

Bidder Signature Page

The bidder must include this signature page in the Attachment A RFP response under Signature Tab.
Please sign in **BLUE INK**.

Company:

CAPITAL Rx

Bidder Name:

ANTHONY J. BARRETT

Bidder Signature:

Anthony J. Barrett

Bidder Primary Contact Name/email:

>(- C:0 ;IV)

Date of Bid Submission:

4/23/20

ATTACHMENT C

HAC & CCOG RFP #2020.03.19

PHARMACY BENEFIT MANAGEMENT SERVICES

REQUIRED BIDDER INFORMATION & CERTIFICATIONS

Purpose of this Attachment C: HAC and CCOG require the following information about bidders who submit proposals in response to this RFP in order to facilitate the development of the contract with the winning bidder(s). The Proposal Team reserves the right to reject a bidder’s proposal if the bidder fails to provide this information fully, accurately, and by the deadline for submitting proposals set in **Section III A – RFP Timeline** in the RFP. Further, some of this information (as identified below) **must** be provided in order for the Proposal Team to accept and consider a bidder’s proposal. **Failure to provide such required information will result in a bidder’s proposal being deemed nonresponsive to this RFP, and therefore disqualified from consideration.**

Instructions: Provide the following information regarding the bidder submitting the proposal. Bidders should complete this document in Microsoft Word by filling out the form fields, printing the completed document, and signing it in the designated signature areas. It is mandatory that the information provided is certified with an original signature (in **BLUE INK**, please) from a person with sufficient authority and/or authorization to represent the bidder. As described in **Section IV A – Initial Qualifying Criteria** of the RFP, bidders are to provide one original completed and signed **Attachment C** in Tab 1 of the Technical Proposal submitted to CCOG and hard copies of the original in Tab 1 of the four Technical Proposals submitted to HAC and Excelsior Solutions. In addition, a scanned electronic copy of the original should be included in the USB jump drive submitted in each of the five proposal packages submitted.

BIDDERS MUST PROVIDE ALL THE INFORMATION OUTLINED BELOW

<p>1. HAC & CCOG RFP Name:</p> <p><u>Pharmacy Benefit Management Services</u></p>	<p>2. Proposal Due Date:</p> <p><u>April 20, 2020 at 5 PM Eastern</u></p>
<p>3. Bidder Name:</p> <p><u>Capital Rx</u></p> <p>(insert legal name of the entity responding to RFP)</p>	<p>4. Bidder Federal Tax ID #:</p> <p><u>35-2612946</u></p>
<p>5. Bidder Corporate Address:</p> <p><u>85 Broad</u> <u>StreetFloor</u> <u>28</u> <u>New York, NY 10004</u></p>	<p>6. Bidder Remittance Address (or "Same" if same as Item #5):</p> <p><u>Same</u></p> <p>_____</p> <p>_____</p> <p>_____</p>

7. Print or type information about the bidder representative/contact person authorized to answer questions regarding the proposal submitted by your company:

Bidder Representative's Name: Anthony Barrett
 Representative's Title: Senior. Ilic.e.e.c.esident Business Qe elopme.nt
 Address 1: 85 Broad Stc.e.et
 Address 2: F/oc.28
 City, State, Zip: New Yock. NY 10004
 Phone#: 646-781-8834
 Fax#: --
 E-Mail Address: tbacre.tt@c.ap-cx.com

8. Print or type the name of the bidder representative authorized to address contractual issues including the authority to execute a contract on behalf of the bidder, and to whom legal notices regarding contract termination or b.l:e.a.ch,...s.b.o.ulcLb_e_sent (if not the same individual as in #7, provide the following information on each such representative and specify their function)

Bidder Representative's Name: Joseph A.l.e.x.andec.
 Representative's Title: C.biet Ope.eating Officer
 Address 1: 85 Broad Stc.e.et
 Address 2: Flooc.28
 City, State, Zip: New Yock. NY 10004
 Phone#: 646-457-4804
 Fax#: --
 E-Mail Address: joe@c.ap-rx om

9. Is this bidder an Ohio certified Minority Business Enterprise ("MBE")? Yes_ No

If yes, attach a copy of current certification as an appendix in Tab 3 of your Techncial Proposal.

10. Mandatory Bidder Certifications:

CCOG may not enter into contracts with any bidders who have been found to be ineligible for state contracts under specific federal or Ohio statutes or regulations. Bidders responding to this RFP MUST certify that they are NOT ineligible by signing each of the four statements below Failure to provide proper affirming signature on any of these statements will result in a bidder's proposal being considered non-responsive to this RFP and eliminated from consideration

I, (AM.ii . r.:)nit/J Rv (signature of representative shown in Item #7, above), hereby certify and affirm that (ins et name of the submitting bidder shown in Item #3 above), has not been debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions by the United States Department of Labor, the United States Department of Health and Human Services, or any other federal department or agency as set forth in 29 CFR Part 98, or 45 CFR Part 76, or other applicable statutes.

AND.

I, [Signature] (signature of representative shown in Item #7, above) hereby certify and affirm that ca ll... (insert name of the submitting bidder shown in Item #3, above), is in compliance with all federal, state and local law, rules and regulations including but not limited to the Occupational Safety and Health Act and the Ohio Bureau of Employment Services and attest to the following: the bidder has -

- Not been penalized or debarred from any public contracts or falsified certified payroll records or any other violation of the Fair Labor Standards Act in the last three (3) years;
- Not been found to have violated any worker's compensation law within the last three (3) years;
- Not violated any employee discrimination law within the last three (3) years;
- Not been found to have committed more than one (1) willful or repeated OSHA violation of a safety standard (as opposed to a record keeping or administrative standard) in the last three (3) years;
- Not had an Experience Modification Rating of greater than 1.5 (a penalty-rated employee with respect to the Bureau of Workers' Compensation risk assessment rating) and
- Not failed to file any required tax returns or failed to pay any required taxes to any governmental entity within the past three (3) years.

