KATHY HOCHUL
Governor

ADRIENNE A. HARRIS
Superintendent

NEW YORK STATE
INDEPENDENT DISPUTE RESOLUTION ENTITY
APPLICATION

Issue Date: November 23, 2022

Applicant Questions Due No Later Than: November 30, 2022

DFS Responses Due: December 7, 2022

Application Due No Later Than: 5:00 PM EST January 4, 2023

One Commerce Plaza
Albany, NY 12257

New York State Department of Financial Services

NEW YORK STATE INDEPENDENT DISPUTE RESOLUTION ENTITY APPLICATION

The process to become an independent dispute resolution entity ("IDRE") is governed by Article 6 of the New York Financial Services Law ("Financial Services Law") and its implementing regulations (23 NYCRR Part 400). Applicants must complete the following forms and provide all requested information to be evaluated for possible certification as an IDRE.

Certifications will be awarded based on the completeness of the application, the quality of the application responses, and the fees reflected in the application. Multiple certifications will be awarded, with the exact number based on the needs of the program.

Instructions: When completing this IDRE application, provide current information. Respond to all questions in consecutive order, complete the checklist at the end of the application, and ensure that responses correspond to the letters and numbers below. Attach additional pages as necessary. Submit by mail to Consumer Assistance Unit, NYS Department of Financial Services, One Commerce Plaza, Albany, New York 12257 or by e-mail to IDRQuestions@dfs.ny.gov . ***If submitting an application via overnight delivery, please also provide notice of the application submission to the IDRQuestions@dfs.ny.gov email address.***

Applicants should refer to Financial Services Law Article 6 and 23 NYCRR Part 400 for definitions and details about the New York State independent dispute resolution ("IDR") process.

Applications must be submitted to and received by the New York State Department of Financial Services ("Department") by 5:00 PM EST on January 4, 2023.

Prohibition on certification:

Any entity that owns or controls; is owned or controlled by; or is under common control with (1) any national, state or local illness, health benefit, or public advocacy group; (2) any national, state or local society or association of hospitals, physicians, or other providers of health care services; or (3) any national, state or local association of health care plans, is prohibited from being certified as an IDRE in New York. *A potential applicant should not complete and submit this application if the potential applicant owns or controls, is owned or controlled by, or is under common control with any of the prohibited organizations.*

_____

Business Name of Applicant

_____

Address

_____

City State Zip

_____

Telephone Number (Area Code First) Fax Number

_____

Name of Chief Executive Officer

_____

Address (if different from above)

_____

City State Zip

_____

Telephone Number (Area Code First) Fax Number

I. ORGANIZATION AND MANAGEMENT

Organizational Structure:

Describe the organizational structure of the applicant and its ability to operate a statewide IDRE, including:

A. Provide the certificate of incorporation, articles of organization, and bylaws or operating agreement of the applicant and, as applicable, those of the proposed applicant's holding company or parent company.

B. Provide the names of all corporations and organizations that control, are controlled by, or are under common control with the applicant, and the nature and extent of any such control.

C. Provide the organizational chart or lines of authority within the applicant organization, holding company, or parent entity.

D. Describe any licensure or certification for similar programs in other states.

Management:

E. Identify applicant's management staff and include a description of the responsibilities of any management staff member who will be involved in the IDR process. Each person identified in this section must complete and submit Attachment 1 of the application.

F. Provide the name and credentials of a medical director appointed by the applicant, who is a physician in possession of a current and valid non-restricted license to practice medicine in the State of New York. The medical director shall complete and submit Attachment 1 of the application.

G. Provide the names and biographies of all controlling employees, officers, and executives of the applicant and information concerning the governing board of applicant, including roles and responsibilities, identification of the board members, and a description of their qualifications, including their education, skills, and experience. Each person identified in this section must complete and submit Attachment 1.

Accreditation:

H. Provide documentation that the applicant is currently accredited by a nationally recognized private accrediting organization.

II. CONFLICT OF INTEREST

Applicant:

A. The Chief Executive Officer must complete and submit a notarized conflict of interest attestation (Attachment 3) on behalf of the corporate entity, and of all the corporate entity's owners, directors, officers, managers, and medical director.

B. Provide a chart listing any material professional, financial, or familial affiliation the applicant, owners, officers, directors, management employees, or the medical director, have with: any health care plan; any owner, officer, director, or management employee of a health care plan; any health care provider, physician's medical group, independent practice association, or provider of pharmaceutical products or services or durable medical equipment; any facility at which health care services would be provided; any officer, director, partner or manager of a physician's medical group, independent practice association, or facility at which a health care service would be provided; or any developers or manufacturers of health services or products.

C. Describe the procedures the applicant has to ensure that a dispute will not be assigned to a reviewer or reviewing health care provider who has a material familial, financial, or professional affiliation with any of those persons listed in 11 NYCRR 400.4(d).

Following Certification as an IDRE:

If an IDRE acquires control of, becomes controlled by, or comes under common control with any national, state, or local illness, health benefit or public advocacy group; any national, state or local society or association of hospitals, physicians, or other providers of health care services; or any national, state or local association of health care plans, the IDRE shall notify the New York State Superintendent of Financial Services ("Superintendent") in writing, with a copy to IDRQuestions@dfs.ny.gov, within three business days of the acquisition or exercise of control. Such notification will render the entity's certification to act as an IDRE void.

III. CONTRACTED SERVICE PROVIDERS

A. Provide a description of the reviewer and reviewing health care provider networks, including:

1. An assessment of the applicant's ability to provide review services statewide.

2. A description of the qualifications of the reviewers and reviewing health care providers retained to review payment disputes including current and past employment history and practice affiliations, as applicable.

3. A description of the procedures to be employed to ensure that reviewers and reviewing health care providers reviewing payment disputes are:

    a. appropriately licensed, registered or certified, if applicable;
    b. trained in the principles, procedures and standards of the applicant;
    c. knowledgeable about the health care service that is the subject of the payment dispute under review; and
    d. with respect to reviewers, trained and experienced in health care billing, reimbursement and usual and customary charges.

B. Complete Attachment 2 providing the number of reviewers and reviewing health care providers retained by the applicant, a description of the areas of expertise available from reviewing health care providers, and the types of cases reviewing health care providers are qualified to review.

IV. QUALITY ASSURANCE AND CONFIDENTIALITY

A. Describe the applicant's quality assurance program. This should include written descriptions of the organizational arrangements and ongoing procedures for the identification, evaluation, resolution, and follow-up of potential and actual problems in payment dispute reviews performed by the reviewer and reviewing health care provider; and the maintenance of program standards pursuant to 23 NYCRR 400.3(a).

B. Provide a copy of written procedures documenting that:

1. Appropriate personnel are accessible not less than 40 hours per week during normal business hours to discuss the dispute resolution process and to allow response to telephone requests; and

2. A response to an accepted or recorded message will be made not less than one business day after the date on which the call was received.

C. Describe the applicant's ability to accept requests for reviews, provide requisite notifications, screen for material affiliations, respond to calls from the Department and meet other requirements during normal business hours.

D. Describe the policies and procedures to ensure the confidentiality of medical and treatment records and review materials.

