State of Maine
132nd Legislature
Joint Standing Committee on Health and Human Services

Testimony of Charles F. Dingman on behalf of Covenant Health

Neither for nor Against
LD 2103, "An Act Requiring Hospitals to Adopt Cybersecurity Plans"

Sponsored by Representative Julie McCabe

February 24, 2026

Senator Ingrwesen, Representative Meyer, and members of the Joint Standing Committee on Health and Human Services, I am Charlie Dingman, a lawyer with the firm of Kozak & Gayer, and I am here today on behalf of Covenant Health. Covenant Health is a multi-state health care organization that supports and oversees the work of several acute and subacute health care providers in Maine, including St. Mary's Regional Medical Center in Lewiston and St. Joseph's Health Care in Bangor, both safety net hospitals, which work with strategic partners to deliver acute, primary, and behavioral health care and to address the social determinants of health in the communities they serve.

My testimony supplements the testimony of Win Brown in opposition to LD 2103. As Win has testified, Covenant appreciates and shares the concerns underlying this bill, and Representative McCabe's thoughtful approach to the issues at hand. Covenant stands ready to continue to share information about what we have learned and can continue to learn from recent cybersecurity incidents at Maine hospitals. Covenant looks forward to working with this Committee and others to improve both preventative measures and hospital resiliency against future attacks.

The specific measures proposed in this bill, however, would tend to complicate rather than improve hospital cybersecurity, adding administrative burdens and confusion due to duplication and overlap with existing federal and state requirements. My colleague Steve Johnson, who has extensive experience in navigating these existing requirements, has prepared an analysis, attached to my testimony, which breaks down the relationships between LD 2103 as currently proposed and the various existing state and federal laws governing information security.

As Mr. Johnson's attached table demonstrates, additional state requirements should not be enacted without careful consideration of the federal and state requirements that already exist. Adding potentially conflicting or duplicative legal requirements will not improve patient care and will impose added administrative costs without corresponding benefits.

The growing sophistication of bad actors in attacking modern information systems must not be ignored and calls for ongoing vigilance and innovation. Covenant is ready and willing to participate in that work. Covenant respectfully submits, however, that the best current response to recent disruptions of hospital operations is ongoing refinement of cybersecurity measures, as required by existing laws.

Thank you for your attention to this testimony. I would be pleased to respond to any questions now, at the work session, or in the interim via the contact information provided below.

Charles F. Dingman, *cdingman@kozakgayer.com, Mobile: (207)-240-9146*
Kozak & Gayer, P.A., 157 Capitol Street, Ste. 1, Augusta, ME 04330 | (207) 621-4390

Review and Analysis of AMENDED LD 2103

Steven L. Johnson, Esq., prepared for Charles F. Dingman, Esq.
Kozak & Gayer, P.A.
February 24, 2026

AMENDED LD 2103: • Would move 22 M.R.S.A. §1832 to 22 M.R.S.A. §1832(1) • Would enact 22 M.R.S.A. §1832(2) (NEW)	**New Cybersecurity Plan Requirements That AMENDED LD 2103 (specifically 22 M.R.S.A. §1832(2)) Would Impose on Maine Hospitals (including Critical Access Hospitals)**	**Comments; Other Applicable State and Federal Laws, Rules and Regulations Imposing the Same or Similar Requirements as AMENDED LD 2103 Would Impose on Maine Hospitals**
22 M.R.S.A. §1832(1), as set forth in AMENDED LD 2103	None.	The relocation of 22 M.R.S.A. §1832 to 22 M.R.S.A. §1832(1) would leave existing Maine law (§1832) intact and impose no new requirements.
New Definitions (22 M.R.S.A. §1832(2)(A)(1)-(3), as set forth in AMENDED LD 2103)		
22 M.R.S.A. §1832(2)(A)(1), as set forth in AMENDED LD 2103	"Cybersecurity": "the process of preventing unauthorized modification, misuse or denial of use, or the unauthorized use, of information that is stored, accessed or transferred from an electronic device to an external recipient."	1. Would apply to any "information" stored, accessed or transferred from any electronic device; not limited to PHI (under HIPAA), "health care information" (under Maine's Health Care Information Confidentiality Statute, 22 M.R.S.A. §1711-C(1)(E)), or "personal information" (under Maine's Notice of Risk to Personal Data Act, 10 M.R.S.A. Chapter 210-B, §1347(6)).
22 M.R.S.A. §1832(2)(A)(2), as set forth in AMENDED LD 2103	"Cybersecurity intrusion": "an unwanted intrusion into a computer system that impacts patient care, private information and security."	1. Cf. HIPAA's definition of "security incident": "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." 45 C.F.R. §164.304. Cf. HIPAA's definition of a "breach": "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [HIPAA]

		which compromises the security or privacy of the protected health information." 45 C.F.R. §164.402. Cf. definition of "breach of the security of the system" or "security breach" in Maine's Notice of Risk to Personal Data Act: "unauthorized acquisition, release or use of an individual's computerized data that includes personal information that compromises the security, confidentiality or integrity of personal information of the individual maintained by a person. Good faith acquisition, release or use of personal information by an employee or agent of a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure to another person." 10 M.R.S.A. §1347(1). 2. "Intrusion" in AMENDED LD 2103 remains undefined. 3. "Private information" in AMENDED LD 2103 is not defined. Does it apply to PHI (as defined by HIPAA)? Does it apply to "health care information" (as defined by Maine's Confidentiality of Health Care Information statute)? Does it apply to "personal information" (as defined by Maine's Notice of Risk to Personal Data Act)? Does it apply to some, all, or more than the above? If it only applies to the above types of information already afforded protected by other laws, it would introduce additional confusion and duplication. If it extends beyond or merely overlaps those categories, it will introduce unproductive vagueness to the regulation of information security. 4. "Computer system" in AMENDED LD 2103 remains undefined. Cf. HIPAA's definition of "information system": "an interconnected set of information resources under the same direct management control