I, SJK-JJO-- (signature of representative shown in Item #7, above) hereby certify and affirm that LIRx (insert name of the submitting bidder shown in Item #3, above), is not on the list established by the Ohio Secretary of State, pursuant to ORC Section 121.23, which identifies persons and businesses with more than one unfair labor practice contempt of court finding against them.

[Signature] AND. (signature of representative shown in Item #7, above) hereby certify and affirm that J...a;usu.o.& (insert name of the submitting bidder shown in Item #3, above), either is not subject to a finding for recovery under ORC Section 9.24, or has taken appropriate remedial steps required under that statute to resolve any findings for recovery, or otherwise qualifies under that section to enter into contracts with CCOG.

11. Supplemental Contract and Equal Employment Opportunity Information on the Bidder:

A. Provided data on bidder employees both nationwide (inclusive of Ohio staff) and the number of Ohio employees:

	<u>Nationwide</u>	<u>Ohio Offices:</u>
Total Number of Employees:	■	___a
% of those who are Women:	■	■
% of those who are Minorities:	■	■

B. If you are the winning bidder and this RFP involves the provision of services to HAC Members and Sourcing Alliance Members, will you subcontract any part of the work?
 NO -or-
 YES, but for less than 50% of the work -or-

YES, for 50% or more of the work

C. If any part of your proposal would be performed by any subcontractors provide the following information on each subcontractor (additional pages may be added as needed):

Subcontractor Name: Walmart
Street Address 1: 702 SW 6th Street
Street Address 2:
City, State, Zip: Bentonville, AR 72716
Work to be Performed: Mail Order Pharmacy & Specialty Pharmacy services

Estimated percentage of total proposal to be performed by subcontractors %
(Do not show dollar amounts here; show % of WORK sub-contractors will perform/provide). Define the part of the work that will be performed by each subcontractor.

Subcontractor's employee information (attach additional pages if needed):

Nationwide Ohio Offices:
Total Number of Employees: [Redacted]
% of those who are Women: [Redacted]
% of those who are Minorities: [Redacted]

12. The Proposal Team has identified the following minimum market size requirements for proposals of bidders participating in this RFP process to be considered; bidders must meet or exceed these requirements:

Minimum enrolled member population of 250,000. What is the current enrolled member population served by your company as of your most recently completed fiscal year? [Redacted]

Minimum drug spend under management of \$500 million annually. What was the drug spend under management during your most recently completed fiscal year? [Redacted]

[Signature] (signature of representative shown in Item #7, above) hereby certify and affirm that W&JALIA (insert name of the submitting bidder shown in Item #3, above) meets the minimum market size requirements of this Attachment C Section 12 and that the enrolled member population and drug spend under management annually figures provided are accurate.

13. I [Signature] (name of bidder representative in Item #7, above) hereby affirm that this proposal submitted HAC and CCOG accurately represents the capabilities and qualifications of Capital Rx (insert name of submitting bidder as shown in item #3, above), and I hereby affirm that the cost(s) proposed in Attachment B - Cost Proposal & Pricing Template for the performance of services and/or provision of goods covered in this proposal in response to this RFP is a firm fixed price structure as described in the Cost Proposal, inclusive of all incidental as well as primary costs to be charged to Participating Groups. (Failure to provide the proper affirming signature on this item may result in the disqualification of your proposal.)

Signature [Signature] Date 11/1/12

Additional Subcontractors

—

Subcontractor Name: [REDACTED]

Street Address 1: 4000 Town Center Blvd.

Street Address 2: Suite 420

City, State, Zip: Canonsburg, PA 15317

Work to be Performed: [REDACTED]

—

Estimated percentage of total proposal to be performed by subcontractors: 1 %
(Do **NOT** show dollar amounts here; **show % of WORK** sub-contractors will perform/provide).
Define the part of the work that will be performed by each subcontractor.

Subcontractor's employee information (attach additional pages if needed):

	Nationwide	Ohio Offices
Total Number of Employees	[REDACTED]	-
% of those who are Women	[REDACTED]	-
% of those who are Minorities	[REDACTED]	-

GOVERNMENT BUSINESS AND FUNDING CONTRACTS
In accordance with section 2909.33 of the Ohio Revised Code

DECLARATION REGARDING MATERIAL ASSISTANCE/NONASSISTANCE TO A TERRORIST ORGANIZATION

This form serves as a declaration of the provision of material assistance to a terrorist organization or organization that supports terrorism as identified by the U.S. Department of State Terrorist Exclusion List (see the Ohio Homeland Security Division website for a reference copy of the Terrorist Exclusion List).

Any answer of "yes" to any question, or the failure to answer "no" to any question on this declaration shall serve as a disclosure that material assistance to an organization identified on the U.S. Department of State Terrorist Exclusion List has been provided. Failure to disclose the provision of material assistance to such an organization or knowingly making false statements regarding material assistance to such an organization is a felony of the fifth degree.

For the purposes of this declaration, "material support or resources" means currency, payment instruments, other financial securities, funds, transfer of funds, and financial services that are in excess of one hundred dollars, as well as communications, lodging, training, safe houses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials.

