SUMMARY OF EXPRESS TERMS

The proposed regulation would create a new section 405.46 of Title 10 (Health) of the Official Compilation of Codes, Rules and Regulations of the State of New York, to create cybersecurity requirements for all hospital facilities.

Section 405.46 (a) identifies all general hospitals in New York State as subject to the regulations.

Section 405.46 (b) defines certain terms and language for purposes of the section.

Section 405.46 (c) establishes the requirements for hospitals to have a cybersecurity program and defines protocols, procedures, and core functions of such program.

Section 405.46 (d) defines the cybersecurity policies that general hospitals will need to create and the topics that should be considered after a risk assessment has been performed.

Section 405.46 (e) requires general hospitals to designate a Chief Information Security Officer.

Section 405.46 (f) sets forth the requirements for testing and vulnerability of a general hospital's cybersecurity program.

Section 405.46 (g) outlines the audit trails and records maintenance and retention requirements of a general hospital's cybersecurity program.

Section 405.46 (h) sets forth the requirements for cybersecurity risk assessments and the considerations for policies and procedures relative to those risk assessments.

Section 405.46 (i) sets forth the requirements for cybersecurity personnel general hospitals must utilize.

Section 405.46 (j) sets forth the policies for third-party service providers of cybersecurity programs.

Section 405.46 (k) sets forth the requirements for identity and access management.

Section 405.46 (l) sets forth the requirements for training and monitoring of the cybersecurity program.

Section 405.46 (m) defines the requirements for an incident response plan in the event of a cybersecurity incident.

Section 405.46 (n) defines the reporting requirements for a general hospital during a cybersecurity incident.

Section 405.46 (o) refers to confidentiality and the applicability of State and federal statutes.

Section 405.46 (p) provides general hospitals one (1) year from the date of adoption to comply with the new regulatory requirements, except that general hospitals must immediately begin reporting to the Department as required by subdivision (n) of this section.

Section 405.46 (q) states that if any provisions of the section are found to be invalid, it shall not affect or impair the validity of other provisions of the section.

Pursuant to the authority vested in the Commissioner of Health by section 2803 of the Public Health Law, Title 10 (Health) of the Official Compilation of Codes, Rules and Regulations of the State of New York is amended by adding a new section 405.46, to be effective upon publication of the Notice of Adoption in the State Register, to read as follows:

405.46 Hospital Cybersecurity Requirements

(a) Applicability. This section shall apply to all general hospitals licensed pursuant to article 28 of the Public Health Law, referred to throughout this section as "hospitals."

(b) Definitions. For the purposes of this section the following terms shall have the following meaning:

(1) "Authorized user" means any employee, contractor, agent or other person that participates in or operates on behalf of the operations of a hospital and is authorized to access and use any information systems and data of such hospital.

(2) "Control" means any mechanism, safeguard, policy or security measure that is put into place pursuant to implementation specification, to satisfy the requirement for a security measure.

(3) "Compensating Control" means any alternative measure that is put into place to satisfy the requirement for a security measure, where the implementation specification for that requirement is deemed not reasonable or appropriate to implement. The hospital must document why it would not be reasonable and appropriate to implement the implementation specification; and implement an equivalent alternative measure if reasonable and appropriate.

(4) “Cybersecurity event” means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse the hospital’s information system or information stored on such information system, including but not limited to health records.

(5) “Cybersecurity incident” means a cybersecurity event that:

(i) has a material adverse impact on the normal operations of the hospital, or;

(ii) has a reasonable likelihood of materially harming any part of the normal operation(s) of the hospital; or

(iii) results in the deployment of ransomware within a material part of the hospital’s information systems.

(6) “Information system” means a discrete set of electronic information resources organized for the collection, processing, storage, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. One such example is an electronic health records system.

(7) “Multi-factor authentication” means authentication that requires more than one distinct authentication factor for successful authentication. The three authentication factors are:

(i) knowledge factors (i.e. something you know), such as a PIN or a password;

(ii) possession factors (i.e. something you have), such as a cryptographic identification device or a token;

(iii) inherence factors (i.e. something you are), such as a biometric characteristic.

(8) “Nonpublic information” means all electronic information that is not publicly available information and is:

(i) a hospital's business-related information, the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of such hospital;

(ii) Personally identifiable information (PII) including any information concerning a natural person which because of name, number, personal mark, or other identifier can be used to identify such natural person. This includes any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired, in combination with any one or more of the following data elements:

(*a*) social security number;

(*b*) drivers' license number or non-driver identification card number;

(*c*) account number, credit or debit card number in combination with any required security code or access code;

(*d*) password or other information that would permit access to an individual's financial account;

(*e*) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code or password; or

(*f*) biometric information, meaning data generated by electronic measures of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or a username or email address in combination

with a password or security question and answer that would permit access to an online account; or

(ii) Protected Health Information (PHI), as defined under 45 CFR 160.103, including but not limited to, any information or data, in any form or medium created by, held by, transmitted by, or derived from a health care provider or an individual and that relates to:

(a) the past, present or future physical, mental or behavioral health, or condition of any individual or a member of the individual's family;

(b) the provision of health care to any individual; or

(c) payment for the provision of health care to any individual.

(9) “Penetration testing” is a test methodology in which assessors attempt to circumvent or defeat the security features of an information system from outside or inside the hospital’s information systems.