		that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people." 45 C.F.R. §164.304. Cf. definition of "system" in Maine's Notice of Risk to Personal Data Act: "a computerized data storage system containing personal information." 10 M.R.S.A. §1347(7).
22 M.R.S.A. §1832(2)(A)(3), as set forth in AMENDED LD 2103	"Security incident response plan": "the part of a cybersecurity plan detailing how hospital employees are to report suspected or known security incidents and how a hospital will respond to suspected or known security incidents."	1. The "Security incident response plan" definition relies on the term "security incident," which is not defined in the bill. Is it intended to have the same meaning as a "cybersecurity intrusion" (which is defined)? Cf. HIPAA's definition of "security incident" noted above. 2. The definition of "cybersecurity intrusion" should either replace "security incident" here, or "security incident" (and HIPAA's definition of it) should replace "cybersecurity intrusion" in 22 M.R.S.A. §1832(2)(A)(2) (in AMENDED LD 2103). The latter approach would work best to achieve consistency and avoid confusion and potential conflict between HIPAA's requirements surrounding security incidents and AMENDED LD 2103's requirements regarding cybersecurity intrusions.
General Cybersecurity Plan Requirements		
22 M.R.S.A. §1832(2) as set forth in AMENDED LD 2103	1. Adoption of a Cybersecurity Plan: A licensed hospital "shall adopt…a cybersecurity plan."	1. This requirement is DUPLICATIVE of requirements Maine hospitals are already subject to under HIPAA's Security Rule (with respect to PHI/ePHI), and Maine's Confidentiality of Health Care Information statute (with respect to "health care information"). 2. Under HIPAA, Maine hospitals are already required to implement and comply with numerous stringent administrative, technical and physical security measures and safeguards (set forth in the HIPAA Security Standards at 45 C.F.R. Part 164, Subpart C) to

		"ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity [hospital]...creates, receives, maintains, or transmits"; to "protect against any reasonably anticipated threats or hazards to the security or integrity of such information"; to "protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under [HIPAA]"; and to "ensure compliance with [the HIPAA Security Rule] by its workforce." 45 C.F.R. §164.306(a)(1)-(4). Such safeguards include, among a host of other things, adoption and implementation of a Security Management Process that includes implementation of "policies and procedures to prevent, detect, contain, and correct security violations" (45 C.F.R. §164.308(a)(1)(i)); conducting "an accurate and thorough assessment [Risk Analysis] of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity" (45 C.F.R. §164.308(a)(1)(ii)(A)); implementing Risk Management "security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level" (45 C.F.R. §164.308(a)(1)(ii)(B)); and implementing "procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports" (45 C.F.R. §164.308(a)(1)(ii)(D)). 3. Under Maine's Confidentiality of Health Care Information statute, hospitals are already required to "develop and implement policies, standards and procedures to protect the confidentiality, security and integrity of health care information to ensure that information is not negligently, inappropriately or unlawfully disclosed." 22 M.R.S.A. §1711-C(7).

22 M.R.S.A. §1832(2) as set forth in AMENDED LD 2103	2. Cybersecurity Plan's Compliance with Best Practices Established by the Cybersecurity and Infrastructure Agency: "The cybersecurity plan must be compliant with best practices established by the Cybersecurity and Infrastructure Security Agency or its current equivalent."	1. This could potentially impose NEW requirements on Maine hospitals based on generic cybersecurity standards that, unlike the HIPAA Security Standards, *are not specific to the health care industry*. The HIPAA Security Standards and technical compliance guidance and tools have been established *specifically for the health care industry* by the U.S. DHHS Office of Civil Rights and the Office of the National Coordinator for Health Information Technology, a staff division within the U.S. DHHS. 2. It would involve additional time and research to determine the extent to which the "best practices" established by the Cybersecurity and Infrastructure Security Agency (see https://www.cisa.gov/topics/cybersecurity-best-practices) are consistent with, more or less stringent than, or duplicative of, the HIPAA Security Standards. 3. To the extent the "best practices" established by the Cybersecurity and Infrastructure Security Agency are inconsistent with the requirements of the HIPAA Security Standards, HIPAA would preempt any state law imposing requirements that are less stringent than HIPAA's requirements. See 45 C.F.R. Part 160, Subpart B ([HIPAA] Preemption of State Law).
22 M.R.S.A. §1832(2) and (2)(H) as set forth in AMENDED LD 2103	3. Submission of Cybersecurity Plan to Maine DHHS: A licensed hospital "shall submit to the department [of health and human services] a cybersecurity plan." Pursuant to §1832(2)(H), the "cybersecurity plan submitted to the [Maine] department [of health and human services]…[is] confidential."	1. This would impose a NEW requirement on Maine hospitals. 2. Currently, Maine hospitals are not required to submit to Maine DHHS a copy of their cybersecurity plan, or other documentary evidence of compliance with Maine's health information security and policy requirements set forth at 22 M.R.S.A. §1711-C(7), or evidence of compliance with the administrative, technical and physical security safeguard requirements of the HIPAA Security Rule, unless such information

		were requested by DHHS, for example, in connection with a complaint investigation or a hospital licensing survey. However, DHHS already has the authority to enter, request, obtain and inspect such information from hospitals under Maine's Hospital Licensing Rules. See 10-144 C.M.R. Chapter 112, Sections 2.15.3, 2.20, 2.20.2, 2.20.3 and 4.2.
22 M.R.S.A. §1832(2) as set forth in AMENDED LD 2103	4. Annual Updates to Cybersecurity Plan: A licensed hospital "shall update the [cybersecurity] plan at least once per year...."	1. The requirement that hospitals update their cybersecurity plans *at least once per year* would impose a NEW timeframe requirement on Maine hospitals. 2. However, under HIPAA, Maine hospitals are already required to "perform a periodic technical and nontechnical evaluation, based initially upon the [security] standards implemented under [the HIPAA Security] rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's...security policies and procedures meet the requirements of [the HIPAA Security Rule]." 45 C.F.R. §164.308(a)(8). 3. Under HIPAA, Maine hospitals are already required to "review and modify the security measures implemented under [the HIPAA Security Standards] as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures". 45 C.F.R. §164.306(e). 4. HIPAA's more flexible "periodic" and "as needed" timeframes for conducting and maintaining such security plan evaluations and updates are more appropriate because environmental and operational