LAST NAME		FIRST NAME		MIDDLE INITIAL
HOME ADDRESS CITY		STATE	ZIP	COUNTY
HOME PHONE		WORK PHONE		

COMPLETE THIS SECTION ONLY IF YOU ARE A COMPANY BUSINESS OR ORGANIZATION

BUSINESS/ORGANIZATION NAME Capital Rx Inc			
BUSINESS ADDRESS 85 Broad Street, Floor 28			
New York	NY	10004	New York
PHONE NUMBER 781-8834			

DECLARATION

In accordance with division (A)(2)(b) of section 2909.32 of the Ohio Revised Code

For each question, indicate either "yes," or "no" in the space provided. Responses must be truthful to the best of your knowledge.

- Are you a member of an organization on the U.S. Department of State Terrorist Exclusion List?
OYes **121** N o
- Have you used any position of prominence you have with any country to persuade others to support an organization on the U.S. Department of State Terrorist Exclusion List?
OYes **'2!** N o

GOVERNMENT BUSINESS AND FUNDING CONTRACTS - CONTINUED

3. Have you knowingly solicited funds or other things of value for an organization on the U.S. Department of State Terrorist Exclusion List?
 O Yes **121** No

4. Have you solicited any individual for membership in an organization on the U.S. Department of State Terrorist Exclusion List?
 O Yes **121** No

5. Have you committed an act that you know, or reasonably should have known, affords "material support or resources" to an organization on the U.S. Department of State Terrorist Exclusion List?
D Yes **121** No

6. Have you hired or compensated a person you knew to be a member of an organization on the U.S. Department of State Terrorist Exclusion List, or a person you knew to be engaged in planning, assisting, or carrying out an act of terrorism?
0 Yes **2J** No

In the event of a denial of a government contract or government funding due to a positive indication that material assistance has been provided to a terrorist organization, or an organization that supports terrorism as identified by the U.S. Department of State Terrorist Exclusion List, a review of the denial may be requested. The request must be sent to the Ohio Department of Public Safety's Division of Homeland Security. The request forms and instructions for filing can be found on the Ohio Homeland Security Division website.

CERTIFICATION

I hereby certify that the answers I have made to all of the questions on this declaration are true to the best of my knowledge. I understand that if this declaration is not completed in its entirety, it will not be processed and I will be automatically disqualified. I understand that I am responsible for the correctness of this declaration. I understand that failure to disclose the provision of material assistance to an organization identified on the U.S. Department of State Terrorist Exclusion List, or knowingly making false statements regarding material assistance to such an organization is a felony of the fifth degree. I understand that any answer of "yes" to any question, or the failure to answer "no" to any question on this declaration shall serve as a disclosure that material assistance to an organization identified on the U.S. Department of State Terrorist Exclusion List has been provided by myself or my organization. If I am signing this on behalf of a company business or organization, I hereby acknowledge that I have the authority to make this certification on behalf of the company, business organization _____ d on page 1 of this declaration .

x _____
 Signature *Bank III*

11/15/20 jd-0
 Date

Request for Taxpayer Identification Number and Certification

Give Form to the requester. Do not send to the IRS.

Go to www.irs.gov/FormW9 for instructions and the latest information.

1 Name (as shown on your income tax return.) Name is required on this line; do not leave this line blank. Capital Rx Inc	
2 Business name/disregarded entity name, if different from above Capital Rx	
3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes. <input type="checkbox"/> Individual sole proprietor or single-member LLC <input checked="" type="checkbox"/> C Corporation <input type="checkbox"/> S Corporation <input type="checkbox"/> Partnership <input type="checkbox"/> Trust/estate <input type="checkbox"/> limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) P Note: Check the appropriate box in the line above for the tax classification of the single member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is not disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.	4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3): Exempt payee code (if any) _____ Exemption from FATCA reporting code (if any) _____
5 Address (number, street, and apt or suite no.) See instructions. 85 Broad Street, Fl 28	Requester's name and address (optional)
6 City, state, and ZIP code New York, NY 10004	
7 list account number(s) here (optional)	

Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the Instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

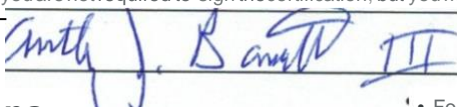
Social security number [I]-[0]-[1][1][1]
or Employer identification number 35 - 2612946

Part II Certification

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
- I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
- I am a U.S. citizen or other U.S. person (defined below); and
- The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person 	Date _____
---	------------

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to www.irs.gov/FormW9.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT Interest earned or paid

- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-8 (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)
Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, later.

By signing the filled-out form, you:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued),
2. Certify that you are not subject to backup withholding, or
3. Claim exemption from backup withholding if you are a U.S. exempt payee. If applicable, you are also certifying that as a U.S. person, your allocable share of any partnership income from a U.S. trade or business is not subject to the withholding tax on foreign partners' share of effectively connected income, and
4. Certify that FATCA code(s) entered on this form (if any) indicating that you are exempt from the FATCA reporting, is correct. See *What is FATCA reporting*, later, for further information.

Note: If you are a U.S. person and a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien;
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States;
- An estate (other than a foreign estate); or
- A domestic trust (as defined in Regulations section 301.7701-7).