V. IDR PROCESS

A. Describe the applicant's methods of recruiting and selecting neutral and impartial reviewers and reviewing health care providers and matching such reviewers and reviewing providers to specific cases.

B. Describe and provide a chart or diagram of the sequence of steps for dispute resolution, from receipt of the dispute through notification to the health care plan, health care provider, Superintendent, and provider, insured, or patient, if applicable, of the dispute determination.

C. Provide a copy of procedures for ensuring that no prohibited material familial, financial or professional affiliation exists with respect to the reviewer and reviewing health care provider assigned to the dispute. The procedures shall include, for each reviewer and reviewing health care provider assigned to review a dispute, a requirement for a signed attestation affirming, under penalty of perjury, that no prohibited material familial, financial or professional affiliation exists with respect to the reviewer's or reviewing health care provider's participation in the review of the dispute.

D. Provide a copy of procedures to ensure that the dispute is reviewed by a neutral and impartial reviewer with training and experience in healthcare billing, reimbursement, and usual and customary charges and that determinations are made in consultation with a neutral and impartial licensed reviewing health care provider in active practice in the same or similar specialty as the health care provider providing the service that is subject to the dispute. For disputes involving physician services, the reviewing health care provider must be a physician in active practice in the same or similar specialty as the physician providing the services who is also, to the extent practicable, licensed in New York.

E. Provide a copy of procedures for the reporting and review of reviewer's and reviewing health care provider's conflicts of interest and for assigning or reassigning a dispute resolution where a conflict or potential conflict is identified.

F. Provide a copy of procedures to ensure that reviews are conducted within the time frames specified in 23 CRR-NY § 400.8 and that any required notices are provided in a timely manner.

G. Provide a description of the applicant's methodology to determine whether the provider's billed charge or the health plan's payment is the more reasonable fee for the services rendered.

H. Provide a copy of procedures to ensure adherence to the requirements of 23 NYCRR Part 400 by any contractor, subcontractor, agent or employee affiliated by contract or otherwise with the proposed IDRE.

I. Provide sample copies of all correspondence that will be sent to health plans, providers, and patients during the course of an IDR review.

J. Provide a copy of the procedures to ensure the applicant will incorporate any updates to Article 6 of the Financial Services Law and 23 NYCRR Part 400 into their processes.

VI. RECORD RETENTION, COMPLIANCE AND INFORMATION SYSTEMS:

A. Describe the applicant's procedures to meet all record retention and compliance requirements set forth in 23 NYCRR § 400.9.

B. In accordance with Attachment XX, provide details on the following items, including all applicable protocols, controls and systems:

1. How will confidential and sensitive data be transmitted to and received by the applicant?

2. How will confidential and sensitive information be protected while in the applicant's custody?

3. How will sensitive information be disposed by the applicant once data retention requirements are met?

VII. FINANCIAL ARRANGEMENTS:

A. Provide the following current financial data:

1. Statement of Revenues and Expenses;

2. Balance Sheet;

3. Methods to repay any indebtedness; sources of capitalization and documentation of accounts, assets, reserves and deposits; and

4. A Certified Financial Statement.

B. Provide a chart with the current fees the applicant will charge for conducting IDR proceedings in accordance with 23 NYCRR § 400.10 The chart shall include the pro-rated fee that will be charged when a good faith negotiation directed by the applicant results in a settlement between the health care plan, non-participating hospital and the non-participating physician, non-participating hospital, or non-participating referred health care provider. The chart shall also include an application processing fee when the dispute is determined by the applicant to be ineligible for review.

Also confirm that the applicant will waive the fee for disputes submitted by patients when the fee would pose a financial hardship to the patient.

	Fee
Full Review	$
Processing Fee for Ineligible Applications	$
Pro-Rated Fee Due to Good Faith Negotiation Resulting in Settlement Agreement	$

Note: All fees shall reflect the total amount that will be charged. Indirect costs, administrative fees and incidental expenses shall be included within the rates in the chart. A fee may not be charged unless it has been filed with the Superintendent and the Superintendent has determined that the fee is reasonable.

C. Describe the applicant's methodology to calculate each of the above fees.

WHEN SUBMITTING YOUR APPLICATION, THIS PAGE MUST BE SUBMITTED IN A SEPARATE SEALED ENVELOPE LABELED AS "COST CHART". IF SUBMITTING VIA OVERNIGHT DELIVERY, SUBMIT THIS COMPLETED PAGE AS A SEPARATE DOCUMENT LABELED AS "COST CHART".

The Department reserves the right to request additional information to evaluate this application.

I hereby attest to the accuracy of the information and the statements made in this application to correctly describe the business practices of my organization, and agree that, if my organization is selected for certification as an IDRE, the organization will comply with all obligations in this application, including its attachments:

_____

Signature of CEO Date:

STATE OF)
SS:
County of)

On this ____ day of _____, 20__, before me personally appeared

_____, to me known and known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that he/she resides at _____, and further that:
he/she is a duly authorized member of _____ , the company described in said instrument; that, he/she is authorized to execute the foregoing instrument on behalf of the company for purposes set forth therein; and that, pursuant to that authority, he/she executed the foregoing instrument in the name of and on behalf of said company as the act and deed of said company.

_____
Notary Public
Registration Number: _____ State of _____

Checklist for IDRE Application	Documents or Acknowledgement Attached
I. ORGANIZATION AND MANAGEMENT	
Organizational Structure	
A. Certificate of incorporation, or other corporate organizational documents	
B. Controlled or Controlling Organizations	
C. Organization Chart	
D. Licensure/Certification as an IDRE in other state(s)	
Management	
E. Management Staff (complete Attachment 1)	
F. Medical Director (complete Attachment 1)	
G. Controlling employees and Board of Directors (complete Attachment 1)	
Accreditation	
H. Certificate of Accreditation	
II. CONFLICT OF INTEREST	
A. Conflict of Interest ("COI") Statements	
B. Chart of Affiliations	
C. Process to ensure COI compliance	
Following Certification as an IDR Entity	
D. Acquisition or control of prohibited entities	
III. CONTRACTED SERVICE PROVIDERS	
A. Reviewer and reviewing health care provider networks	
1. Assessment of ability to provide services	
2. Qualifications of reviewers and reviewing health care providers	
3. Attachment 2	
Procedures to ensure reviewers and reviewing providers are licensed, trained in requirements and qualified	
B. Attachment 2 summarizing the network and their areas of expertise	
IV. QUALITY ASSURANCE AND CONFIDENTIALITY	
A. Description of Quality Assurance program	
B. Procedures documenting applicant staff is available	
C. Description of applicant's ability to accept disputes and follow requirements of program	
D. Describe procedures to ensure confidentiality of records	
V. IDR PROCESS	
A. Recruitment and selection of reviewers and reviewing health care providers	
B. Dispute process description and chart	

C. Procedures to ensure no prohibited affiliations exist	
D. Procedure to ensure reviewer and reviewing health care provider is qualified and neutral	
E. Conflict of interest procedures	
F. Procedure to ensure disputes are reviewed timely	
G. Methodology for determining reasonable fee	