		changes can create security vulnerabilities necessitating evaluations and updates more frequently than annually.
22 M.R.S.A. §1832(2) as set forth in AMENDED LD 2103	5. Submission of Annually Updated Cybersecurity Plan to Maine DHHS: A licensed hospital "shall…submit the updated [cybersecurity] plan to the [Maine] department [of health and human services]."	1. This would impose a NEW requirement on Maine hospitals. 2. As noted above, currently Maine hospitals are not required to submit to Maine DHHS a copy of their cybersecurity plan, or other documentary evidence of compliance with Maine's health information security and policy requirements set forth at 22 M.R.S.A. §1711-C(7), or evidence of compliance with the administrative, technical and physical safeguard requirements of the HIPAA Security Rule, unless such information were requested by DHHS, for example, in connection with a complaint investigation or a hospital licensing survey. However, DHHS already has the authority to enter, request, obtain and inspect such information from hospitals under Maine's Hospital Licensing Rules, and to require a Maine hospital to adopt and implement a plan of correction to address any identified licensing violations or compliance deficiencies. See 10-144 C.M.R. Chapter 112, Sections 2.15.3, 2.17, 2.17.1, 2.17.2, 2.17.3, 2.20, 2.20.2, 2.20.3 and 4.2.
Specific Cybersecurity Plan Requirements		
22 M.R.S.A. §1832(2)(B)(1) as set forth in AMENDED LD 2103	6. Cybersecurity Intrusion Notifications: "The cybersecurity plan must include…[a] provision for the timely notification of a cybersecurity intrusion to appropriate parties, including, but not limited to law enforcement agency [sic?], patients, municipalities, state regulators, media and hospital personnel. The hospital shall include in all public communications related	1. These provisions would impose NEW notification requirements on Maine hospitals—specifically notification of law enforcement agencies, municipalities and state regulators—while DUPLICATING other notification requirements Maine hospitals are already subject to under HIPAA and Maine's Notice of Risk to Personal Data Act. These provisions would also impose a NEW requirement on Maine hospitals to include in all public

	to the cybersecurity intrusion information regarding patient rights and the contact information for registering a patient complaint."	communications related to a cybersecurity intrusion information on patient rights and on how to file a complaint. 2. These provisions do not specify a timeframe for defining when notification is considered "timely". Would recommend deferring to notification timeframes established by other applicable law (HIPAA, Maine's Notice of Risk to Personal Data Act, discussed below). 3. What's the rationale for notification of municipalities? And if such notification is going to be required, shouldn't it be limited to the municipality in which the hospital is located, or within a particular distance from the hospital or served by the hospital? <u>Maine Hospitals' Existing Breach Notification Obligations</u> 4. Under HIPAA, Maine hospitals are already required to notify affected individuals of any security and/or privacy breaches of their PHI/ePHI within 60 days of discovery of the breach. See 45 C.F.R. §164.404(a)(1) and (b). Maine hospitals are also required to notify the Secretary of the Federal DHHS of any such breaches. See 45 C.F.R. §164.408(a). Additionally, for breaches involving more than 500 residents, Maine hospitals are also required to notify the media. See 45 C.F.R. §164.406(a). 5. Under Maine's Notice of Risk to Personal Data Act, Maine hospitals are already required to notify affected individuals, as well as state regulators or the Maine Attorney General, of any breaches of "personal information" "as expediently as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement," but not more than 30 days after discovery of the breach and identification of its scope.

		10 M.R.S.A. §1348(1) and (5). Notification of nationwide consumer reporting agencies is also required in breaches of personal information involving more than 1,000 persons. 10 M.R.S.A. §1348(4). <u>Maine Hospitals' Existing Obligations to Inform Patients about Their Rights, including the Right to File Complaints</u> 6. Under HIPAA's breach notification requirements, Maine hospitals are already required to include in individual breach notifications "contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address." 45 C.F.R. §164.404(c)(1)(E). 7. All hospital patients are also already informed at the time of intake or admission of their HIPAA privacy rights and of their privacy-related rights under state law in each hospital's HIPAA Notice of Privacy Practices, including their right to notification of any breaches of their PHI/ePHI, their right to file a privacy-related complaint with the hospital and with the Secretary of the U.S. DHHS, and contact information about how to exercise such rights and file such a complaint. See 45 C.F.R. §164.520(a)(1), (b)(1)(iv)(A)-(F), (b)(1)(v)(A), and (b)(1)(vi)-(vii). Hospitals also make their HIPAA Notices of Privacy Practices available to patients and the public on their websites. 8. Under Federal Medicare Conditions of Participation for Hospitals, Maine hospitals are already required to notify patients of their rights, including their rights with respect to the confidentiality of their medical records, their right to access such records, and their right to file a complaint. See 42 C.F.R. §482.13(a)(1), (a)(2), and (d)(1)-(2).

		9. Under Federal Medicare Conditions of Participation for Critical Access Hospitals, Maine CAHs are already required to notify patients of their rights, including their rights with respect to the confidentiality of their medical records, their right to access such records, and their right to file a complaint. See 42 C.F.R. §485.614(a)(1), (a)(2), and (d)(1)-(2).
22 M.R.S.A. §1832(2)(B)(2) as set forth in AMENDED LD 2103	7. Cybersecurity Backup Communication Response: "The cybersecurity plan must include…[a] backup communication response provision that ensures continuity of care for patients in the event of a disruption of hospital computer systems caused by a cybersecurity intrusion or a natural or human driven disaster, and including: (a) a process by which patients are provided same day access to paper copies of medical records; (b) a complaint process for patients who are experiencing challenges accessing medical care and a system to triage patient complaints, including: (i) a requirement that emergent concerns receive a response within 48 hours of the submission of the inquiry and that non-emergent concerns receive a response with 7 days of the submission of the inquiry; and (ii) a requirement for the timely management of requests related to prescriptions; and (c) a provision requiring that all manually charted records be timely integrated into the hospital's electronic record system."	1. Some of these provisions would impose NEW requirements on Maine hospitals, namely, the requirement to provide patients same-day access to paper copies of their hospital medical records, the requirement that patient complaints be triaged and responded to within specific timeframes, and the requirement for the timely management of prescriptions. Other of these provisions would impose DUPLICATIVE requirements on Maine hospitals to which Maine hospitals are already subject under other applicable laws indicated below. Backup Communication Response That Ensures Continuity of Care 2. Under Medicare Conditions of Participation for Hospitals and Critical Access Hospitals, Maine hospitals and CAHs are already required to develop and maintain a Communication Plan as part of their mandatory Emergency Preparedness Plan that must be reviewed and updated at least every 2 years, that identifies the primary and alternate means of communicating with the hospital's staff and Federal, State, tribal, regional, and local emergency management agencies, and that includes a method for sharing information and medical documentation for patients under the hospital's care, as necessary, with other health care providers to maintain the continuity of care. 42 C.F.R. §482.15(c); and 42 C.F.R. §485.625(c).