Special rules for partnerships. Partnerships that conduct a trade or business in the United States are generally required to pay a withholding tax under section 1446 on any foreign partners' share of effectively connected taxable income from such business. Further, in certain cases where a Form W-9 has not been received, the rules under section 1446 require a partnership to presume that a partner is a foreign person, and pay the section 1446 withholding tax. Therefore, if you are a U.S. person that is a partner in a partnership conducting a trade or business in the United States, provide Form W-9 to the partnership to establish your U.S. status and avoid section 1446 withholding on your share of partnership income.

In the cases below, the following person must give Form W-9 to the partnership for purposes of establishing its U.S. status and avoiding withholding on its allocable share of net income from the partnership conducting a trade or business in the United States.

- In the case of a disregarded entity with a U.S. owner, the U.S. owner of the disregarded entity and not the entity;
- In the case of a grantor trust with a U.S. grantor or other U.S. owner, generally, the U.S. grantor or other U.S. owner of the grantor trust and not the trust; and
- In the case of a U.S. trust (other than a grantor trust), the U.S. trust (other than a grantor trust) and not the beneficiaries of the trust.

Foreign person. If you are a foreign person or the U.S. branch of a foreign bank that has elected to be treated as a U.S. person, do not use Form W-9. Instead, use the appropriate Form W-8 or Form 8233 (see Pub. 515, *Withholding of Tax on Nonresident Aliens and Foreign Entities*).

Nonresident alien who becomes a resident alien. Generally, only a nonresident alien individual may use the terms of a tax treaty to reduce or eliminate U.S. tax on certain types of income. However, most tax treaties contain a provision known as a "saving clause." Exceptions specified in the saving clause may permit an exemption from tax to continue for certain types of income even after the payee has otherwise become a U.S. resident alien for tax purposes.

If you are a U.S. resident alien who is relying on an exception contained in the saving clause of a tax treaty to claim an exemption from U.S. tax on certain types of income, you must attach a statement to Form W-9 that specifies the following five items.

1. The treaty country. Generally, this must be the same treaty under which you claimed exemption from tax as a nonresident alien.
2. The treaty article addressing the income.
3. The article number (or location) in the tax treaty that contains the saving clause and its exceptions.
4. The type and amount of income that qualifies for the exemption from tax.
5. Sufficient facts to justify the exemption from tax under the terms of the treaty article.

Example. Article 20 of the U.S.-China income tax treaty allows an exemption from tax for scholarship income received by a Chinese student temporarily present in the United States. Under U.S. law, this student will become a resident alien for tax purposes if his or her stay in the United States exceeds 5 calendar years. However, paragraph 2 of the first Protocol to the U.S.-China treaty (dated April 30, 1984) allows the provisions of Article 20 to continue to apply even after the Chinese student becomes a resident alien of the United States. A Chinese student who qualifies for this exception (under paragraph 2 of the first protocol) and is relying on this exception to claim an exemption from tax on his or her scholarship or fellowship income would attach to Form W-9 a statement that includes the information described above to support that exemption.

If you are a nonresident alien or a foreign entity, give the requester the appropriate completed Form W-8 or Form 8233.

Backup Withholding

What is backup withholding? Persons making certain payments to you must under certain conditions withhold and pay to the IRS 24% of such payments. This is called "backup withholding." Payments that may be subject to backup withholding include interest, tax-exempt interest, dividends, broker and barter exchange transactions, rents, royalties, nonemployee pay, payments made in settlement of payment card and third party network transactions, and certain payments from fishing boat operators. Real estate transactions are not subject to backup withholding.

You will not be subject to backup withholding on payments you receive if you give the requester your correct TIN, make the proper certifications, and report all your taxable interest and dividends on your tax return.

Payments you receive will be subject to backup withholding if:

1. You do not furnish your TIN to the requester,
2. You do not certify your TIN when required (see the instructions for Part II for details),
3. The IRS tells the requester that you furnished an incorrect TIN,
4. The IRS tells you that you are subject to backup withholding because you did not report all your interest and dividends on your tax return (for reportable interest and dividends only), or
5. You do not certify to the requester that you are not subject to backup withholding under 4 above (for reportable interest and dividend accounts opened after 1983 only).

Certain payees and payments are exempt from backup withholding. See *Exempt payee code*, later, and the separate Instructions for the Requester of Form W-9 for more information.

Also see *Special rules for partnerships*, earlier.

What is FATCA Reporting?

The Foreign Account Tax Compliance Act (FATCA) requires a participating foreign financial institution to report all United States account holders that are specified United States persons. Certain payees are exempt from FATCA reporting. See *Exemption from FATCA reporting code*, later, and the Instructions for the Requester of Form W-9 for more information.

Updating Your Information

You must provide updated information to any person to whom you claimed to be an exempt payee if you are no longer an exempt payee and anticipate receiving reportable payments in the future from this person. For example, you may need to provide updated information if you are a C corporation that elects to be an S corporation, or if you no longer are tax exempt. In addition, you must furnish a new Form W-9 if the name or TIN changes for the account; for example, if the grantor of a grantor trust dies.

Penalties

Failure to furnish TIN. If you fail to furnish your correct TIN to a requester, you are subject to a penalty of \$50 for each such failure unless your failure is due to reasonable cause and not to willful neglect.

Civil penalty for false information with respect to withholding. If you make a false statement with no reasonable basis that results in no backup withholding, you are subject to a \$500 penalty.

Criminal penalty for falsifying information. Willfully falsifying certifications or affirmations may subject you to criminal penalties including fines and/or imprisonment.

Misuse of TINs. If the requester discloses or uses TINs in violation of federal law, the requester may be subject to civil and criminal penalties.