(10) “Privileged account” means any authorized user account or service account that can be used to perform security-relevant functions that ordinary users are not authorized to perform, including but not limited to the ability to add, change or remove other accounts, or make configuration changes to information systems.

(11) “Publicly available information” means any information that a hospital has a reasonable basis to believe is lawfully made available to the general public from widely distributed media; or disclosures to the general public that are required to be made by Federal, State or local law. For the purposes of this paragraph, a hospital has a reasonable basis to believe that information is lawfully made available to the general public if the hospital has taken steps to determine that:

(i) the information is of the type that is available to the general public;

(ii) no individual who could have lawfully objected to the information being disclosed to the general public, has made such a request; and

(iii) disclosure to the general public would not violate other Federal, State, or local government laws, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA).

(12) “Risk assessment” means the risk assessment that each hospital must conduct under subdivision (h) of this section.

(c) Cybersecurity Program Requirements.

(1) Each hospital shall establish within its policies and procedures a cybersecurity program based on the hospital’s risk assessment.

(2) The cybersecurity program shall be designed to perform the following core functions:

(i) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the hospital’s information systems and the continuity of the hospital’s business and operations;

(ii) use defensive infrastructure and the implementation of policies and procedures to protect the hospital’s information systems, the continuity of the hospital’s business and operations, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;

(iii) detect cybersecurity events;

(iv) respond to identified or detected cybersecurity events to mitigate any negative effects;

(v) recover from cybersecurity events and incidents and restore normal operations and services; and

(vi) fulfill applicable statutory and regulatory reporting obligations.

(3) Each hospital's cybersecurity program shall include policies and protocols to limit user access privileges to information systems that provide access to nonpublic information. Each hospital shall periodically review such access privileges, and such access privileges shall be based on the hospital's risk assessment, and other State and Federal laws, including but not limited to the administrative, physical and technical safeguards under HIPAA.

(4) Each hospital's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the hospital, and procedures for evaluating, assessing and testing the security of externally developed applications utilized by the hospital. All such procedures, guidelines and standards shall be annually reviewed, assessed, updated and attested as such by the chief information security officer (CISO) (or a qualified designee) of the hospital.

(5) Each hospital's cybersecurity program shall include policies and procedures for the secure disposal, on a periodic basis, of any nonpublic information identified that is no longer necessary for business operations or for other legitimate business purposes of the hospital, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

(6) Each hospital's cybersecurity program shall implement security measures and controls, including encryption, to protect nonpublic information held or transmitted by the hospital, both in transit over external networks and at rest, which takes into account necessary controls identified in the hospital's risk assessment.

(i) To the extent a hospital determines that encryption of nonpublic information in transit over external networks is infeasible, the hospital shall instead secure such nonpublic information using effective compensating controls reviewed and approved by the hospital's CISO.

(ii) To the extent a hospital determines that encryption of nonpublic information at rest is infeasible, the hospital shall instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the hospital's CISO.

(iii) To the extent that a hospital is utilizing compensating controls under this paragraph, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed and documented by the CISO as needed to continue securing nonpublic information. Such reviews and associated documentation shall be completed at minimum on an annual basis.

(7) Each hospital's cybersecurity program shall implement security controls to mitigate risks arising from electronic mail-based threats, including but not limited to spoofing, phishing, and fraud. Such controls shall be reviewed and updated on a regular basis to ensure their effectiveness against evolving threats.

(d) Cybersecurity policy.

(1) Each hospital shall maintain and implement policies and procedures for the protection of its information systems and nonpublic information stored on those information systems, and the continuity of the hospital's business and operations, in accordance with the hospital's risk assessment and applicable State and Federal laws and regulations. The hospital shall be responsible for developing and enforcing the hospital's cybersecurity policy, and overseeing and implementing the hospital's cybersecurity program, established pursuant to subdivision (c) of this section.

(2) The hospital's cybersecurity policy, upon recommendation by the CISO shall be approved by the hospital's governing body, established pursuant to section 405.2 of this Part. If a committee is established for the specific purpose of supervising the hospital's cybersecurity measures, the

committee shall present the cybersecurity policy to the governing body for full approval and implementation.

(3) The cybersecurity policies shall be based on the hospital's risk assessment and address, at a minimum, the following topics:

(i) information security;

(ii) data governance and classification;

(iii) asset inventory and device management;

(iv) access controls and identity management;

(v) business continuity and disaster recovery planning and resources;

(vi) systems operations and availability concerns;

(vii) systems and network security;

(viii) systems and network monitoring;

(ix) systems and application development and quality assurance;

(x) physical security and environmental controls;

(xi) patient data privacy;

(xii) vendor and third-party service provider management;

(xiii) risk assessment as defined in subdivision (h) of this section;

(xiv) training and monitoring as defined in subdivision (l) of this section; and

(xv) overall incident response as defined in subdivision (m) of this section;

(e) Chief Information Security Officer.

(1) Each hospital shall designate an individual from senior- or executive-level staff, qualified in training, experience, and expertise, to serve as the hospital's Chief Information Security Officer, or "CISO."

(2) Notwithstanding the provisions set forth in subdivision (i) of this section, the hospital's CISO may be an employee of the facility, or an employee of a third-party or contract vendor. If the CISO is an employee of a third-party or contract vendor, the governing body, as defined under section 405.2 of this Part, shall approve the contract on an annual basis.