		3. Under HIPAA, Maine hospitals are already required to adopt and implement security measures to "ensure the…integrity, and availability of all electronic protected health information" in the event of a security incident or breach to ensure that such information is available to patients and their health care providers for treatment, communication and continuity of care purposes. See 45 C.F.R. §164.306(a)(1). In such circumstances, Maine hospitals are already required to ensure that patients' PHI/ePHI is available in "retrievable exact copies" via "procedures to restore any loss of data" and that "enable continuation of critical business processes…while operating in emergency mode." 45 C.F.R. §164.308(a)(7)(ii)(A)-(C). 4. Under HIPAA, Maine hospitals are already required to implement a Contingency Plan and "establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, …system failure…) that damages systems that contain electronic protected health information." 45 C.F.R. §164.308(7)(i). The Contingency Plan must include "procedures to create and maintain retrievable exact copies of electronic protected health information," "procedures to restore any loss of data," "procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode," "procedures for periodic testing and revision of contingency plans," and assessment of "the relative criticality of specific applications and data in support of other contingency plan components." 45 C.F.R. §164.308(7)(ii)(A)-(E).

		5. Under HIPAA, Maine hospitals are already required to "review and modify the security measures implemented under [the HIPAA Security Standards] as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures". 45 C.F.R. §164.306(e). <u>Same Day Patient Access to Paper Copies of Their Medical Records; Maine Hospitals' Existing Obligations to Provide Patients Access to Copies of Their Medical Records</u>: 6. Under Medicare Conditions of Participation for Hospitals and CAHs, Maine hospitals are already required to provide patients access to copies of their medical records "within a reasonable time frame." See 42 C.F.R. §482.13(d)(2); and 42 C.F.R. 485.614(d)(2). 7. Under HIPAA, Maine hospitals are already required to provide patients access to copies of their medical records "in a timely manner" but within 30 days of a request. 45 C.F.R. §164.524(b)(2)(i) and (c)(3)(i). 8. Under Maine's Patient Access to Hospital Medical Records statute, Maine hospitals are already required to provide patients copies of their medical records in accordance with HIPAA's requirements and timeframe. See 22 M.R.S.A. §1711. <u>Triaged Patient Complaint Process and Response Timeframes; Maine Hospitals' Existing Obligations Regarding Patient Complaints</u> 9. Under Maine's Hospital Licensing Rules, Maine hospitals are already required to have a patient complaint process, regardless of the nature or subject matter of the complaint: "Each hospital must publish a

		toll-free telephone number for complainants to contact the hospital. Each hospital must educate the public about hospital complaint resolution procedures. At a minimum, each hospital must post information in a public part of the hospital explaining the complaint resolution procedures and listing the toll-free complaint telephone number." 10-144 C.M.R. Chapter 112, Section 4.1.1. 10. Under Medicare Conditions of Participation for Hospitals and CAHs, Maine hospitals are already required to have a patient grievance process for the resolution of patient complaints, regardless of the nature or subject matter of the complaint. See 42 C.F.R. §482.13(a)(2)(i)-(iii); and 42 C.F.R. §485.614(a)(2)(i)-(iii). 11. Under HIPAA, patients already have the right to file a complaint with the hospital and with the Secretary of the Federal DHHS (via DHHS's Office of Civil Rights) anytime they believe their HIPAA privacy rights may have been violated, including violations of their right to access their PHI/hospital medical records. 45 C.F.R. §164.520(b)(1)(vi). 12. Under Maine law, patients have the right to notify the Maine Attorney General anytime they believe a hospital may have violated their rights with respect to their health care information, including their right to access their health care information. 22 M.R.S.A. §1711-C(13)(A). 13. Federal Medicare Conditions of Participation for both Hospitals and CAHs already require that hospitals resolve all patient complaints in a "prompt" manner, but defer to hospitals and CAHs to "specify time frames" for their review and resolution of such

		complaints. See 42 C.F.R. §482.13(a)(2) and (a)(2)(ii); and 42 C.F.R. 485.614(a)(2) and (a)(2)(ii). 14. Under Maine's Hospital Licensing Rules, patients are "encouraged" by the Maine DHHS "to resolve complaints directly with the hospital before initiating a department complaint investigation," and "[e]ach hospital must publish a toll-free telephone number for complainants to contact the hospital. Each hospital must educate the public about hospital complaint resolution procedures. At a minimum, each hospital must post information in a public part of the hospital explaining the complaint resolution procedures and listing the toll-free complaint telephone number. 10-144 C.M.R. Chapter 112, Sections 4.1 and 4.1.1. Hospitals are provided 45 days to investigate a complaint and to file a report of its investigation with the Maine DHHS. See 10-144 C.M.R. Chapter 112, Section 4.6.3. <u>Timely Management of Prescriptions</u>: 15. Maine hospitals and their prescribing providers are already stringently regulated with respect to the management of prescriptions, including by CMS, the DEA and the Maine Board of Pharmacy. See, e.g., 42 C.F.R. §482.23(c); Maine Pharmacy Act, 32 M.R.S.A. Chapter 117; 02-392 C.M.R. Chapters 1-38 (Maine Board of Pharmacy Rules). <u>Timely Integration of Manually Charted Records into Electronic Record System</u>: 16. Patients already have the right under both HIPAA and Maine law to access copies of their hospital medical records in whatever form they exist, whether in electronic or hardcopy paper form, and whether or not