H. Procedure for ensuring applicant's contracted entities follow program requirements	
I. Provide samples of all correspondence to be used	
J. Procedures to ensure updates to 23 NYCRR Part 400 are incorporated into process in a timely manner	
VI. RECORD RETENTION, COMPLIANCE AND INFORMATION SYSTEMS	
A. Record retention procedures	
B. Confidential data	
1. Receipt	
2. Storage	
3. Disposal	
VII. FINANCIAL ARRANGEMENTS	
A. Financial Statements	
1. Statement of Revenues and Expenses	
2. Balance Sheet	
3. Method to pay debt, source of capital and documentation of accounts, assets, reserves and deposits	
4. Certified Financial Statement	
B. Proposed fees for IDRs	
Waiver for financial hardship	
C. Applicant's methodology for developing fees	
Attachment 1	
Attachment 2	
Attachment 3	
Attachment 4	
Attachment 5	

Attachment 1

(Page 1 of 7)

INSTRUCTIONS: –Attachment 1 should be duplicated and forwarded to each of the following individuals for completion:

- all directors, officers, executives
- the medical director
- all owners

At the end of Attachment 1 is an affidavit that must be completed by each individual listed above. Without all signed and notarized affidavits this application will be considered incomplete.

Omission of any information requested may lead to exclusion of the applicant from consideration for a certification or revocation of the certificate if such certificate is already awarded.

PERSONAL QUALIFYING INFORMATION:

A. PERSONAL IDENTIFYING:

NAME (Last) (First) (Middle Initial)

ADDRESS (residence)

CITY STATE ZIP CODE

TELEPHONE NUMBER (Area Code)

BUSINESS NAME AND ADDRESS

CITY STATE ZIP CODE

TELEPHONE NUMBER (Area Code)

DATE OF BIRTH Month / Day / Year PLACE OF BIRTH COUNTY/STATE SOCIAL SECURITY #

CURRENT OR PROPOSED POSITION WITH THE INDEPENDENT DISPUTE RESOLUTION ENTITY

B. INDIVIDUAL EMPLOYMENT HISTORY:

Start with MOST RECENT employment and include employment for the last 10 years. A resume may be included but any additional information requested below and not contained in such resume should be added. Photocopy and attach additional pages if necessary.

NAME OF EMPLOYER

ADDRESS OF EMPLOYER

CITY STATE ZIP CODE

DATES OF EMPLOYMENT TYPE OF BUSINESS
FROM: TO:

NAME OF SUPERVISOR/REFERENCE TELEPHONE NUMBER

POSITION/RESPONSIBILITIES

REASON FOR DEPARTURE

EMPLOYMENT HISTORY CONTINUED:

NAME OF EMPLOYER:	
ADDRESS OF EMPLOYER	
CITY STATE ZIP CODE	
DATES OF EMPLOYMENT From: To:	TYPE OF BUSINESS
NAME OF SUPERVISOR OR REFERENCE	TELEPHONE NUMBER (area code)
RESPONSIBILITIES	
REASON FOR DEPARTURE	

NAME OF EMPLOYER:	
ADDRESS OF EMPLOYER	
CITY STATE ZIP CODE	
DATES OF EMPLOYMENT From: To:	TYPE OF BUSINESS
NAME OF SUPERVISOR OR REFERENCE	TELEPHONE NUMBER (area code)
RESPONSIBILITIES	
REASON FOR DEPARTURE	

NAME OF EMPLOYER:	
ADDRESS OF EMPLOYER	
CITY STATE ZIP CODE	
DATES OF EMPLOYMENT From: To:	TYPE OF BUSINESS
NAME OF SUPERVISOR OR REFERENCE	TELEPHONE NUMBER (area code)
RESPONSIBILITIES	
REASON FOR DEPARTURE	

C. LICENSES:

Type of License (including Specialty)	Institution Granting License and Address	Date Received	Date of Expiration

D. EDUCATIONAL HISTORY (College and Subsequent Education):

Institution	Address	Attended from/to	Degree	Date Received

E. HISTORY OF ANY LEGAL ACTIONS:

1. Have you ever changed your name or used an alias?

❑ YES ❑ NO

NOTE: If "YES," attach an explanation including other names(s) date(s) and the reason(s) for each change.

2. Except for minor traffic violations, have you ever been indicted or been convicted or had a sentence imposed or suspended, or been pardoned of a conviction for any crime?

❑ YES ❑ NO

3. Are there any criminal actions pending against you?

❑ YES ❑ NO

4. Have you ever been named as a defendant in any civil action or proceeding in which there was an issue of moral turpitude, including but not limited to fraud or breach of fiduciary responsibility?

❑ YES ❑ NO

NOTE: If "YES" to 2, 3, or 4, attach explanation(s) including the date of the action or proceeding, place (county of the filing), the civil docket number, if available, and the disposition of the case if any.

5. Have you ever been an owner, officer, trustee, management employee or controlling stockholder of an entity which, while you occupied any such position or served in any such capacity with respect to it:

a. suffered the suspension or revocation of its certificate of authority or license to do business in any state?

❑ YES ❑ NO

b. was denied a certificate of authority, license or contract to do business in any state?

❑ YES ❑ NO

NOTE: If "YES" to any of the above, attach an explanation.

Attachment 1

(Page 4 of 7)

AFFILIATION WITH OTHER HEALTH CARE OPERATIONS:

INSTRUCTIONS: The purpose of this section is to obtain a complete listing of any health care operations with which the owners, officers, directors, executives or medical director of the IDRE have been affiliated within the past 10 years.
Affiliation with health care operations for the purposes of this section includes serving as an officer, director, member of the management staff, a shareholder of 10 percent or more of a health care operation's shares or key advisor for a health care operation.

1. For the past 10 years, have you owned or operated any health care or health related operations or held a management position or had any affiliations with health care or health related operations in New York, in the USA, or in other countries?

❑ YES ❑ NO

NOTE: If "YES," complete the following chart:

Name & Address of Health Care Operation	Affiliation Dates From/To	Nature of Affiliation with Facility	Agency Licensing	License #

2. Are/were these health care operations in compliance with applicable laws and regulations during your affiliation?

❑ YES ❑ NO

NOTE: If "NO," complete the following: (attach additional pages if necessary)

NATURE OF VIOLATION

AGENCY OR BODY ENFORCING VIOLATION (name & address)

STEPS TAKEN BY FACILITY TO REMEDY VIOLATION

Has suspension, revocation or accreditation since been restored? ❑ YES ❑ NO

NOTE: If "NO", give an explanation.

3. Has the IDRE or any of its holding companies operated as an IDRE for any other state?

❑ YES ❑ NO

In that capacity as an IDRE, have you been cited for any violation, deficiency, or improper conduct?

❑ YES ❑ NO

If "YES," please list all completed, current or pending actions.

PERSONAL FINANCIAL INVOLVEMENT:

A. Financial Support for the IDRE:

Is the owner, any members of a partnership, or directors and executives of for profit and not-for-profit corporations or other business corporations intending to provide capital for use in owning, organizing or operating the IDRE?