(3) The CISO of each hospital shall report in writing, at least annually to the hospital's governing body, on the hospital's cybersecurity program and material cybersecurity risks. Such report shall, at minimum include:

(i) the confidentiality of nonpublic information and the integrity and security of the hospital's information systems;

(ii) the hospital's cybersecurity policies and procedures, including their implementation status and any recommendations for revisions;

(iii) material cybersecurity risks to the hospital;

(iv) overall effectiveness of the hospital's cybersecurity program; and

(v) any cybersecurity incidents as defined herein involving the hospital during the time period addressed by the report, as well as steps taken to mitigate future events.

(f) Testing and vulnerability assessments.

(1) The cybersecurity program for each hospital shall include monitoring and testing, developed in accordance with the hospital's risk assessment, designed to assess the effectiveness of the hospital's cybersecurity program and assess changes in information systems that may create or indicate vulnerabilities.

(2) The monitoring and testing shall include at a minimum:

(i) penetration testing of the hospital's information systems by a qualified internal or external party at least annually based upon the hospital's risk assessment;

(ii) automated scans or manual or automated reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the hospital's information systems based on the risk assessment; and

(iii) timely remediation of vulnerabilities based on the risk they pose to the hospital.

(g) Audit Trails and Records Maintenance.

(1) Each hospital shall securely maintain systems that are designed to support normal operations and obligations of the hospital. Records pertaining to systems design, security, and maintenance supporting such normal operations shall be maintained for a minimum of six years.

(2) Each hospital shall also securely maintain systems to include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the hospital, and cybersecurity incidents as defined herein. Records pertaining to such audit trail systems shall be maintained for a minimum of six years.

(3) Designs for the security systems and audit trails required pursuant to paragraphs (1) and (2) of this subdivision shall be based on the hospital's risk assessment.

(h) Risk assessment.

(1) Each hospital shall conduct an accurate and thorough annual risk assessment of the hospital's potential risks and vulnerabilities to the confidentiality, integrity, and availability of nonpublic information, such as electronic protected health information, held by the hospital, and the continuity of the hospital's business and operations, as well as information systems sufficient to inform the design of the cybersecurity program as required by this section. Such risk assessment shall be updated as reasonably necessary, and no less than annually, and address changes to the hospital's information systems, nonpublic information or business operations supported by those

information systems. The risk assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the hospital's business operations, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems. Risk assessments performed for other regulatory purposes, such as HIPAA, shall be acceptable under this provision provided they comport with the requirements herein. Other risk assessments performed for other regulatory purposes, such as HIPAA, may be extended to comply this section and incorporate other risk assessments performed by qualified internal or external parties.

(2) The risk assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall, at a minimum include:

(i) criteria for the evaluation and categorization of identified cybersecurity risks, vulnerabilities, and threats facing the hospital;

(ii) criteria for the assessment of the confidentiality, integrity, security and availability of the hospital's information systems and nonpublic information, including the identification and adequacy of existing controls in the context of identified risks, the determination of the likelihood of threat occurrence and the determination of the potential impact on threat occurrence, and the determination of the level of risk; and

(iii) requirements describing how identified risks and threats will be mitigated or accepted based on the risk assessment and how the cybersecurity policies and programs will address the risks.

(i) Cybersecurity personnel.

(1) Each hospital shall:

(i) utilize qualified cybersecurity personnel of the hospital, an affiliate or a third-party service provider sufficient to manage the hospital's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in subdivision (c) of this section and in accordance with the hospital's risk assessment;

(2) Each hospital may utilize an affiliate or qualified third-party service provider to assist in complying with the requirements set forth in this section.

(j) Security policies for third-party service providers.

(1) Each hospital shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers. Such policies and procedures shall be based upon the hospital's risk assessment and shall, at a minimum, address the following:

(i) the identification and baseline assessment (if applicable) of third-party service providers; and

(ii) minimum cybersecurity practices required to be met by such third-party service providers in order for them to do business with the hospital.

(2) Such policies and procedures shall include relevant guidelines for due diligence and contractual protections relating to third-party service providers, including, at a minimum, guidelines addressing:

(i) ensuring third-party service provider's policies and procedures for access controls are consistent with industry standards;

(ii) the third-party service provider's policies and procedures for use of encryption or another method to protect nonpublic information in transit and at rest;

(iii) notice to be provided to the hospital in the event of a cybersecurity incident directly impacting the hospital's information systems or the hospital's nonpublic information being held by the third-party service provider; and

(iv) representations and warranties addressing the third-party service provider's cybersecurity policies and procedures that relate to the security of the hospital's information systems or nonpublic information.

(k) Identity and Access Management.

(1) Each hospital shall use multi-factor authentication, risk-based authentication, or other compensating control to protect against unauthorized access to nonpublic information or information systems.

(2) Multi-factor authentication shall be utilized for any individual accessing the hospital's internal networks from an external network, unless the hospital's CISO has approved in writing the use of compensating controls.

(3) Each hospital shall limit user access privileges to information systems that provide access to nonpublic information to only those necessary to perform the user's job;

(4) Each hospital shall separate non-privileged and privileged accounts;

(5) Each hospital shall limit the number of privileged accounts and limit the access functions of privileged accounts to only those necessary to perform the user's job;

(6) Each hospital shall limit the use of privileged accounts to only when performing functions requiring the use of such access;

(7) Each hospital shall periodically, but at a minimum annually, review all user access privileges and remove or disable accounts and access that are no longer necessary;

(8) Each hospital shall disable or securely configure all protocols that permit remote control of devices; and

(9) Each hospital shall promptly terminate access following departures.