		such paper records are or not integrated in the hospital's electronic medical record for the patient, within the timeframes established under HIPAA and Maine law. 22 M.R.S.A. §1711; 45 C.F.R. §164.524. However, Maine hospitals already routinely incorporate paper records into their EMR systems in accordance with their HIPAA-mandated "designated record set" policies and procedures. 17. Medicare Conditions of Participation for Hospitals and CAHs already require hospitals to maintain accurate, promptly completed, properly filed and retained, and accessible medical records for each hospital patient, regardless of whether such records are in hardcopy or electronic form, and that any such records be safeguarded against loss, destruction or unauthorized use. See 42 C.F.R. §482.24; 42 C.F.R. §485.638. 18. HIPAA also already requires that hospitals ensure that all records upon which patient care decisions are made be maintained and accessible in the form of one or more "designated record sets," which are not required to be maintained in electronic form. See 45 C.F.R. §164.501 and §164.524.
22 M.R.S.A. §1832(2)(B)(3) as set forth in AMENDED LD 2103	8. Triage of Hospital Services: "The cybersecurity plan must include…[a] provision to ensure proper triage of hospital services in the event of a disruption of hospital computer systems, including: (a) a provision for the triage of all hospital services, including elective procedures, based on system capacities and patient needs; (b) a provision for the diversion of hospital services as necessary, including emergency and nonemergency transportation services; and (c) a	1. These provisions would impose DUPLICATIVE requirements on Maine hospitals to which they are already subject under other applicable laws indicated below. 2. Under Medicare Conditions of Participation for Hospitals and CAHs, Maine hospitals are already required to develop and maintain a comprehensive Emergency Preparedness Plan that addresses "patient population, including, but not limited to, persons at-risk; the type of services the hospital has the ability to provide in an emergency; and continuity of operations,"

	requirement for written agreements with other hospitals and healthcare providers located within 150 miles to facilitate continuity of care during hospital system downtime."	that includes "a process for cooperation and collaboration with local, tribal, regional, State, and Federal emergency preparedness officials' efforts to maintain an integrated response during a disaster or emergency situation," that includes policies and procedures for the "safe evacuation from the hospital, which includes consideration of care and treatment needs of evacuees; staff responsibilities; transportation; identification of evacuation location(s); and primary and alternate means of communication with external sources of assistance," that includes "a system of medical documentation that preserves patient information, protects confidentiality of patient information, and secures and maintains the availability of records," and that includes "the development of arrangements with other hospitals and other providers to receive patients in the event of limitations or cessation of operations to maintain the continuity of services to hospital patients." 42 C.F.R. §482.15(a)(3)-(4) and (b)(3), (b)(5), and (b)(7); and 42 C.F.R. §485.625(a)(3)-(4) and (b)(3), (b)(5), and (b)(7). Moreover, anytime a Maine hospital undertakes an emergency evacuation of patients the hospital such action constitutes a reportable "incident" to the Maine DHHS within 24 hours under Maine Hospital Licensing Rules. See 10-144 C.M.R. Chapter 112, Section 1.6. 3. Hospitals with dedicated emergency departments are subject to and regulated by the Federal Emergency Treatment and Active Labor Act (EMTALA) and the Federal EMTALA regulations and are already required by EMTALA to appropriately and timely triage and conduct medical screening examinations of any patient presenting to the hospital with a potential emergency medical condition within the capacity and capabilities of the hospital at any given time and regardless of the circumstances (whether a natural disaster, bomb threat,

		mass casualty, or cyber-incident) giving rise to the need to triage presenting patients. 42 C.F.R. §489.24. 4. The Federal EMTALA regulations and CMS's EMTALA Interpretive Guidelines also already address hospitals' Federal EMTALA obligations with respect to patients presenting to a hospital that is on diversionary status (regardless of the circumstances giving rise to the hospital's reason for going on diversionary status), and the process for the proper diversion and transfer of hospital patients in such circumstances. See 42 C.F.R. §489.24; CMS State Operations Manual, Appendix V (Rev. 191, 07-19-19). (It's likely that Maine's EMS Act, EMS Rules and EMS Protocols also address such circumstances, though we would need more time to look into the particulars.)
22 M.R.S.A. §1832(2)(B)(4) as set forth in AMENDED LD 2103	9. Written Security Incident Response Plan: "The cybersecurity plan must include…a written security incident response plan documenting how employees are to report suspected or known security incidents and how the hospital will clinically respond to suspected or known security incidents. The security incident response plan must include provisions detailing how hospital personnel can effectively communicate with one another and with outside medical providers in the event electronic systems are non-operable. The security incident response plan must be made available to all hospital personnel."	1. This requirement would impose DUPLICATIVE requirements on Maine hospitals to which they are already subject under other applicable laws indicated below. 2. HIPAA already stringently regulates how Maine hospitals are required to respond to "security incidents". Hospitals are required to (i) "implement policies and procedures to address security incidents" (45 C.F.R. §164.308(a)(6)(i)); (ii) "respond to suspected or known security incidents" (45 C.F.R. §164.308(a)(6)(ii)); (iii) "mitigate, to the extent practicable, harmful effects of security incidents that are known" (45 C.F.R. §164.308(a)(6)(ii)); (iv) "document security incidents and their outcomes" (45 C.F.R. §164.308(a)(6)(ii)); and (v) "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." 45 C.F.R. §164.308(a)(ii)(D).

		3. HIPAA also requires hospitals to require hospital contractors (HIPAA "business associates") to "report to the covered entity [hospital] any security incident of which it becomes aware, including breaches of unsecured protected health information...." 45 C.F.R. §164.314(a)(2)(i)(C)). 4. HIPAA already stringently regulates how hospitals are required to respond to "security incidents" that involve known, reported and suspected "breaches" of PHI/ePHI, including requiring known or suspected breaches to be reported internally by hospital workforce members and requiring each breach to be investigated, mitigated and documented in a Risk Assessment. See 45 C.F.R. Part 164, Subpart D; 45 C.F.R. §164.402 (paragraph 2 of the definition of "breach") and §164.414(a); 45 C.F.R. §164.308(a)(6)(ii); and 45 C.F.R. §164.530(f). 5. Maine's Notice of Risk to Personal Data Act already stringently regulates how hospitals are required to respond to security incidents that involve breaches of computer systems containing "personal information," and requires that all known, reported or suspected breaches be reasonably and promptly investigated in good faith. See 10 M.R.S.A. Chapter 210-A; 10 M.R.S.A. §1348(1)(B). 6. Under Medicare Conditions of Participation for Hospitals, Maine hospitals are already required to "develop and maintain a comprehensive emergency preparedness program, utilizing an all-hazards approach," that is based on a facility-based and community-based risk assessment, that must be reviewed and updated at least every 2 years, that addresses the hospital's patient population, including persons at-risk, the type of services the hospital has the