❑ YES ❑ NO

NOTE: If "YES," provide the following:

- Attach a personal financial statement for each individual providing financial support from personal finances for the agent.
- Make clear the percent of the business which each person controls, and document its value;
- Lessors are to attach documents showing their financial ability to fulfill any construction obligations;
- Any additional information pertinent to determination of either the agent's financial capabilities or the project's feasibility must also be attached; and
- For a change in ownership control, submit affidavits from both the party from which the operational interest is being acquired and the party acquiring the interest. Interest, for the purposes of this section, means right, title or share in a facility, participation in any advantage, profit and responsibility from or for the facility.

B. Transactions with the IDRE or its Holding Company:

Have any transactions involving money, extension of credit, liens, notes, bonds or mortgages occurred or are such transactions anticipated between the IDRE and you or any of your relative(s) or between the holding company and you or any of your relatives(s)?

❑ YES ❑ NO

NOTE: If "YES," complete the Disclosure of Transactions Form below identifying such transactions.

DEFINITIONS:

RELATIVE, for the purposed of this section, means any relationship as a spouse, child, parent, sibling, spouse's parent, spouse's child, child's parent, child's spouse or sibling's spouse.

TRANSACTION, for the purposes of this section, is any business transaction or series of transactions that during any one fiscal year, represents 5 percent of the total annual operating expenses of any of the parties to the transaction. Transactions include any sale or leasing of any property. Salaries paid to employees for services provided in the normal course of their employment are not included in this definition. No single transaction of less than $500 need be reported.

Attachment 1
(Page 6 of 7)

DISCLOSURE OF TRANSACTIONS FORM

PARTIES INVOLVED IN TRANSACTION

TYPE OF TRANSACTION

VALUE OF TRANSACTION

PERCENT OF OPERATING COSTS/ DOLLARS

PERCENT INTEREST RATE/ DOLLARS

REASON FOR TRANSACTION

METHOD OF REPAYMENT

PARTIES INVOLVED IN TRANSACTION

TYPE OF TRANSACTION

VALUE OF TRANSACTION

PERCENT OF OPERATING COSTS/ DOLLARS

PERCENT INTEREST RATE/ DOLLARS

REASON FOR TRANSACTION

METHOD OF REPAYMENT

(Attach additional sheets if necessary)

AFFIDAVIT

(to be completed with Attachment 1) **(Attachment 1, page 7 of 7)**

I, _____being duly sworn deposes and says
NAME (Last, first, middle initial)

I am a _____ _____ _____ of
(POSITION / TITLE)
_____.
ORGANIZATION/CORPORATION

I certify that I have provided all the information requested in Attachment 1 including a complete list of any and all hospitals, nursing homes, clinics, health maintenance organizations, halfway houses, hotels, other institutions of care, external appeal organizations, IDRE's, operations involving the custody or treatment for the physically or mentally afflicted with which I have been affiliated within the past 10 years as an operator, owner, incorporator, director, partner, medical director or shareholder with 10 percent or more of the shares of the entity.

I certify, under penalty of perjury, that if no names of such health care operations have been provided, I have had no such affiliations in the past 10 years and that the information contained herein is accurate, true and complete.

Signature _____ Date_____

STATE OF)
SS:
County of)

On this ____ day of _____, 20__, before me personally appeared

_____, to me known and known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that he/she resides at _____, and further that:
he/she is a duly authorized member of _____ the company described in said instrument; that, he/she is authorized to execute the foregoing instrument on behalf of the company for purposes set forth therein; and that, pursuant to that authority, he/she executed the foregoing instrument in the name of and on behalf of said company as the act and deed of said company.

_____
Notary Public
Registration Number: _____ State of _____

ATTACHMENT 2

Independent Dispute Resolution Entity Provider Listing

For the medical director and each reviewing health care provider and reviewer of the IDRE, complete the following information. Identify potential conflicts of interest for each reviewer:

Name	State and License No.(s)	Clinical Specialty	Practice Affiliations	Research Focus (if applicable)	Academic Affiliation

The above information is accurate and complete for all participating peer reviewers and the medical director of the IDRE.

_____ _____

CEO Signature Date

STATE OF)
SS:
County of)

On this ____ day of _____, 20___, before me personally appeared _____, to me known and known to me to be the person who executed the

foregoing instrument, who, being duly sworn by me did depose and say that he/she resides at _____, and further that:

he/she is a duly authorized member of _____, the company described in said instrument; that, he/she is authorized to execute the foregoing instrument on behalf of the company for purposes set forth therein; and that, pursuant to that authority, he/she executed the foregoing instrument in the name of and on behalf of said company as the act and deed of said company.

_____
Notary Public
Registration Number: _____ State of _____

ATTACHMENT 3

Conflict of Interest Attestation

To be executed by the CEO on behalf of the corporate entity, owners, officers, directors, medical director and management employees of the IDRE.

> For purposes of this attestation, "material familial affiliation" means any relationship as a spouse, child, parent, sibling, spouse's parent, spouse's child, child's parent, child's spouse, or sibling's spouse.
>
> "Material financial affiliation" means any financial interest more than five percent of total annual revenue or total annual income of an IDRE or officer, director, or management employee thereof; or clinical peer reviewer employed or engaged thereby to conduct any IDR. The term material financial affiliation shall not include revenue received from a health care plan by (a) an IDRE to conduct an IDR pursuant to New York Insurance Law Article 6, or (b) a clinical peer reviewer for health services rendered to enrollees.
>
> "Material professional affiliation" means any physician-patient relationship, any partnership or employment relationship, a shareholder or similar ownership interest in a professional corporation, or any independent contractor arrangement that constitutes a material financial affiliation with any expert or any officer or director of the independent organization.

I Whereas, the IDRE shall not own or control, be owned or controlled by, or exercise common control with any of the following:

A. any national, state or local illness, health benefit or public advocacy group;
B. any national, state or local society or association of hospitals, physicians, or other providers of health care services; or,
C. any national, state or local association of health care plans; and

II Whereas, no IDRE or officer, director, or management employee thereof; or clinical peer reviewer employed or engaged thereby to conduct any IDR pursuant to this title, shall have any material professional affiliation, material familial affiliation, material financial affiliation, or other affiliation prescribed pursuant to regulation, in relation to an IDR, with any of the following:

A. any health care plan;
B. any officer, director, or management employee of a health care plan;
C. any health care provider, physician's medical group, independent practice association, or provider of pharmaceutical products or services or durable medical equipment;
D. any health service facilities; and
E. any developer or manufacturer of health services

Now, therefore, I, _____, in my capacity as Chief Executive Officer of , _____,
(Name of Chief Executive Officer) **(Name of IDRE)**

do attest and affirm under penalty of perjury that _____has no disqualifying relationship as described in Section I above,
(Name of Independent Dispute Resolution Entity)

and further, that neither _____nor any of its owners, officers, directors, Medical Director, Management employees, or
(Name of Independent Dispute Resolution Entity)

clinical peer reviewers currently employed or engaged have any material affiliation (as defined above) with any person or entity listed in Section II above except as indicated on the attached sheet(s) incorporated and made as part hereof.

Name of Chief Executive Officer _____

_____ _____
Signature Date

STATE OF)
SS:
County of)

On this ____ day of _____, 20__, before me personally appeared

_____, to me known and known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that he/she resides at _____, and further that:

he/she is a duly authorized member of _____ the company described in said instrument; that, he/she is authorized to execute the foregoing instrument on behalf of the company for purposes set forth therein; and that, pursuant to that authority, he/she executed the foregoing instrument in the name of and on behalf of said company as the act and deed of said company.