(l) Training and monitoring.

As part of its cybersecurity program, each hospital shall, at a minimum:

(1) Implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, nonpublic information by such authorized users.

(2) Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the hospital in its risk assessment, which may include annual phishing exercises and training/remediation for employees.

(m) Incident response plan.

(1) As part of its cybersecurity program, each hospital shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity incident materially affecting the confidentiality, integrity or availability of the hospital's information systems or the continuing functionality of any aspect of the hospital's business or operations.

(2) Such incident response plan shall, at a minimum, address the following areas:

(i) the goals of the incident response plan;

(ii) the definition of clear roles and responsibilities, a list of actual personnel and both business hour and off-business hour contact information with levels of decision-making authority;

(iii) external and internal communications and information sharing about any incidents;

(iv) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(v) the internal processes for responding to a cybersecurity event including, at a minimum, mitigation, downtime procedures and contingency plan, and process for determining if a cybersecurity event becomes a cybersecurity incident, and processes for determining if a cybersecurity incident has a material adverse impact on the hospital;

(vi) documentation and reporting regarding cybersecurity events and related incident response activities; and

(vii) the evaluation and revision as necessary of the incident response plan following a cybersecurity event.

(n) Department Reporting.

(1) The hospital or their designee shall notify the department as promptly as possible, but no later than 72 hours after determining a cybersecurity incident, as defined herein, has occurred, in a manner prescribed by the department. Notification to the department under this section does not replace any other notifications required under State or Federal laws or regulations.

(2) Each hospital shall maintain and submit for examination, in such time and manner and containing such information, as the department determines to be necessary, including but not limited to any and all documentation, such as records, schedules, reports, and data required and supporting the required documentation by this section. All such documentation must be maintained for a minimum of six years.

(3) To the extent a hospital has identified areas, systems or processes that require material improvement, updating or redesign, the hospital shall document the identification and the remedial efforts planned, and underway, to address such areas, systems or processes. Such documentation must be available for inspection by the department, in such time and manner as prescribed by the department, and must be maintained for a minimum of six years.

(o) Confidentiality.

Information provided by a hospital pursuant to this Part shall be subject to the applicable provisions of the Public Health Law, Mental Hygiene Law, Education Law, and the Public Officers Law or any other applicable State or Federal law or regulations in relation to disclosure.

(p) Compliance period.

(1) Covered entities shall have one year from the effective date of this section to comply with the requirements set forth herein, provided, however, subdivision (n) of this section shall be effective immediately upon adoption.

(q) Severability.

If any provision of this section or the application thereof to any person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this section or the application thereof to other persons or circumstances.

REGULATORY IMPACT STATEMENT

Statutory Authority:

Public Health Law (PHL) § 2803(2)(a) authorizes the Public Health and Health Planning Council (PHHPC) to adopt and amend rules and regulations, subject to the approval of the Commissioner of Health (Commissioner), to implement PHL Article 28 and establish minimum standards for health care facilities, including general hospitals.

Legislative Objectives:

The legislative objectives of PHL Article 28 include the protection of the health of the residents of the State by promoting the efficient provision and proper utilization of high-quality health services at a reasonable cost.

These regulations fulfill this legislative objective by ensuring that general hospitals within New York State implement minimum cybersecurity controls to safeguard protected health information (PHI) and personally identifying information (PII) from being publicly disclosed or used for identity theft.

Needs and Benefits:

The healthcare industry is one of the most targeted communities for cybersecurity scams and breaches due to the significant amount of sensitive and financially lucrative information healthcare facilities collect. Currently in New York State there are no cybersecurity requirements for the safeguarding and security of patients' protected health information (PHI) and personally identifying information (PII). As a result, New Yorkers seeking medical care

have no guaranteed minimum levels of protection of their information. As a result of this, there have been several high-profile cybersecurity breaches at facilities across the state which have resulted in not only a loss of patient financial and health data, but in some cases has also delayed care.

Additionally, cybersecurity events at hospitals can have significant, far-reaching, and long-term impacts to the provision of patient care and operation of the facility. Governor Hochul has been focusing on cybersecurity and ensuring that New Yorkers data stays safe no matter where they go. The promulgation and implementation of cybersecurity focused regulations supports this initiative. These regulations will ensure all hospitals develop, implement, and maintain minimum cybersecurity standards, including cybersecurity staffing, network monitoring and testing, policy and program development, employee training and remediation, incident response, appropriate reporting protocols and records retention.

There will be multiple benefits to the adoption of these regulations. Given the significant differences in preparedness statewide against cybersecurity attacks, these regulations will ensure hospitals are required to maintain a minimum level of readiness to prepare for, respond to, and quickly recover from cybersecurity incidents.