		ability to provide in an emergency, and the continuity of operations, and that must "include a process for cooperation and collaboration with local, tribal, regional, State, and Federal emergency preparedness officials' efforts to maintain an integrated response during a disaster or emergency situation." 42 C.F.R. §482.15(a) and (a)(1)-(4). The hospital's Emergency Preparedness Plan must also provide for the safe evacuation from the hospital, including consideration of care and treatment needs of evacuees, staff responsibilities, transportation, identification of evacuation locations, and primary and alternate means of communication with external sources of assistance (42 C.F.R. §482.15(b)(3)), and for the development of arrangements with other hospitals and other providers to receive patients in the event of limitations or cessation of operations to maintain the continuity of services to hospital patients (42 C.F.R. §482.15(b)(7)). 7. Under Medicare Conditions of Participation for Critical Access Hospitals, Maine CAHs are also already required to "develop and maintain a comprehensive emergency preparedness program, utilizing an all-hazards approach," that is based on a facility-based and community-based risk assessment, that must be reviewed and updated at least every 2 years, that addresses the CAH's patient population, including persons at-risk, the type of services the CAH has the ability to provide in an emergency, and the continuity of operations, and that must "include a process for cooperation and collaboration with local, tribal, regional, State, and Federal emergency preparedness officials' efforts to maintain an integrated response during a disaster or emergency situation." 42 C.F.R. §485.625(a) and (a)(1)-(4). The CAH's Emergency Preparedness Plan must also provide for the safe evacuation from the hospital, including consideration of

		care and treatment needs of evacuees, staff responsibilities, transportation, identification of evacuation locations, and primary and alternate means of communication with external sources of assistance (42 C.F.R. §482.15(b)(3)), and for the development of arrangements with other CAHs or other providers to receive patients in the event of limitations or cessation of operations to maintain the continuity of services to CAH patients (42 C.F.R. §485.625(b)(7)).
22 M.R.S.A. §1832(2)(B)(5) as set forth in AMENDED LD 2103	10. Cybersecurity Training: "The cybersecurity plan must include…[a] provision for, at a minimum, annual cybersecurity training for hospital employees, hospital board members and organizations affiliated with the hospital, including new employee and annual training for all employees who use electronic health record systems for patient care. The training must include information relating to the management of patient records in the event of unplanned the [sic] hospital's electronic health record downtime, including training on paper charting."	1. This requirement would impose DUPLICATIVE requirements on Maine hospitals. 2. Maine hospitals are already required by HIPAA to "implement a security awareness and training program for all members of its workforce (including management)," that includes "periodic security updates," "procedures for guarding against, detecting, and reporting malicious software," "procedures for monitoring log-in attempts and reporting discrepancies," and "procedures for creating, changing, and safeguarding passwords." 45 C.F.R. §164.308(a)(5)(i)-(ii). 3. HIPAA also already requires Maine hospitals to "train all members of its workforce on the policies and procedures with respect to protected health information required by [HIPAA, including training on HIPAA's breach notification requirements], as necessary and appropriate for members of the workforce to carry out their functions within the covered entity." 45 C.F.R. §164.530(b)(1). Such training must be provided to each member of the hospital's workforce "within a reasonable period of time after the person joints the covered entity's workforce" and "to each member of the workforce whose functions are affected by a material change in the policies and procedures…within a reasonable period of time after the material change

		becomes effective...." 45 C.F.R. §164.530(b)(2)(i)(A)-(C). Such training must also be documented. 45 C.F.R. §164.530(b)(2)(ii). 4. Although "organizations affiliated with the hospital" is ambiguous and of uncertain meaning and scope, Maine hospitals are already required by HIPAA to ensure that all persons and entities performing contracted services for a hospital that involve access to hospital patients' PHI/ePHI comply with HIPAA's privacy and security requirements, including workforce member HIPAA training requirements, in a legally binding HIPAA "business associate agreement". See 45 C.F.R. § 164.302 ("A...business associate must comply with the applicable standards, implementation specifications, and requirements of [the HIPAA Security Standards] with respect to electronic protected health information of a covered entity."). 5. Under Medicare Conditions of Participation for Hospitals and CAHs, Maine hospitals/CAHs are already required to implement a staff training program at least every 2 years on the hospital's comprehensive Emergency Preparedness Program and the Program's policies and procedures. 42 C.F.R. §482.15(d)(1). 42 C.F.R. §485.625(d)(1).
22 M.R.S.A. §1832(2)(B)(6) as set forth in AMENDED LD 2103	11. Annual Test Run of Hospital's Downtime Procedures: "The cybersecurity plan must include...a requirement that the hospital perform an annual test run involving all hospital shifts and units of downtime procedures for the hospital's cybersecurity plan and a requirement that all downtime paperwork be reviewed and updated at the time of the annual test run."	1. This is DUPLICATIVE of what Maine hospitals are already required to do under HIPAA, and on a more frequent and stringent basis under the Medicare Conditions of Participation for Hospitals and CAHs. 2. Under Medicare Conditions of Participation for Hospitals and CAHs, Maine hospitals/CAHs are already required to "conduct exercises to test [their] emergency [preparedness] plan at least twice per year," including "an annual full-scale exercise that is community-based" plus an additional annual exercise

		that is either a community- or facility-based functional exercise, a mock disaster drill, or a tabletop exercise or workshop"; hospitals'/CAHs' responses to such tests and exercises must also be analyzed and documented and the Emergency Preparedness Plan must be revised as needed in light of such testing/exercises. 42 C.F.R. §482.15(d) and (d)(2)(i)-(iii); and 42 C.F.R. §485.625(d) and (d)(2)(i)-(iii). 3. Under HIPAA, Maine hospitals are already required to implement a Contingency Plan and "establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, ...system failure...) that damages systems that contain electronic protected health information." 45 C.F.R. §164.308(7)(i). Such Contingency Plan must include a Data Backup Plan ("procedures to create and maintain retrievable exact copies of electronic protected health information"), a Disaster Recovery Plan ("procedures to restore any loss of data"), an Emergency Mode Operation Plan ("procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode"), Testing and Revising Procedures ("procedures for periodic testing and revision of contingency plans"), and a Data Criticality Analysis of the hospital's applications and data (an assessment of "the relative criticality of specific applications and data in support of other contingency plan components"). 45 C.F.R. §164.308(7)(ii)(A)-(E). Maine hospitals are currently required to perform such security Contingency Plan evaluations on a "periodic" basis as necessary to