_____
Notary Public
Registration Number: _____ State of _____

Attachment 4

INFORMATION SECURITY & CYBER SECURITY REQUIREMENTS

1. Definition and Obligations During Certification

The term "Confidential Information" as used herein includes all electronic or hard copy information, records, and communications that an IDRE gains access to in the course of rendering IDR services, including, but not limited to, any information, records, or communications that the Department or the State, regardless of form or medium of disclosure (e.g., verbal, hard copy, or electronic) or source of information (e.g., the Department, other state agencies, regulated entities, electronic systems, federal government, or third-party consultants) provides to an IDRE, its officers, agents, employees, and subcontractors or that an IDRE, its officers, agents, employees, and subcontractors obtain, discover, derive, or otherwise become aware of as a result of an IDRE's performance of IDR services. During the term of its certification, an IDRE shall maintain the security, confidentiality, integrity, and availability of all Confidential Information in accordance with the following clauses. An IDRE shall ensure that its officers, agents, employees, partners, and subcontractors, if any, are fully aware of an IDRE's obligations and shall take all commercially reasonable steps to ensure their compliance to prevent unauthorized use, access, or disclosure of Confidential Information. Failure by an IDRE or its officers, agents, employees, partners, and subcontractors to fully comply with these requirements shall be deemed a failure to meet its obligations and may result in the Department suspending, canceling, and/or terminating the certification of an IDRE for cause or to pursue any other legal or equitable remedies available.

(a) Compliance with the Department and NYS Information Security Policies and Standards

Each IDRE warrants, covenants, and represents that it will comply fully with all security policies and standards of the Department, including New York State Information Technology Services ("ITS") Information Security policies and standards located at https://its.ny.gov/eiso/policies/security.

Except for any privilege or privacy right recognized by law, individuals have no legitimate expectation of privacy during any access of the Department's Confidential Information. Any access may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to all computer files; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems), and other electronic records. Unauthorized access to the Department's Confidential Information is not permitted.

The Department shall have the right at any time to require that an IDRE remove from interaction with the Department any IDRE representative whom the Department believes is detrimental to its working relationship with an IDRE. The Department will provide an IDRE with notice of its determination and the reasons it requests the removal. If the Department signifies that a potential security violation exists with respect to the request, an IDRE shall immediately remove such individual. An IDRE shall not assign the individual to any aspect of the IDR process without the Department's consent.

An IDRE, to the extent the following meets or exceeds ITS Information Security policies described above, shall use industry standard security measures, including standard encryption protocols, to protect and guard the confidentiality, security, integrity, and availability of Confidential Information, and adhere to all the Department's security policies. An IDRE shall be strictly prohibited from using Confidential Information in any fashion other than that defined herein. There may be instances whereby the Department will communicate security procedures necessitated by the Department's operations. An IDRE will use reasonable efforts to implement same.

Each IDRE warrants that it will be properly informed and trained regarding security standards and is prohibited from disclosing Confidential Information to any persons without a need to know.

(b) **Protection and Transmission of Confidential Information**

An IDRE shall use appropriate means to preserve and protect Confidential Information. This includes, but is not limited to, preventing, tampering with, disengaging, or otherwise circumventing Department or third-party IT security controls; use of stable storage media; regular data backups and archiving; password protection of volumes; and data encryption. Consistent with the NYS Encryption Standard at https://its.ny.gov/tables/technologypolicyindex, to the extent doing so is applicable based on the specific services provided by an IDRE, an IDRE must encrypt Confidential Information at rest, on file storage, database storage, or on back-up media, and in transit in accordance with local, state, and federal laws, rules, regulations, ordinances, policies, standards, and guidelines. An IDRE must use up-to-date secure means for all electronic transmission or exchange of system, user, and application data with the Department, with encryption at rest specifically using, at minimum, FIPS 140.2 approved cryptographic modules, and the secure means used for electronic transmission or exchange of system, user, and application data with the Department shall be up-to-date and align with industry best practices. An IDRE agrees that to the extent it has been authorized to use such storage, any and all Confidential Information will only be stored, processed, and maintained solely on designated target devices, and that no Confidential Information at any time will be processed on or transferred to any portable computing device or any portable storage medium.

(c) **Physical Transport of Confidential Information**

To the extent the Department agrees that an IDRE may physically transport any Confidential Information, such physical transport may only occur upon the written direction and approval of the Department. This includes but is not limited to transport between an IDRE's offices, to and from third parties, and to the Department.

(d) **Data Storage, Access, and Location - Offshore Restrictions**

The Department and each IDRE agree that: (a) all Confidential Information shall remain within, and may not be stored or accessed from outside of, the Continental United States ("CONUS"); and (b) unless expressly agreed to in a writing approved by a Department-authorized signatory adhering to established Department practices, an IDRE shall not have remote access to the Department's information technology resources.

All access to Confidential Information, physical or virtual, must be conducted within CONUS and have adequate security systems in place to protect against the unauthorized access to New York State facilities and Confidential Information stored therein. An IDRE shall not send or permit to be sent to any location outside of the CONUS any Confidential Information related to its IDR services.

Upon the Department's prior written approval, to the extent an IDRE requires access to Department system or application audit logs for support and troubleshooting, an IDRE or any subcontractors shall maintain such logs only within CONUS, shall take the strictest measures to ensure such logs do not contain Confidential Information including production data, and shall maintain such logs in a secure environment subject to audits by the Department.

(e) **Separation of Duties/Access Controls**

An IDRE must ensure that all Confidential Information that it holds as an IDRE is stored in a controlled access environment to ensure data confidentiality, integrity, and availability. An IDRE shall provide the Department with a list of the physical locations where it has stored any

Confidential Information at any given time and shall update that list if the physical location changes. All IDRE facilities must have adequate security systems in place to protect against the unauthorized access to such facilities and data stored therein. An IDRE shall restrict access to and within such facilities through an access control system that requires positive identification of authorized individuals as well as maintains a log of all access (e.g., date and time of the event, type of event, user identity, component of the information system, and outcome of the event). An IDRE shall have a formal procedure in place for granting and terminating computer system access to Confidential Information and to track access. Access to Confidential Information by an IDRE for any type of projects outside of those approved by the Department is prohibited.

The Department requires an IDRE to follow the principle of least privilege by adhering to separation of job duties and limiting an IDRE's staff knowledge of Confidential Information to that which is absolutely necessary to perform IDR job duties. Upon request, an IDRE will provide documentation to the Department clearly defining the security roles and access levels for each of its staff working with Confidential Information with a level of specificity approved by the Department.

(f) **Cloud Security Requirements**

If cloud-based services are a component of the solution or services to be provided by an IDRE, an IDRE shall comply with FedRAMP (https://www.fedramp.gov) standards for cloud services, and local, state, and federal laws, rules, regulations, ordinances, policies, standards, and guidelines.