Costs:

Costs to Regulated Parties:

The costs associated with the implementation by regulated facilities will vary significantly due to the varying levels of cybersecurity programs and policies hospitals currently have in place. Some facilities may have mature monitoring, training and response programs, whereas others may not. Therefore, the costs could vary from tens of thousands to tens of millions. Hospitals will be allowed to sub-contract for cybersecurity services and this may reduce

the overall cost of program implementation. It is estimated that effective cybersecurity programs can cost between $250,000 and $10 Million to develop and implement initially and anywhere from $50,000 - $2 Million or more to maintain on a yearly basis depending on the facility size. For small hospitals (of which there are 15 and are defined as less than 10 acute care or ICU beds), ongoing annual costs are estimated to be $50,000-$200,000. For medium sized hospitals (of which there are 62 and are defined as those with between 10 and 100 beds), ongoing costs are estimated to be $200,000-$500,000. For large hospitals (of which there are 114 and are defined as those with more than 100 beds), ongoing annual costs are estimated to be $2 million.

Costs to Local and State Governments:

There are currently fifteen facilities which would be subject to these proposed regulations which are operated by local municipalities. As such, they would be subject to the same regulations as those operated by private entities. The estimated costs they would incur would depend on their size, as noted above.

Local Government Mandates:

These regulations do impose a program, service, duty or other responsibility upon 4 separate city, county and State governments to the extent they do not already comply with the proposed regulations.

Paperwork:

These regulations impose additional paperwork in the form of procedures, policies, guidelines, and reporting documents. These requirements are necessary to ensure the efficacy of a cybersecurity program and also provide accountability and transparency for hospitals.

Duplication:

There is no duplication of this initiative in existing State law. The Heath Insurance Portability and Accountability Act (HIPAA) Security Rule does provide broad requirements for safeguarding PHI, but the regulations contained herein are intended to supplement HIPAA.

Alternatives:

The alternative to the proposed regulation would be not enacting the cybersecurity requirements. This option is not appropriate due to the demonstrated need to protect PHI and PII at hospitals within the State. The Department in 2023 has responded to more than 1 cybersecurity incident per month, several of which have forced hospitals to go on diversion, stopped their billing procedures, and required facilities to operate on downtime procedures which can severely hamper the care delivery process. Over 225,000 patients had data possibly compromised in one breach alone.

In order to respond to comments received by facilities, the proposed regulations were modified to lengthen and simplify the compliance period in order to maximize the ability for facilities to come into compliance. Furthermore, the Department removed the requirement for a Chief Information Security Officer to be employed directly by the facility, and instead allow them to be a virtual or 3rd party vendor upon approval by the facilities' governing body.

Federal Standards:

Federal regulations governing protection of PHI and PII are contained within HIPAA, however they are overly vague and provide limited guidance on cybersecurity and the protection of PHI and PII.

Compliance Schedule:

General hospitals will have one year from the effective date of the regulation to comply with the requirements set forth herein. However, subdivision (n) of the regulation, requiring general hospitals to notify the department as promptly as possible, but no later than 72 hours after determining a cybersecurity incident, as defined herein, has occurred, will be effective upon adoption in the State Register. The schedule as proposed was modified as a direct result of outreach to facilities by the Department who provided feedback on the difficulty in developing cybersecurity programs.

Contact Person:

Katherine E. Ceroalo
New York State Department of Health
Bureau of House Counsel, Regulatory Affairs Unit
Corning Tower Building, Rm. 2438
Empire State Plaza
Albany, New York 12237
(518) 473-7488
(518) 473-2019 (FAX)
REGSQNA@health.ny.gov

REGULATORY FLEXIBILITY ANALYSIS FOR SMALL BUSINESSES AND LOCAL GOVERNMENTS

Effect of Rule:

The proposed regulations will affect all general hospitals licensed pursuant to Article 28 of the Public Health Law, regardless of size or location. There are currently 226 hospitals in New York State, including Veteran's Affairs facilities (which would not be affected by these proposed regulations). These regulations will not affect local governments unless they operate a general hospital. In NYS, there are 15 hospitals operated by municipalities; Lewis County Hospital in Lewis County, NY, Wyoming County Hospital in Wyoming County, 12 facilities operated by New York City Health and Hospitals Corporation, and Helen Hayes hospital operated by the State of New York.

Currently in New York State there are no cybersecurity requirements for the safeguarding and security of patients' protected health information (PHI) and personally identifying information (PII). As a result, New Yorkers seeking medical care have no guaranteed minimum levels of protection of their information. As a result of this, there have been several high-profile cybersecurity breaches at facilities across the state which have resulted in not only a loss of patient financial and health data, but in some cases has also delayed care. Additionally, cybersecurity events at hospitals can have significant, far-reaching, and long-term impacts to the provision of patient care and operation of the facility. These regulations will ensure all hospitals develop, implement, and maintain minimum cybersecurity standards, including cybersecurity staffing, network monitoring and testing, policy and program development, employee training and remediation, incident response and appropriate reporting protocols and records retention.

Compliance Requirements:

The proposed regulations require that hospitals develop, implement and maintain minimum cybersecurity standards and programs, including information technology (IT) staffing, network monitoring and testing, policy and program development, employee training and remediation, incident response, appropriate reporting protocols and records retention.

Professional Services:

Depending on the current state of an existing cybersecurity program, a facility or system may need to contract with a third-party service provider for anything from staffing, network monitoring, incident response, or staff training. Facilities will be required to hire or appoint a Chief Information Security Officer (CISO). The draft regulations currently allow for the CISO to be a direct employee of the facility, or an employee of a virtual or third-party contractor upon consent and approval of the governing body. Facilities may also need to hire or contract additional information technology staff to ensure compliance with the new regulations. Additionally, the facilities may need to purchase information security programs or contract with third-party vendors to monitor for malicious network traffic, perform compliance testing with authorized users and ensure protected health information and personally identifying information is kept secure.