		respond to environmental or operational changes affecting the security of PHI/ePHI.[1] 4. Additionally, Maine hospitals are also already required under HIPAA to "perform a periodic technical and nontechnical evaluation, based initially upon the [security] standards implemented under [the HIPAA Security] rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's…security policies and procedures meet the requirements of [the HIPAA Security Rule]." 45 C.F.R. §164.308(a)(8). 5. Under HIPAA, Maine hospitals are also already required to "review and modify the security measures implemented under [the HIPAA Security Standards] as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures". 45 C.F.R. §164.306(e).
22 M.R.S.A. §1832(2)(B)(7) as set forth in AMENDED LD 2103	12. Written Procedures for Testing and Revising Cybersecurity Plan: "The cybersecurity plan must include…written procedures for testing and revising the cybersecurity plan, including (a) a requirement that the hospital perform an annual analysis of the criticality of their information systems and technology assets to determine the priority for	1. This would impose DUPLICATIVE requirements on Maine hospitals to which they are already subject under the HIPAA Security Standards and Medicare Conditions of Participation for Hospitals and CAHs. 2. *See comments above in response to #11 in the second column.*

[1] The HIPAA Security Rule reasonably adopts a "flexibility" approach with respect to a hospital's adoption and implementation of any specific security measures so that a hospital may "take into account" the "size, complexity, and capabilities" of the hospital, the hospital's "technical infrastructure, hardware, and software security capabilities," "the costs of security measures," and "the probability and criticality of potential risks to electronic protected health information." 45 C.F.R. §164.306(b)(1) and (b)(2)(i)-(iv).

	restoration; (b) a requirement that the hospital perform a tabletop simulation of a cybersecurity incident resulting in the disruption of hospital computer systems; and (c) a requirement that the hospital perform continuous vulnerability scans and annual penetration testing to identify network vulnerabilities."	3. Under HIPAA Security Standards, Maine hospitals are already required to "assess the relative criticality of specific applications and data in support of other contingency plan components" (45 C.F.R. §164.308(a)(7)(E)), to have "security incident procedures" to "identify and respond to suspected or known security incidents" and to "mitigate…harmful effects of security incidents" (45 C.F.R. §164.308(a)(6)(i)-(ii)) and "procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports" (45 C.F.R. §164.308(1)(ii)(D)), and to conduct periodic Risk Analyses that accurately and thoroughly assess "the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information" (45 C.F.R. §164.308(a)(1)(ii)(A)).
22 M.R.S.A. §1832(2)(B)(7) as set forth in AMENDED LD 2103	13. Submission of Results of Cybersecurity Plan Tests: "The hospital must submit the results of tests [of the cybersecurity plan] to the [Maine] department [of health and human services] at the time of the annual submission of the hospital's cybersecurity plan."	1. This would impose a NEW requirement on Maine hospitals.
22 M.R.S.A. §1832(2)(B)(8) as set forth in AMENDED LD 2103	14. Timely Restoration of Communication with Maine HealthInfoNet: "The cybersecurity plan must include…a provision for timely restoration of communication with the state-designated statewide health information exchange described at section 1711-C, subsection 18."	1. This would impose a NEW requirement on Maine hospitals, though restoration of communication with Maine HealthInfoNet would likely already be incorporated into a hospital's Communication and Emergency Preparedness Plans required under Medicare Conditions of Participation for Hospitals and CAHs, as well as into hospitals' mandatory Contingency Plan, Emergency Operation Mode Plan, and Data Backup and Recovery Plans required under the HIPAA Security Standards.
22 M.R.S.A. §1832(2)(B)(9) as set forth in AMENDED LD 2103	15. Review of Responses to Cybersecurity Incidents Occurring Since January 1, 2024: "The cybersecurity plan must include…a	1. This would impose DUPLICATIVE requirements on Maine hospitals to which they are already subject under HIPAA with respect to PHI/ePHI.

	provision requiring the review of the hospital's response to any cybersecurity incidents that have taken place at the hospital since January 1, 2024, including lessons learned and a description of any actions taken by the hospital to prevent future occurrences and to mitigate the harm caused by similar events. The report must include information regarding the involvement of security consultants, law enforcement and cyber insurance."	2. As noted above, Maine hospitals are already required by the HIPAA Security Standards to investigate, respond to, mitigate and document all known or suspected security incidents and their outcomes, and to update their security measures, safeguards, policies and procedures anytime such security incidents identify risks and vulnerabilities warranting such revisions. 3. As noted above, Maine hospitals are already required to respond to, perform a Risk Assessment, and mitigate and document all suspected, reported or known breaches of PHI/ePHI, and to update their security measures, safeguards, policies and procedures anytime such breaches identify risks and vulnerabilities warranting such revisions. 4. Under HIPAA, Maine hospitals already have an obligation to mitigate, to the extent practicable, harmful effects of security incidents and breaches, and to notify affected patients of such mitigation measures taken in cases of security incidents involving breaches of PHI/ePHI. See 45 C.F.R. §164.530(f); §164.308(a)(6); and §164.404(c)(1)(D).
22 M.R.S.A. §1832(2)(C) as set forth in AMENDED LD 2103	16. Development of Cybersecurity Plan with Input from Working Group: "The cybersecurity plan must be developed and maintained with the input of an annual working group that includes frontline health care workers employed by the hospital and those workers' labor unions."	1. This would impose a NEW requirement on Maine hospitals. 2. To the extent that input from the working group would involve input inconsistent with HIPAA, HIPAA would preempt any state law requirement that would impose less stringent requirements than HIPAA already imposes. See 45 C.F.R. Part 160, Subpart B ([HIPAA] Preemption of State Law).
22 M.R.S.A. §1832(2)(D) as set forth in AMENDED LD 2103	17. Retention of Hardcopy Documentation Created during Electronic Health System Downtimes: "A hospital…must maintain physical copies of all forms and other	1. This would impose DUPLICATIVE requirements on Maine hospitals already required by Federal Medicare Conditions of Participation, Maine Hospital Licensing Rules, and HIPAA, to maintain current and accurate