(g) **Compliance with the NYS Statutory Breach Notification and Data Security Requirements**

An IDRE shall be responsible for complying with the statutory breach notification and data security requirements set forth in New York General Business Law ("GBL") §§ 899-aa and 899-bb and New York State Technology Law ("State Technology Law") § 208 as well as the following terms contained herein with respect to any private information (as defined in GBL § 899-aa) received by an IDRE ("Private Information") that is within the control of an IDRE either on the Department's or the State's information security systems or an IDRE's information security system. In the event of a "breach of the security of the system" (as defined by GBL § 899-aa), an IDRE shall immediately commence an investigation, in cooperation with the Department and the State to determine the scope of the breach and restore the security of the system to prevent any further breaches. An IDRE shall also notify the Department of any breach of the security of the system within (four) 4 hours following discovery of such breach. Notice of such breach shall be sent to the Department at:

information.security@dfs.ny.gov

Except as otherwise instructed by the Department, an IDRE shall, to the fullest extent possible, first consult with and receive authorization from the Department prior to notifying any individuals, the NYS Department of State, the NYS Division of State Police, the NYS Office of the Attorney General ("OAG"), or any consumer reporting agencies of a breach of the security of the system or concerning any determination to delay notification due to law enforcement investigations.

Nothing herein shall in any way impair the authority of OAG to bring an action against an IDRE to enforce the provisions of applicable statutory breach notification and data security provisions or limit an IDRE's liability for any violations of GBL § 899-aa, GBL § 899-bb, State Technology Law § 208, or any other applicable laws, rules, or regulations. In the event that an IDRE is advised by a law enforcement agency pursuant to GBL §899-aa(4) to delay the notice under GBL §899-aa(3), an IDRE shall provide the notice to the Department not more than twenty-four (24) hours after an IDRE has been advised that it may provide the notice under GBL §899-aa(3).

In accordance with applicable statutory breach notification and data security provisions, an IDRE is responsible for complying with the following terms with respect to any Private Information received by

or on behalf of the Department as an IDRE. An IDRE:

(i) Shall supply the Department with a copy of its breach notification policy, which shall be modified to be in compliance with this provision.

(ii) Shall encrypt any database fields and backup tapes that contain Private Information as set forth in applicable statutory breach notification and data security provisions.

(iii) Shall ensure that the Department's Private Information is encrypted in transit to/from an IDRE's systems.

(iv) Shall ensure that Private Information is not displayed to users on computer screens or in printed reports; however, specific users who are authorized to view the private data elements and who have been properly authenticated may view/receive such data.

(v) Shall monitor for breaches of security to any of its systems that store or process the Department's Private Information.

(vi) Shall take all steps as set forth in applicable statutory breach notification and data security provisions to ensure Private Information will not be released without authorization from the State.

(vii) In the event a security breach occurs as defined by GBL § 899-aa, notify the Department's contact at information.security@dfs.ny.gov within four (4) hours of becoming aware of the breach and commence an investigation in cooperation with the Department to determine the scope and cause of the breach, and to prevent the future recurrence of such security breaches.

(viii) Coordinate all communication regarding the data breach with the Department's Chief Information Security Officer and the State.

(ix) Take immediate steps necessary to restore the information security system to prevent further breaches and take corrective action in the timeframe required by the Department and State. If an IDRE is unable to complete the corrective action within the required timeframe, in addition to any other remedies available, the Department and/or the State may contract with a third-party to provide the required services until corrective actions and services resume in a manner acceptable to the Department. An IDRE will be responsible for the cost of these services during this period.

(x) Shall be responsible for providing all notices required by applicable statutory breach notification and data security provisions and for all costs associated with providing said notices.

The Department reserves the right to require commercially standard credit monitoring for any and all individuals affected by the data breach at the sole expense of an IDRE for a period to be determined by the Department, but not less than twelve (12) months, which shall begin thirty (30) days following the notice of offer from an IDRE of such credit monitoring to those affected individuals, which shall be within a reasonable time following the identification of such affected individuals. The Department reserves the right to require notice by regular or electronic mail.

(h) **Breaches Not Addressed by GBL § 899-aa, GBL § 899-bb, or State Technology Law § 208**

In addition to any responsibilities of an IDRE for reporting breaches of Private Information under GBL § 899-aa, GBL § 899-bb, or State Technology Law § 208, an IDRE must, within four 4 hours of becoming aware of a breach, report to the Department *any* breaches or information security incidents of any Confidential Information whether it consists of Private Information or otherwise. Notice of such incident shall be sent to the Department at:

information.security@dfs.ny.gov

An IDRE shall ensure that the personnel charged with carrying out IDR services are aware of an IDRE's obligations to the Department hereunder. An IDRE's staff browsing, viewing, altering, appending, or modifying the Confidential Information in violation of an IDRE's own security policies

shall be deemed to have breached the security of the System. An IDRE represents and warrants that the Confidential Information that it hosts for the Department remains at all times the property of the Department and must be fully accessible to the Department during the term of its certification as an IDRE and at the conclusion of certification. An IDRE's responsibilities, includes taking all reasonable measures at no additional cost to the Department to ensure that the Department is able to extract or receive any and all Confidential Information out of an IDRE's hosted solution, including metadata and attachments, in a format that is accessible to the Department and capable of being used in other technical solutions, as further described below.

2. Data Transparency, Accessibility, Migration & Destruction at Expiration/Termination of Certification

(a) **Data Migration**

An IDRE shall ensure that the services it performs as an IDRE are performed in such a way that ensures easy migration of any Confidential Information held by an IDRE as required by the Department. This may include:

(i) An IDRE keeping Confidential Information, including Department policy and profile information, separate from processes of any software itself and maintaining that information in a format that allows the Department to easily transfer it to an alternative application platform;

(ii) An IDRE making its Application Programming Interfaces (APIs) available to the Department; and

(iii) An IDRE reformatting data and/or applications at an IDRE's own expense in order to allow the Department easily to switch to alternative software providers or move the Confidential Information back in-house at the Department.

(b) **Data Return and Destruction - In General**

During any period of suspension of services or while an IDRE is certified, an IDRE will not take any action to intentionally erase any Confidential Information.

At the expiration or termination of an IDRE's certification, an IDRE shall implement an orderly return of Confidential Information and the subsequent secure disposal of Confidential Information. The Department shall be entitled to any post-termination assistance generally made available by an IDRE with respect to the services it provides unless a unique alternative data retrieval arrangement has been established between the parties.

At the Department's option, an IDRE must provide the Department with a copy of all Confidential Information, including metadata and attachments, in a mutually agreed upon, commercially standard format at no additional charges to the Department, and give the Department continued access to the Confidential Information for no less than ninety (90) days beyond the expiration or termination of IDRE certification. Thereafter, except for data required to be maintained by local, state, and federal laws, rules, regulations, ordinances, policies, standards, and guidelines or the certification, an IDRE shall destroy Confidential Information from its systems and wipe all its data storage devices to eliminate any and all Confidential Information from an IDRE's systems. The sanitization process must be in compliance with NYS Security Policy NYS-S13-003, http://www.its.ny.gov/document/sanitizationsecure-disposal-standard, and, where required, Criminal Justice Information Services ("CJIS") sanitization and disposal standards. If immediate purging of all data storage components is not possible, an IDRE will certify that any Confidential Information remaining in any storage component will be safeguarded to prevent unauthorized disclosures until such purging is possible. an IDRE must then certify to the Department, in writing,

that it has complied with the provisions of this paragraph including any supporting documentation as requested.