Compliance Costs:

Given the variability in cybersecurity preparedness and current programs at facilities, the initial startup and ongoing costs could vary significantly. After initial conversations with facilities to gain a basic understanding of costs, it is estimated that effective cybersecurity

programs can cost millions to develop and implement initially, and anywhere from $50,000-$2 million or more to maintain on a yearly basis depending on the facility size. For small hospitals (of which there are 15 and are defined as less than 10 acute care or ICU beds), ongoing annual costs are estimated to be $50,000-$200,000. For medium sized hospitals (of which there are 62 and are defined as those with between 10 and 100 beds), ongoing costs are estimated to be $200,000-$500,000. For large hospitals (of which there are 114 and are defined as those with more than 100 beds), ongoing annual costs are estimated to be $2 million.

Economic and Technological Feasibility:

It is both economically and technologically feasible for hospitals to become compliant with the proposed regulations. There currently exists a significant amount of technology and software which can be licensed or purchased to provide network monitoring, notification, staff training and exercises and multifactor or risk-based authentication, among others. Economically, it will be easier for hospitals which are part of large healthcare systems or located in more urban areas to comply with these regulations than it may be for smaller or more rural facilities. This is due to the fact that the larger facilities and systems may already have aspects of the regulations already functioning as part of a mature cybersecurity program, or may have access to more capital and resources than smaller, more rural or standalone facilities. While several facilities voiced concerns related to the cost of implementation, the consequences of what can occur as a result of a cyber-attack far outweigh those costs. Days or weeks of downtime with an inability to bill for services can cost tens of millions of dollars (at a minimum), as well as the unknown cost of lost productivity, cancellation of elective surgeries, purchase of new computers, etc, can well exceed the yearly maintenance program costs.

Minimizing Adverse Impact:

The Department of Health conducted several rounds of outreach to affected healthcare facilities and healthcare associations as part of the regulatory drafting process, to understand what makes a successful cybersecurity program, what things should be avoided or be flexible, and how the Department can work with them to enhance preparedness in New York State. As a result of those discussions, the Department took significant steps to ensure that no specific references to technology, programs or software were included into the regulations. In this way, it allows for facilities to become compliant with the regulations however they may be able to, without the regulation becoming too prescriptive, or requiring use of overly expensive or specific software. These regulations establish truly baseline, general requirements that allow maximum flexibility to healthcare facilities to comply based on their operations. While other approaches to cybersecurity programs were considered, as required under SAPA § 202-b(1), there are unfortunately no alternatives to cybersecurity, as the health and welfare of patients both current and former at a facility can be adversely affected by a network breach. Facilities will have one year from implementation to come into compliance with the regulations except for incident reporting. The compliance period as proposed will not only maximize the ability for facilities to come into compliance, but was modified as a result of feedback received from those facilities. While these regulations will result in some cost to facilities, the Department will be taking action to mitigate these impacts. In January of this year, the Department released Statewide IV and Statewide V funding totaling $650 million to assist with implementation of, and compliance with, the regulatory requirements. This funding was appropriated in the SFY 24 budget with the intention of supporting facilities' technological needs, including for cybersecurity purposes.

Small Business and Local Government Participation:

During the drafting process, the Department conducted several rounds of outreach to over 25 different hospitals and hospital/healthcare associations to understand the current state of the industry, cybersecurity program best practices and areas to avoid.

Parties the Department reached out to:
University of Rochester MC
Kaleida Health
Northwell Health
NY Presbyterian
Elizabethtown Hospital
Arnot Ogden MC
Geneva General Hospital
Soldiers and Sailors Memorial Hospital
Rochester General Hospital
Unity Hospital
Wyoming County Hospital
Richmond University Medical Center
Healthcare Association of NYS
Iroquois Healthcare Association
Healthcare Association of Central and Western NY
Suburban Hospital Alliance of NYS
Greater NY Healthcare Association

As there are facilities run by city, county and state municipalities, a cross section of them was invited to participate in the roundtable discussion related to cybersecurity programs and proposed regulations. The Department has some direct communication methods through the Health Commerce system which will be utilized to reach out to C Suite executives at each facility after the regulations are publicly posted and available for comment.

RURAL AREA FLEXIBILITY ANALYSIS

Types and Estimated Numbers of Rural Areas:

Rural areas as defined by Executive Law § 418(7) are counties with a population less than 200,000 and towns with a population density less than 150 people per square mile. For the purposes of this regulation, there are 44 counties with a population of less than 200,000, which have a total of 76 regulated facilities. The proposed rule will apply statewide to all general hospitals regulated under Article 28 of the Public Health Law.