Specific Instructions

Line 1

You must enter one of the following on this line; **do not** leave this line blank. The name should match the name on your tax return.

If this Form W-9 is for a joint account (other than an account maintained by a foreign financial institution (FFI)), list first, and then circle, the name of the person or entity whose number you entered in Part I of Form W-9. If you are providing Form W-9 to an FFI to document a joint account, each holder of the account that is a U.S. person must provide a Form W-9.

a. **Individual.** Generally, enter the name shown on your tax return. If you have changed your last name without informing the Social Security Administration (SSA) of the name change, enter your first name, the last name as shown on your social security card, and your new last name.

Note: ITIN applicant: Enter your individual name as it was entered on your Form W-7 application, line 1a. This should also be the same as the name you entered on the Form 1040/1040A/1040EZ you filed with your application.

b. **Sole proprietor or single-member LLC.** Enter your individual name as shown on your 1040/1040A/1040EZ on line 1. You may enter your business, trade, or "doing business as" (DBA) name on line 2.

c. **Partnership, LLC that is not a single-member LLC, C corporation, or S corporation.** Enter the entity's name as shown on the entity's tax return on line 1 and any business, trade, or DBA name on line 2.

d. **Other entities.** Enter your name as shown on required U.S. federal tax documents on line 1. This name should match the name shown on the charter or other legal document creating the entity. You may enter any business, trade, or DBA name on line 2.

e. **Disregarded entity.** For U.S. federal tax purposes, an entity that is disregarded as an entity separate from its owner is treated as a "disregarded entity." See Regulations section 301.7701-2(c)(2)(iii). Enter the owner's name on line 1. The name of the entity entered on line 1 should never be a disregarded entity. The name on line 1 should be the name shown on the income tax return on which the income should be reported. For example, if a foreign LLC that is treated as a disregarded entity for U.S. federal tax purposes has a single owner that is a U.S. person, the U.S. owner's name is required to be provided on line 1. If the direct owner of the entity is also a disregarded entity, enter the first owner that is not disregarded for federal tax purposes. Enter the disregarded entity's name on line 2, "Business name/disregarded entity name." If the owner of the disregarded entity is a foreign person, the owner must complete an appropriate Form W-8 instead of a Form W-9. This is the case even if the foreign person has a U.S. TIN.

Line 2

If you have a business name, trade name, DBA name, or disregarded entity name, you may enter it on line 2.

Line 3

Check the appropriate box on line 3 for the U.S. federal tax classification of the person whose name is entered on line 1. Check only one box on line 3.

IF the entity/person on line 1 is a(n) . . .	THEN check the box for . . .
• Corporation	Corporation
• Individual • Sole proprietorship, or • Single-member limited liability company (LLC) owned by an individual and disregarded for U.S. federal tax purposes.	Individual/sole proprietor or single-member LLC
• LLC treated as a partnership for U.S. federal tax purposes, • LLC that has filed Form 8832 or 2553 to be taxed as a corporation, or • LLC that is disregarded as an entity separate from its owner but the owner is another LLC that is not disregarded for U.S. federal tax purposes.	Limited liability company and enter the appropriate tax classification. (P= Partnership; C= C corporation; or S= S corporation)
• Partnership	Partnership
• Trust/estate	Trust/estate

Line 4, Exemptions

If you are exempt from backup withholding and/or FATCA reporting, enter in the appropriate space on line 4 any code(s) that may apply to you.

Exempt payee code.

- Generally, individuals (including sole proprietors) are not exempt from backup withholding.
- Except as provided below, corporations are exempt from backup withholding for certain payments, including interest and dividends.
- Corporations are not exempt from backup withholding for payments made in settlement of payment card or third party network transactions.
- Corporations are not exempt from backup withholding with respect to attorneys' fees or gross proceeds paid to attorneys, and corporations that provide medical or health care services are not exempt with respect to payments reportable on Form 1099-MISC.

The following codes identify payees that are exempt from backup withholding. Enter the appropriate code in the space in line 4.

- 1—An organization exempt from tax under section 501(a), any IRA, or a custodial account under section 403(b)(7) if the account satisfies the requirements of section 401(f)(2)
- 2—The United States or any of its agencies or instrumentalities³—
A state, the District of Columbia, a U.S. commonwealth or possession, or any of their political subdivisions or instrumentalities
- 4—A foreign government or any of its political subdivisions, agencies, or instrumentalities
- 5—A corporation
- 6—A dealer in securities or commodities required to register in the United States, the District of Columbia, or a U.S. commonwealth or possession
- 7—A futures commission merchant registered with the Commodity Futures Trading Commission
- 8—A real estate investment trust
- 9—An entity registered at all times during the tax year under the Investment Company Act of 1940
- 10—A common trust fund operated by a bank under section 584(a)¹¹—
A financial institution
- 12—A middleman known in the investment community as a nominee or custodian
- 13—A trust exempt from tax under section 664 or described in section 4947

The following chart shows types of payments that may be exempt from backup withholding. The chart applies to the exempt payees listed above, 1 through 13.

IF the payment is for . . .	THEN the payment is exempt for . . .
Interest and dividend payments	All exempt payees except for 7
Broker transactions	Exempt payees 1 through 4 and 6 through 11 and all C corporations. S corporations must not enter an exempt payee code because they are exempt only for sales of noncovered securities acquired prior to 2012.
Barter exchange transactions and patronage dividends	Exempt payees 1 through 4
Payments over \$600 required to be reported and direct sales over \$5,000 ¹	Generally, exempt payees 1 through 5 ²
Payments made in settlement of payment card or third party network transactions	Exempt payees 1 through 4

¹ See Form 1099-MISC, Miscellaneous Income, and its instructions.