(c) **Data Return and Destruction - Regulated Data**

The Department considers the protection of sensitive and Confidential Information and business systems to be of the utmost importance. The Confidential Information collected and maintained by the Department is protected by a myriad of federal, state, and local laws, rules, regulations, ordinances, policies, standards, and guidelines. Access to and use of Confidential Information is limited to authorized government employees and legally designated agents, for authorized purposes only.

Attachment 5, entitled "PRIMARY SECURITY AND PRIVACY MANDATES," reflects several significant Federal and State laws, rules, regulations, ordinances, policies, standards, and guidelines that providers doing business with the Department must be aware of and comply with if applicable to the services being provided. Links to further guidance are included in that Attachment. The list is intentionally US-centric and is not intended to be all-inclusive. Further, since local, state, and federal laws, rules, regulations, ordinances, policies, standards, and guidelines and industry guidelines change, consulting definitive sources to assure a clear understanding of compliance requirements is critical.

To the extent that an IDRE has access to federal, state, or local government regulated data pursuant to its responsibilities as an IDRE, an IDRE agrees that it will abide by the requirements of those federal, state, and local laws, rules, regulations, ordinances, policies, standards, and guidelines, and will require in writing its officers, agents, employees, partners or subcontractors to similarly abide by any such requirements including the execution of any documents or agreements required to be executed, certifying their compliance with same.

An IDRE must, in accordance with applicable law and the instructions of the Department: maintain such regulated data for the time period required by applicable laws, rules, regulations, ordinances, policies, standards, and guidelines; exercise due care for the protection of data; and maintain appropriate data integrity safeguards against the deletion or alteration of such data. In the event that any regulated data is lost or destroyed because of any act or omission of an IDRE or any non-compliance with the obligations of certification, then an IDRE shall, at its own expense, use its best efforts in accordance with industry standards to reconstruct such data as soon as feasible. In such event, an IDRE shall reimburse the Department for any costs incurred by the Department in correcting, recreating, restoring, or reprocessing such data or in assisting therewith.

In the event that it becomes necessary for an IDRE to receive Confidential Information that federal, state, or local laws, rules, regulations, ordinances, policies, standards, and guidelines prohibits from disclosure, an IDRE hereby agrees to return or destroy all such Confidential Information that has been received by an IDRE when the purpose that necessitated its receipt by an IDRE has been completed. In addition, an IDRE agrees, after termination of its certification as an IDRE, not to retain any Confidential Information that federal, state, or local laws, rules, regulations, ordinances, policies, standards, and guidelines prohibits from disclosure.

Notwithstanding the foregoing, if the return or destruction of the Confidential Information is not feasible, an IDRE agrees to extend the protections of the certification for as long as necessary to protect the Confidential Information and to limit any further use or disclosure of that Confidential Information. If an IDRE elects to destroy Confidential Information, it shall use reasonable efforts to achieve the same and notify the Department accordingly. An IDRE agrees that it will use all appropriate safeguards to prevent any unauthorized use or unauthorized disclosure of Confidential Information that federal, state, or local laws, rules, regulations, ordinances, policies, standards, and guidelines prohibit from disclosure.

(d) **Audits of an IDRE's Security Controls**

An IDRE may be asked to provide recent independent audit reports on its security and compliance controls before and during the term of its IDRE certification. The Department shall have the right to send its officers and employees into the offices of an IDRE for inspection and audit of the facilities and operations used by an IDRE in the performance of any work as an IDRE. On the basis of such inspection, an IDRE may be required by the Department to implement specific additional security and compliance measures in cases where an IDRE is found to be noncompliant with certification safeguards. The Department will provide at least two (2) weeks' notice of its intention to exercise this audit right and will not use an independent third-party that is a competitor of an IDRE. Such audit shall be conducted to ensure compliance with the requirements of the certification.

(e) **Accessing NYS Facilities**

An IDRE may access Department information technology resources and NYS Facilities solely at the Department's request, and solely for work associated with its certification. In the event an IDRE accesses NYS Facilities, an IDRE will comply fully with all security procedures of the Department concerning such access communicated to it in its performance as an IDRE.

An IDRE agrees that it will adopt procedures to ensure the confidentiality, security, integrity, and availability of all Confidential Information provided to an IDRE under its certification. Those procedures include, for each prospective and current officers, agents, employees, partners, and subcontractors of an IDRE designated to work under its IDRE certification that they are required:

(i) if entering NYS Facilities through physical means, to be required to undergo the same security clearances as are required of those workforce members of the Department who physically access NYS Facilities including, upon request by Department, submitting identifying information and being fingerprinted on-site at IDRE expense. The Department shall arrange for the scheduling of such fingerprinting activities on Department premises; or

(ii) if using or entering NYS Facilities through electronic, telecommunications, information technology, or any other virtual means, to be required to undergo the same security clearances as are required of those workforce members of the Department who access NYS Facilities including, upon request by the Department, submitting identifying information and being fingerprinted at an IDRE's location at an IDRE's expense. An IDRE shall arrange for the scheduling of such fingerprinting activities at a law enforcement agency in an IDRE's locale, and in accordance with the law of the jurisdiction in which such fingerprinting takes place, either

(a) submit those fingerprints to a local law enforcement or criminal justice agency for the purpose of obtaining a criminal history record report, and, at the Department's discretion, to the Federal Bureau of Investigation for a national criminal history record check, and report to the Department the substance of the criminal record of any of the fingerprinted individuals; or

(b) mail those fingerprints to the Department for the Department to submit them for the purpose of obtaining a criminal history record report(s).

Attachment 5

PRIMARY SECURITY AND PRIVACY MANDATES[1]

Significant federal and state laws, regulations, policies, standards, and guidelines

- Criminal Justice Information Services (CJIS) Security Policy
- Federal Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
  National Institute of Technology Standards
- Gramm-Leach-Bliley Act (GLB)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- IRS Publication 1075
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)
- Electronic Communications Privacy Act, Stored Communications Act and the PATRIOT Act
- New York State Breach Notification Act: https://its.ny.gov/breach-notification
- NYS Cyber Security Policy and related Standards: https://its.ny.gov/eiso/policies/security
- NYS Cyber Incident Reporting: https://its.ny.gov/incident-reporting
- Minimum Acceptable Risk Standards for Exchanges (MARS-E)

1.1 Criminal Justice Information Services ("CJIS") Security Policy

The CJIS Security Policy represents a shared responsibility between the Federal Bureau of Investigations ("FBI") and CJIS System Agencies ("CSA") and State Identification Bureau ("SIB"). For the State of New York, the NY State Police is the CSA, and the Division of Criminal Justice Services is the SIB. The policy covers the roles and responsibilities for the FBI and the CSA and service providers covered under CJIS security addendums and CJS management control agreements.