	paperwork required to maintain continuity of care during electronic health systems downtime."	medical records for all patients at all times, whether in electronic or hardcopy form. See 45 C.F.R. §482.24 and §485.638; 10-144 C.M.R. Chapter 112, Section 3.1; and HIPAA's "designated record set" requirements noted elsewhere herein.
22 M.R.S.A. §1832(2)(E) as set forth in AMENDED LD 2103	18. Annual Cybersecurity Plan Audit: "A hospital…must annually subject the hospital's cybersecurity plan to an audit by an independent, certified cybersecurity auditor or cybersecurity expert to determine the adequacy of the cybersecurity plan and identify any necessary improvements to such plans and processes."	1. This provision would impose a NEW requirement on Maine hospitals. 2. Maine hospitals are already required by HIPAA to ensure that they comply with HIPAA's Security Standards, whether or not they utilize an independent certified cybersecurity auditor or expert to confirm such compliance.
22 M.R.S.A. §1832(2)(E) and (2)(H) as set forth in AMENDED LD 2103	19. Submission of Cybersecurity Plan Audits to Maine Department of Health and Human Services: "The hospital shall submit the results of each [cybersecurity plan] audit to the [Maine] department [of health and human services]." Pursuant to §1832(2)(H), the "the results of [a cybersecurity plan] audit submitted to the [Maine] department [of health and human services]…are confidential."	1. This would impose a NEW requirement on Maine hospitals.
22 M.R.S.A. §1832(2)(F) as set forth in AMENDED LD 2103	20. Information on How to File a Complaint with the Maine Department of Health and Human Services: "A hospital…must make available to employees and the public information regarding how to file a complaint with the [Maine] department [of health and human services], including by posting this information in public areas of the hospital."	1. This provision would impose DUPLICATIVE requirements on Maine hospitals (regarding the provision of information to patients on how to file a complaint) to which hospitals are already subject under other applicable laws indicated below, as well as a NEW requirement for hospitals to notify their own employees about how to file a complaint with the Maine DHHS. 2. Under Maine's Hospital Licensing Rules, Maine hospitals are already required to have a patient complaint process, regardless of the nature or subject matter of the complaint: "Each hospital must publish

		a toll-free telephone number for complainants to contact the hospital. Each hospital must educate the public about hospital complaint resolution procedures. At a minimum, each hospital must post information in a public part of the hospital explaining the complaint resolution procedures and listing the toll-free complaint telephone number." 10-144 C.M.R. Chapter 112, Section 4.1.1. 3. Under CMS Medicare Conditions of Participation for Hospitals and CAHs, Maine hospitals/CAHs are already required to have a patient grievance process for the resolution of patient complaints, regardless of the nature or subject matter of the complaint. See 42 C.F.R. §482.13(a)(2)(i)-(iii); and 42 C.F.R. §485.614(a)(2)(i)-(iii). 4. As noted elsewhere herein, under HIPAA, patients already have the right to file a complaint with the hospital and with the Federal DHHS Office of Civil Rights anytime they believe their HIPAA privacy rights may have been violated, including their right to access their PHI/hospital medical records. Patients are already notified of such right in hospitals' HIPAA Notice of Privacy Practices, required by the HIPAA Privacy Standards. 5. Under Maine's Hospital Licensing Rules, patients are "encouraged" by the Maine DHHS "to resolve complaints directly with the hospital before initiating a department complaint investigation," and "[e]ach hospital must publish a toll-free telephone number for complainants to contact the hospital. Each hospital must educate the public about hospital complaint resolution procedures. At a minimum, each hospital must post information in a public part of the hospital explaining the complaint resolution procedures and

		listing the toll-free complaint telephone number. 10-144 C.M.R. Chapter 112, Sections 4.1 and 4.1.1. Hospitals are provided 45 days to investigate a complaint and to file a report of its investigation with the Maine DHHS. See 10-144 C.M.R. Chapter 112, Section 4.6.3. 6. Under Maine law, patients have the right to notify the Maine Attorney General anytime they believe a hospital may have violated their rights with respect to their health care information, including their right to access their health care information. 22 M.R.S.A. §1711-C(13)(A).
22 M.R.S.A. §1832(2)(G) as set forth in AMENDED LD 2103	21. Coordination with Maine Center for Disease Control and Prevention: "A hospital…must coordinate with personnel from the Maine Center for Disease Control and Prevention and must allow such personnel access to the hospital facility in the event of a cybersecurity intrusion."	1. This provision would impose a NEW requirement on Maine hospitals. 2. What is the rationale for coordinating with the Maine Center for Disease Control and Prevention? Ordinarily, a cybersecurity incident or breach would not fall within the scope of the Maine CDCP's public health functions. 3. Under Maine's Hospital Licensing Rules, the Maine DHHS (and its Division of Licensing and Certification) already has the right to access licensed hospital facilities and to inspect the records thereof. See 10-144 C.M.R. Chapter 112, Sections 2.20 and 2.20.3.
22 M.R.S.A. §1832(2)(H) as set forth in AMENDED LD 2103	22. Confidentiality of Cybersecurity Plans and Audits Submitted to Maine DHHS: "A cybersecurity plan submitted to the [Maine] department [of health and human services]…and the results of an audit submitted to the [Maine] department [of health and human services]…are confidential."	Addressed above in #3 and #19.

Additional Comments:

1. Virtually all of the issues the AMENDED LD 2103 is intended to remedy and prevent going forward are already more than adequately addressed in existing state and federal health care privacy and security laws, rules and regulations.

2. To the extent that a security incident or breach or cyberattack stems from a hospital's failure to have had in place adequate and legally compliant security policies, procedures, measures and safeguards, the issue is one of enforcement of existing health care privacy and security laws and regulations, not the absence of adequate health care security laws, regulations and standards.

3. Remedies already exist for such compliance deficiencies under existing state and federal laws, e.g., via HIPAA complaints to the U.S. Secretary of Health and Human Services, via mandatory breach notification to individuals and to the Secretary of the U.S. DHHS already required under HIPAA, and via state hospital licensing complaints, investigations and surveys.

4. Additionally, under Section 13410(e) of the HITECH Act amendments to HIPAA, state attorneys general also have enforcement authority with respect to violations of HIPAA's privacy and security requirements, the authority to enjoin further violations, and the authority to pursue civil actions and damages on behalf affected Maine patients.