Reporting, Recordkeeping and Other Compliance Requirements; and Professional Services:

1. Recordkeeping- Article 28 facilities will be required to develop cybersecurity policies, protocols and procedures within one year of the adoption of the proposed regulations. Facilities will be required to maintain records of program compliance by employees, security breaches by outside entities (both successful and unsuccessful), and other program documentation for at least 6 years.
2. Reporting: Article 28 facilities will be required to report any cybersecurity incidents, as defined in the proposed regulation, as promptly as possible, but no later than 72 hours after determining a cybersecurity incident has occurred. Facilities will also be required to provide a report to the Department upon request of all cybersecurity incidents within the previous reporting period.
3. Professional services- Facilities will be required to hire or appoint a Chief Information Security Officer (CISO). The draft regulations currently allow for the CISO to be a direct employee of the facility, or an employee of a virtual or third-party contractor upon consent and approval of the governing body. Facilities may also need to hire or contract

additional information technology staff to ensure compliance with the new regulations. Additionally, the facilities may need to purchase information security programs or contract with third-party vendors to monitor for malicious network traffic, perform compliance testing with authorized users and ensure protected health information, personally identifying information, and nonpublic information is kept secure.

Costs:

The costs for this program will vary depending on the level of preparedness of each facility. For less mature programs which require significant development, the initial funding required could range from $250,000 to $10 million. For small hospitals (of which there are 15 and are defined as less than 10 acute care or ICU beds), ongoing annual costs are estimated to be $50,000-$200,000. For medium sized hospitals (of which there are 62 and are defined as those with between 10 and 100 beds), ongoing costs are estimated to be $200,000-$500,000. For large hospitals (of which there are 114 and are defined as those with more than 100 beds), ongoing annual costs are estimated to be $2 million. Facilities may be able to purchase equipment or services from State Contract lists where appropriate and applicable. Facilities will also be able to contract with appropriate third-party vendors or contractors to help ensure compliance with the proposed regulations.

Minimizing Adverse Impact:

The Department has included flexibility within the regulations for facilities to ensure they are compliant with the requirements, including allowing for third-party or vendor contractors to complete compliance reporting and measures on behalf of them. Additionally, facilities will have

one year from the adoption of the proposed regulations to implement the requirements and ensure compliance. While these regulations will result in some cost to facilities, the Department will be taking action to mitigate these impacts. In January of this year, the Department released Statewide IV and Statewide V funding totaling $650 million to assist with implementation of, and compliance with, the regulatory requirements. This funding was appropriated in the SFY 24 budget with the intention of supporting facilities' technological needs, including for cybersecurity purposes.

Rural Area Participation:

In consideration of SAPA § 202-bb(7), the Department conducted multiple rounds of outreach with facilities of a diversity of sizes, including those located in rural areas such as Ellenville Regional Hospital and Arnot Ogden Medical Center. This outreach consisted of one-on-one conference calls with specific facilities, which occurred June 12-22, 2023, as well as a roundtable in August 2023 where over 25 facilities, healthcare associations and Department of Health staff were invited to discuss the current state of cybersecurity programs, best practices and required elements of a good cybersecurity program. While many facilities agreed about the need for mature cybersecurity program amid increasing cybersecurity threats, many voiced concerns about the costs of these programs. The Department listened to all of the feedback provided and modified some of the language in the proposed regulations. For example, the Department simplified and lengthened the compliance period to allow facilities the maximum amount of time to be in compliance.

STATEMENT IN LIEU OF JOB IMPACT STATEMENT

A Job Impact Statement for these amendments is not being submitted because it is apparent from the nature and purpose of the amendments that they will not have a substantial adverse impact on jobs and/or employment opportunities.

ASSESSMENT OF PUBLIC COMMENT

Comment: Two commenters stated that the definition of non-public information expands beyond a hospital's primary objective, which is patient care. The commenters recommended limiting the definition to protected health information (PHI) and personally identifying information (PII).

Response: The proposed regulation aims to enhance the overall cybersecurity resilience of hospitals in New York and preparedness statewide against cybersecurity attacks. The scope of the regulations extends beyond the protection of PHI and PII data to cover the systems that support the continuity of patient care across the hospital ecosystem. No substantial changes were made to the proposed regulation as a result of these comments; however, the Department made minor revisions to the definition of non-public information to explicitly mention PHI and PII.

Comment: One commenter recommended that the regulations align with existing controlling cybersecurity standards. They suggested that the less confusing and more economical approach is to incorporate by reference controlling rules and standards. The commenter took an example of multi-factor authentication (MFA) and stated that there is an industry standard toward requiring a stronger level of MFA that is more resistant to phishing attacks so the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) will likely update their definitions. The commenter suggested using incorporation by reference in the regulations so that the Department will not have to update definitions as and when federal standards are amended.

Response: The Department will consider these comments in future rulemaking if there are significant changes to federal regulations. The Department anticipates publishing a document mapping the requirements in the regulations to existing NIST and Cybersecurity Performance Goals (CPG) standards. As a result of this comment, the definition of multi-factor authentication (MFA) has been amended to remain in alignment with future changes in federal rulemakings or industry standards.

Comment: One commenter recommended adding Endpoint Detection Response (EDR) as a requirement to the regulation as it can be leveraged to perform multiple cybersecurity tasks and be used to develop a comprehensive, risk-based cybersecurity strategy. The commenter also suggested including practical security practices in the regulations such as logging, threat hunting and machine-learning based prevention provided by next-gen SIEM solutions.

Response: The Department understands that EDR is an important tool in any organization's cybersecurity program. However, listing a specific tool such as EDR, or any other industry standard tool is out of scope of this regulation. Appropriate tool selection should be aligned to a hospital's risk assessment. No changes to the proposed regulation were made as a result of this comment.