² However, the following payments made to a corporation and reportable on Form 1099-MISC are not exempt from backup withholding: medical and health care payments, attorneys' fees, gross proceeds paid to an attorney reportable under section 6045(f), and payments for services paid by a federal executive agency.

Exemption from FATCA reporting code. The following codes identify payees that are exempt from reporting under FATCA. These codes apply to persons submitting this form for accounts maintained outside of the United States by certain foreign financial institutions. Therefore, if you are only submitting this form for an account you hold in the United States, you may leave this field blank. Consult with the person requesting this form if you are uncertain if the financial institution is subject to these requirements. A requester may indicate that a code is not required by providing you with a Form W-9 with "Not Applicable" (or any similar indication) written or printed on the line for a FATCA exemption code.

A—An organization exempt from tax under section 501(a) or any individual retirement plan as defined in section 7701(a)(37)

B—The United States or any of its agencies or instrumentalities

C—A state, the District of Columbia, a U.S. commonwealth or possession, or any of their political subdivisions or instrumentalities

D—A corporation the stock of which is regularly traded on one or more established securities markets, as described in Regulations section 1.1472-1(c)(1)(i)

E—A corporation that is a member of the same expanded affiliated group as a corporation described in Regulations section 1.1472-1(c)(1)(i)

F—A dealer in securities, commodities, or derivative financial instruments (including notional principal contracts, futures, forwards, and options) that is registered as such under the laws of the United States or any state

G—A real estate investment trust

H—A regulated investment company as defined in section 851 or an entity registered at all times during the tax year under the Investment Company Act of 1940

I—A common trust fund as defined in section 584(a)J—

A bank as defined in section 581

K—A broker

L—A trust exempt from tax under section 664 or described in section 4947(a)(1)

M—A tax exempt trust under a section 403(b) plan or section 457(g) plan

Note: You may wish to consult with the financial institution requesting this form to determine whether the FATCA code and/or exempt payee code should be completed.

Line 5

Enter your address (number, street, and apartment or suite number). This is where the requester of this Form W-9 will mail your information returns. If this address differs from the one the requester already has on file, write NEW at the top. If a new address is provided, there is still a chance the old address will be used until the payor changes your address in their records.

Line 6

Enter your city, state, and ZIP code.

Part I. Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. If you are a resident alien and you do not have and are not eligible to get an SSN, your TIN is your IRS individual taxpayer identification number (ITIN). Enter it in the social security number box. If you do not have an ITIN, see *How to get a TIN* below.

If you are a sole proprietor and you have an EIN, you may enter either your SSN or EIN.

If you are a single-member LLC that is disregarded as an entity separate from its owner, enter the owner's SSN (or EIN, if the owner has one). Do not enter the disregarded entity's EIN. If the LLC is classified as a corporation or partnership, enter the entity's EIN.

Note: See *What Name and Number To Give the Requester*, later, for further clarification of name and TIN combinations.

How to get a TIN. If you do not have a TIN, apply for one immediately. To apply for an SSN, get Form SS-5, Application for a Social Security Card, from your local SSA office or get this form online at www.SSA.gov. You may also get this form by calling 1-800-772-1213. Use Form W-7, Application for IRS Individual Taxpayer Identification Number, to apply for an ITIN, or Form SS-4, Application for Employer Identification Number, to apply for an EIN. You can apply for an EIN online by accessing the IRS website at www.irs.gov/Businesses and clicking on Employer Identification Number (EIN) under Starting a Business. Go to www.irs.gov/Forms to view, download, or print Form W-7 and/or Form SS-4. Or, you can go to www.irs.gov/OrderForms to place an order and have Form W-7 and/or SS-4 mailed to you within 10 business days.

If you are asked to complete Form W-9 but do not have a TIN, apply for a TIN and write "Applied For" in the space for the TIN, sign and date the form, and give it to the requester. For interest and dividend payments, and certain payments made with respect to readily tradable instruments, generally you will have 60 days to get a TIN and give it to the requester before you are subject to backup withholding on payments. The 60-day rule does not apply to other types of payments. You will be subject to backup withholding on all such payments until you provide your TIN to the requester.

Note: Entering "Applied For" means that you have already applied for a TIN or that you intend to apply for one soon.

Caution: A disregarded U.S. entity that has a foreign owner must use the appropriate Form W-8.

Part II. Certification

To establish to the withholding agent that you are a U.S. person, or resident alien, sign Form W-9. You may be requested to sign by the withholding agent even if item 1, 4, or 5 below indicates otherwise.

For a joint account, only the person whose TIN is shown in Part I should sign (when required). In the case of a disregarded entity, the person identified on line 1 must sign. Exempt payees, see *Exempt payee code*, earlier.

Signature requirements. Complete the certification as indicated in items 1 through 5 below.

1. Interest, dividend, and barter exchange accounts opened before 1984 and broker accounts considered active during 1983.

You must give your correct TIN, but you do not have to sign the certification.

2. Interest, dividend, broker, and barter exchange accounts opened after 1983 and broker accounts considered inactive during 1983. You must sign the certification or backup withholding will apply. If you are subject to backup withholding and you are merely providing your correct TIN to the requester, you must cross out item 2 in the certification before signing the form.

