case. The committee determined that best practices may change more frequently, while policies tend to change less frequently. Therefore, to remain more evergreen, the committee decided ultimately to use the term "best practices". (3)
24. The committee initially recommended that education be addressed from a broad perspective. This was shifted to address education providers directly in order to be more actionable. (3)
25. The committee specifically included the terminology "education and training programs" to include not only academic training programs, but to also include post graduate training and continuing professional education. Using "education and training programs" would also encompass organizations that provide other forms of education as well. (3)
26. The committee decided to divide the cybersecurity statement into two parts – one for education providers and one for learners – to address both parties and their individual responsibilities relating to cybersecurity education and training. The addition of statement 4 puts the action directly on the learner. (3, 4)