Comment: Two commenters requested clarification on what specific cybersecurity incident logs must be maintained by hospitals and recommend including the necessary key languages in the regulatory texts. One commenter stated that this requirement could be read as requiring hospitals to maintain log data of all security incidents which may potentially increase cost for hospitals.

Response: The proposed regulation states that "*Each hospital shall also securely maintain*

systems to include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the hospital, and cybersecurity incidents as defined in subdivision (b) of this section." The regulation only requires hospitals to retain logs from cybersecurity incidents that had a material adverse impact on the hospital, and therefore were required to be reported to the Department. No changes to the proposed regulation were necessary as a result of these comments.

Comment: Two commenters stated their opinion on third-party service provider cybersecurity requirements. One commenter mentioned that the third-party service provider requirements are prescriptive, requiring hospitals to ensure their vendors meet certain requirements, including the following: maintaining policies and procedures for access controls that are consistent with industry standards; maintaining policies and procedures addressing encryption; providing notice in the event of a cyber incident; and providing representation and warranties to the hospital about their cybersecurity posture. One commenter stated that these requirements go beyond controlling cybersecurity standards and requested that the Department amend the regulation to remove the prescriptive requirements. Another commenter recommended that minimum standards be adopted for third-party vendors, as hospitals may lack leverage with them when demanding contract terms specified in the regulations.

Response: The third-party vendor requirements in the regulations are minimum cybersecurity best practices, widely utilized across industries. These requirements are essential to maintain a hospital's security resiliency while contracting with third-party vendors. Hospitals shall conduct risk assessments and further detail third-party security policies and procedures based on their size, scope and security posture. No changes to the proposed regulation were made as a result of

these comments.

Comment: One commenter recommended hospitals to implement Zero Trust Architecture in addition to multi-factor authentication (MFA) because, according to the commenter, it radically reduces or prevents lateral movement and privilege escalation during a compromise and can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

Response: The Department understands the value of Zero Trust Architecture. Adoption of Zero Trust Architecture should be based on hospital risk assessment and feasibility of implementation. No changes to the proposed regulation were made as a result of this comment.

Comment: Three commenters appreciated the Department revising the Department reporting timeline from two hours to 72 hours.

Response: The Department appreciates these comments in support of the regulation.

Comment: One commenter requested that the regulations include a more thoughtful approach to Department reporting and suggested introducing some leniency if a covered entity is unable to submit a required report. They also suggested the Department conduct a crosswalk between the information it receives via Health-ISAC and that which is being requested from hospitals via the regulations, and consider ways to ensure non-duplicative reporting.

Response: The purpose of this regulation is to ensure continued functioning of patient care and hospital operations. The 72-hour timeframe has been defined specifically for material incidents, and reporting within this time will allow the Department to setup health emergency response and limit exposure to other NYS entities.

The Department is a member of several Information Sharing and Analysis Centers (ISAC). The data normally distributed by ISACs are useful in responding to cybersecurity incidents; however, the Department requires additional data points in its reporting requirements to prioritize health emergency responses and ensure continuity of patient care services and hospital operations. The Department will continue to have discussions with the ISACs and other partner organizations to explore efficient and effective reporting and incident response. No changes to the proposed regulation were made as a result of this comment.

Comment: One commenter stated that the proposed regulations conflict with HIPAA regulations when it comes to the appointment of a CISO, as the HIPAA security rule states that covered entities must identify a security official to develop security policies, and the HIPAA privacy rule states that covered entities must appoint a privacy official, who, in most cases, is the Security Officer.

Response: The regulations state "*The hospital's cybersecurity policy, upon recommendation by the CISO shall be approved by the hospital's governing body, established pursuant to section 405.2 of this Part. If a committee is established for the specific purpose of supervising the hospital's cybersecurity measures, the committee shall present the cybersecurity policy to the governing body for full approval and implementation.*" The hospital's policies will be reviewed by the CISO; however, the approval will happen only by the hospital's governing body comprising of stakeholders within the hospital such as the Chief Privacy Officer (CPO) and other senior-level executives such as the Chief Compliance Officer and the Chief Risk Officer. No changes to the proposed regulation are necessary as a result of this comment.

Comment: One commenter stated that there may be a conflict with Social Services Law § 363-d and 18 NYCRR Part 521 and also mentioned that some of the roles and responsibilities of the CISO listed in the proposed regulations conflict with the roles of other senior professionals within the administrative construct of hospitals throughout the State such as the Chief Compliance Officer, Chief Privacy Officer or Chief Risk Officer.

Response: The regulations state that the responsibility of publishing policies falls under the hospital's governing body. The hospital CISO shall recommend and review cybersecurity policies in collaboration with other stakeholders within the hospital, such as the CPO and other senior-level executives such as the Chief Compliance Officer and the Chief Risk Officer. No changes to the proposed regulation are necessary as a result of this comment.

Comment: One commenter stated that managed care organizations that are subject to the proposed regulations and 18 NYCRR Part 521, are also subject to 23 NYCRR Part 500. The commenter stated that given the requirements of 23 NYCRR Part 500, as well as the requirements of 18 NYCRR Part 521, it may be difficult for managed care companies to fulfill 23 NYCRR Part 500, 18 NYCRR Part 521, and the proposed regulations.

Response: The proposed regulations only apply to Article 28 general hospitals and not to managed care organizations. Nevertheless, the Department does not foresee any conflict between the regulations cited by the commenter and therefore no changes to the proposed regulation were made as a result of this comment.