CJIS requirements guidance:

- https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

1.2 Federal Educational Rights and Privacy Act ("FERPA") - State Ed, Higher Ed

Protects the privacy of student education records. "Education records" are those records, files, documents, and other materials that 1) contain information directly related to a student; and 2) are maintained by an educational institution. Examples: Grades, courses taken, schedule, test scores, advising records, educational services received, disciplinary actions, student identification number, Social Security number, student private email.
FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA requirements guidance:

- http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- Electronic Code of Federal Regulations, Title 34, Part 99

1.3 Federal Information Security Management Act of 2002 ("FISMA")

FISMA requires each federal agency to develop, document, and implement an effective agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. It is Title III of the E-Government Act of 2002. It affects Federal agencies, and other agencies they share data with.

[1] Please note that any hyperlinks provided in this document are subject to change and are not exhaustive of all resources available.

Key requirements/provisions include:

- Periodic risk assessments.
- Policies and procedures based on these assessments that cost-effectively reduce information security risk and ensure security is addressed throughout the life cycle of each information system.
- Subordinate plans for information security for networks, facilities, etc.
- Security awareness training for personnel.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and controls, at least on an annual basis.
- A process to address deficiencies in information security policies.
- Procedures for detecting, reporting, and responding to security incidents.
- Procedures and plans to ensure continuity of operations for information systems that support the organization's operations and assets.

FISMA requirements guidance:

- https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma
- https://www.dhs.gov/cisa/federal-information-security-modernization-act

FISMA requires that federal agencies comply with Federal Information Processing Standards (FIPS) developed by the National Institute of Standards and Technology ("NIST"). Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget ("OMB") policy OMB Memorandum M-10-15 directs agencies to follow NIST guidance.

NIST Special Publications: https://csrc.nist.gov/publications/sp

1.4 Gramm-Leach-Bliley Act of 1999 ("GLB")

GLB (also known as the Financial Modernization Act of 1999) includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, the Safeguards Rule, and pretexting provisions.

GLB affects financial institutions (banks, securities firms, insurance companies), as well as companies providing financial products and services to consumers (including lending, brokering, or servicing any type of consumer loan; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; and collecting consumer debts).

Key requirements/provisions: The privacy requirements of GLB include three principal parts:

- The Financial Privacy Rule: Requires financial institutions to give customers privacy notices that explain their information collection and sharing practices. In turn, customers have the right to limit some sharing of their information. Financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information.
- The Safeguards Rule: Requires all financial institutions to design, implement, and maintain safeguards to protect the confidentiality and integrity of personal consumer information.
- Pretexting provisions: Protects consumers from individuals and companies that obtain their personal financial information under false pretenses, including fraudulent statements and impersonation.

GLB requirements guidance:

- https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
- https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/financial-privacy-rule

1.5 Health Information Portability and Accountability Act ("HIPAA")

HIPAA has two major arms: Privacy and Security. Privacy tends to be a business (non-IT) focus, involving the program, HIPAA Privacy Officer and legal. Security tends to be more IT-focused (though it does cover handling of paper records as well).

Many health agencies have compliance requirements that are more stringent than HIPAA – HIPAA is the baseline. For example, the NYS Public Health law has tight requirements regarding AIDS information. The federal regulations at 42 CFR Part 2 guide privacy requirements of substance abuse information. The NYS Mental Hygiene law extends HIPAA consent requirements. Accordingly, meeting baseline HIPAA requirements may not be sufficient in all cases.

HHS (Federal Health and Human Services) HIPAA resources and requirements:

- Privacy rule: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- Security rule: https://www.hhs.gov/hipaa/for-professionals/security/index.html

Summarized versions:

- https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

HHS Educational Series bulletins:

- https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

AMA summary of violation (HHS Office of Civil Rights (OCR) audits can result in significant fines for not following the rules regardless of the scope of impact from a breach).

- https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

1.6 Health Information Technology for Economic and Clinical Health Act ("HITECH")

HITECH, enacted in 2009, promotes the adoption and meaningful use of health information technology. Subtitle D of HITECH addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

HITECH requirements guidance:

- https://www.hhs.gov/hipaa/for-professionals/security/guidance/hitech-act-rulemakingimplementation-update/index.html

1.7 IRS Safeguard Program, Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities

Pub1075 contains specific requirements for safeguarding federal tax information (current revision effective on Jan. 1, 2014).

- https://www.irs.gov/privacy-disclosure/safeguards-program
- https://www.irs.gov/pub/irs-pdf/p1075.pdf

1.8 Payment Card Industry Data Security Standard ("PCI DSS")

The PCI DSS is a set of requirements for enhancing security of payment customer account data, developed by the founders of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa to help facilitate global adoption of consistent data security measures. PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The Council also issued requirements called the Payment Application Data Security Standard (PA DSS) and PCI Pin Transaction Security (PCI PTS). PCI DSS affects retailers,

credit card companies, and anyone else handling credit card data. Currently, PCI DSS specifies 12 requirements, organized in six basic objectives:

Objective 1: Build and Maintain a Secure Retail Point of Sale System.
- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Objective 2: Protect Cardholder Data
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Objective 3: Maintain a Vulnerability Management Program
- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Objective 4: Implement Strong Access Control Measures
- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Objective 5: Regularly Monitor and Test Networks
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Objective 6: Maintain an Information Security Policy
- Requirement 12: Maintain a policy that addresses information security

PCI compliance requirements:
- PCI Document Library: https://www.pcisecuritystandards.org/document_library
- PA DSS: https://www.pcisecuritystandards.org/minisite/en/pa-dss-v2-0.php
- PCI PTS: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

1.9 Sarbanes-Oxley Act of 2002 (“SOX”)

SOX is designed to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. It was enacted after the high-profile Enron and WorldCom financial scandals of the early 2000s. It is administered by the Securities and Exchange Commission, which publishes SOX rules and requirements defining audit requirements and the records businesses should store and for how long. It affects U.S. public company boards, management and public accounting firms.

The Act is organized into 11 titles:
1. Public Company Accounting Oversight
2. Auditor Independence
3. Corporate Responsibility
4. Enhanced Financial Disclosures
5. Analyst Conflicts of Interest
6. Commission Resources and Authority
7. Studies and Reports
8. Corporate and Criminal Fraud Accountability
9. White-Collar Crime Penalty Enhancements
10. Corporate Tax Returns
11. Corporate Fraud Accountability

SOX requirement guidance:
- https://www.congress.gov/bill/107th-congress/house-bill/3763

- https://pcaobus.org/

1.10 The U.S. Electronic Communications Privacy Act, The U.S. Stored Communications Act, The U.S. PATRIOT Act

The Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA) create statutory privacy rights for people's electronic communications stored by a third-party service provider in "electronic," "computer," "temporary" or "intermediate" storage. Certain types of electronic communications (unread mail that is newer than 180 days) may only be obtained by law enforcement from a service provider via a search warrant. Other electronic communications and user information may be more easily obtained by law enforcement from a third-party provider by a court order or subpoena. Any communications may be obtained by law enforcement from a third-party provider if the end user has provided consent. End users should be careful not to give such consent by clicking through a Terms of Use and/or Privacy Policy or by signing a contract. The PATRIOT Act allows law enforcement to obtain or intercept electronic communications and other end user data from third-party service providers for terrorism investigations using protocols that are less stringent than those that would normally apply.

- U.S. Electronic Communications Privacy Act: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285
- U.S. Stored Communications Act: http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim
  U.S. PATRIOT Act: https://www.justice.gov/archive/ll/highlights.htm