3. Real estate transactions. You must sign the certification. You may cross out item 2 of the certification.

4. Other payments. You must give your correct TIN, but you do not have to sign the certification unless you have been notified that you have previously given an incorrect TIN. "Other payments" include payments made in the course of the requester's trade or business for rents, royalties, goods (other than bills for merchandise), medical and health care services (including payments to corporations), payments to a nonemployee for services, payments made in settlement of payment card and third party network transactions, payments to certain fishing boat crew members and fishermen, and gross proceeds paid to attorneys (including payments to corporations).

5. Mortgage interest paid by you, acquisition or abandonment of secured property, cancellation of debt, qualified tuition program payments (under section 529), ABLE accounts (under section 529A), IRA, Coverdell ESA, Archer MSA or HSA contributions or distributions, and pension distributions. You must give your correct TIN, but you do not have to sign the certification.

What Name and Number To Give the Requester

For this type of account:	Give name and SSN of:
1. Individual	The individual
2. Two or more individuals (joint account) other than an account maintained by an FFI	The actual owner of the account or, if combined funds, the first individual on the account ¹
3. Two or more U.S. persons (joint account maintained by an FFI)	Each holder of the account
4. Custodial account of a minor (Uniform Gift to Minors Act)	The minor ²
5. a. The usual revocable savings trust (grantor is also trustee) b. So-called trust account that is not a legal or valid trust under state law	The grantor-trustee ¹ The actual owner ¹
6. Sole proprietorship or disregarded entity owned by an individual	The owner ³
7. Grantor trust filing under Optional Form 1099 Filing Method 1 (see Regulations section 1.671-4(b)(2)(i)(A))	The grantor ⁴
For this type of account:	Give name and EIN of:
8. Disregarded entity not owned by an individual	The owner
9. A valid trust, estate, or pension trust	Legal entity ⁴
10. Corporation or LLC electing corporate status on Form 8832 or Form 2553	The corporation
11. Association, club, religious, charitable, educational, or other tax-exempt organization	The organization
12. Partnership or multi-member LLC	The partnership
13. A broker or registered nominee	The broker or nominee

For this type of account:	Give name and EIN of:
14. Account with the Department of Agriculture in the name of a public entity (such as a state or local government, school district, or prison) that receives agricultural program payments	The public entity
15. Grantor trust filing under the Form 1041 Filing Method or the Optional Form 1099 Filing Method 2 (see Regulations section 1.671-4(b)(2)(j)(B))	The trust

¹ List first and circle the name of the person whose number you furnish. If only one person on a joint account has an SSN, that person's number must be furnished.

² Circle the minor's name and furnish the minor's SSN.

³ You must show your individual name and you may also enter your business or DBA name on the "Business name/disregarded entity" name line. You may use either your SSN or EIN (if you have one), but the IRS encourages you to use your SSN.

⁴ List first and circle the name of the trust, estate, or pension trust. (Do not furnish the TIN of the personal representative or trustee unless the legal entity itself is not designated in the account title.) Also see *Special rules for partnerships*, earlier.

***Note:** The grantor also must provide a Form W-9 to trustee of trust.

Note: If no name is circled when more than one name is listed, the number will be considered to be that of the first name listed.

Secure Your Tax Records From Identity Theft

Identity theft occurs when someone uses your personal information such as your name, SSN, or other identifying information, without your permission, to commit fraud or other crimes. An identity thief may use your SSN to get a job or may file a tax return using your SSN to receive a refund.

To reduce your risk:

- Protect your SSN,
- Ensure your employer is protecting your SSN, and
- Be careful when choosing a tax preparer.

If your tax records are affected by identity theft and you receive a notice from the IRS, respond right away to the name and phone number printed on the IRS notice or letter.

If your tax records are not currently affected by identity theft but you think you are at risk due to a lost or stolen purse or wallet, questionable credit card activity or credit report, contact the IRS Identity Theft Hotline at 1-800-908-4490 or submit Form 14039.

For more information, see Pub. 5027, Identity Theft Information for Taxpayers.

Victims of identity theft who are experiencing economic harm or a systemic problem, or are seeking help in resolving tax problems that have not been resolved through normal channels, may be eligible for Taxpayer Advocate Service (TAS) assistance. You can reach TAS by calling the TAS toll-free case intake line at 1-877-777-4778 or TTY/TDD 1-800-829-4059.

Protect yourself from suspicious emails or phishing schemes.

Phishing is the creation and use of email and websites designed to mimic legitimate business emails and websites. The most common act is sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The IRS does not initiate contacts with taxpayers via emails. Also, the IRS does not request personal detailed information through email or ask taxpayers for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

If you receive an unsolicited email claiming to be from the IRS, forward this message to phishing@irs.gov. You may also report misuse of the IRS name, logo, or other IRS property to the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484. You can forward suspicious emails to the Federal Trade Commission at spam@uce.gov or report them at www.ftc.gov/complaint. You can contact the FTC at www.ftc.gov/idtheft or 877-IDTHEFT (877-438-4338). If you have been the victim of identity theft, see www.IdentityTheft.gov and Pub. 5027.

Visit www.irs.gov/IdentityTheft to learn more about identity theft and how to reduce your risk.

Privacy Act Notice

Section 6109 of the Internal Revenue Code requires you to provide your correct TIN to persons (including federal agencies) who are required to file information returns with the IRS to report interest, dividends, or certain other income paid to you; mortgage interest you paid; the acquisition or abandonment of secured property; the cancellation of debt; or contributions you made to an IRA, Archer MSA, or HSA. The person collecting this form uses the information on the form to file information returns with the IRS, reporting the above information. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation and to cities, states, the District of Columbia, and U.S. commonwealths and possessions for use in administering their laws. The information also may be disclosed to other countries under a treaty, to federal and state agencies to enforce civil and criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. You must provide your TIN whether or not you are required to file a tax return. Under section 3406, payers must generally withhold a percentage of taxable interest, dividend, and certain other payments to a payee who does not give a TIN to the payer. Certain penalties may also apply for providing false or fraudulent information.

June 28, 2019

Background

Internal Audit performs an annual HIPAA security risk analysis focused on the safeguarding of Magellan's key electronic Protected Health Information (ePHI) assets and the data they house. Magellan stores, processes, and transmits Protected Health Information (PHI), which includes ePHI. The use, protection and disclosure of this information is subject to requirements set forth in the Final Privacy Rule and the Final Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including modifications resulting from the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Omnibus Rule of 2013.

Scope of Review

Leveraging existing guidance and interpretation of HIPAA security risk analysis requirements (§164.308(a)(1)(ii)(A)), independent third-party assessments for SOC2 and HITRUST and internal SOX control assessments for 2018, Internal Audit analyzed the state of threats and vulnerabilities to the security, confidentiality, integrity, and availability of applicable ePHI. Internal Audit facilitated risk assessments for a sample of 35 key system owners within the organization to assess each systems' ability to implement controls to prevent the aforementioned threats and vulnerabilities. Risk was evaluated for the total number of threat/vulnerability pairs across media type (server, desktop, laptop, mobile, etc.) through which each application provides access to ePHI. Each pair was assigned a risk ranking and the identified risks were ranked in order of the risk level. For a list of applications in scope refer to **Appendix A**.

Conclusion

Threats and vulnerabilities associated with the security, confidentiality, integrity, and availability of ePHI were evaluated for each system and in aggregate as an organization. Key areas identified for further oversight and improvement were Identity & Access Management, Application Development Security and Vulnerability Management. The assessment noted that the Office of Information Security, under the direction of the Chief Information Security Officer, is actively monitoring the various risks these threats and vulnerabilities represent (including those cited above) and is actively tracking any known gaps and issues in the ServiceNow GRC platform. Internal Audit will be following up on the status of mitigation of these risk areas.

Appendix A

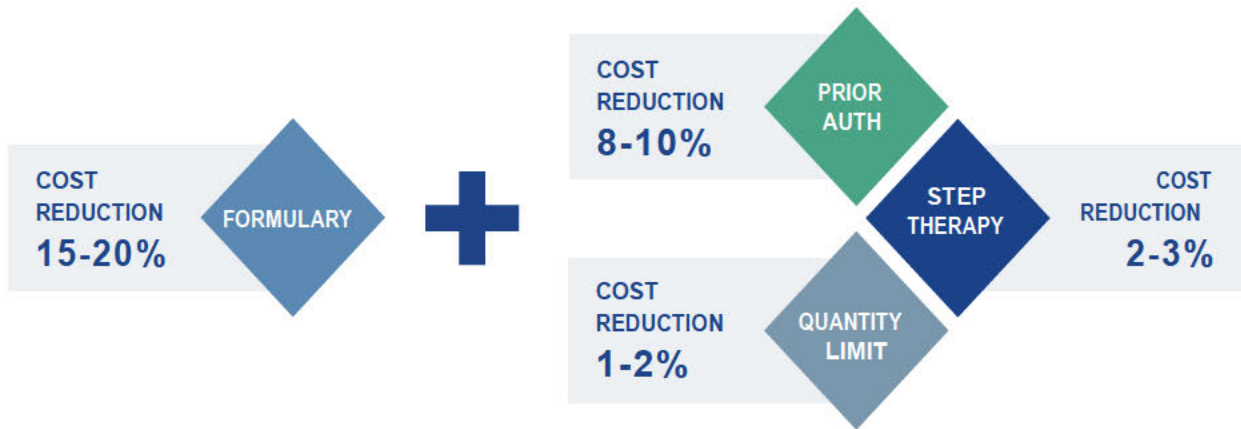
The following applications are business critical systems that were selected for this Assessment:

- Avaya WFO (Work Force Optimization)
- BBI
- CAPS / RCAPS
- Case Trakker
- CCIS
- CDMI – MRS*
- Correspondence Publisher (MHC)
- Correspondence Publisher (MRx)
- CPR+
- CRM*
- Data Warehouse
- eRebate AWS
- FirstFinancial
- FirstIQ
- FirstRebate*
- FirstRx Claims Engine
- Florida Blue*
- Glacier
- Integrate
- Integrated Product (IP)
- IPD CorrPub – CIA*
- IPD / RPD*
- LEVI
- MagellanAssist
- MagellanProvider
- MRx Assist
- MRx Explore
- MRx Auth
- ODS
- Pharmacy Data Management System (PDMS)
- Pharmacy Data Warehouse (PDW)
- QNXT
- TDS Financial
- Total Member Record
- TruCare

**Applications identified as not containing ePHI.*

Clinical Management Prior Authorization Overview

Capital Rx offers a complete suite of formulary and clinical programs included in our core services. Through strategic formulary placement decisions, we deliver annual savings of 15-20% for plan sponsors. To enhance our ability to realize lowest net cost, our clinical services also include customizable utilization management programs – such as quantity limits, step therapy and prior authorizations. Collectively, these levers can drive an additional 10-15% in annual savings. To address the specific benefit goals of each sponsor, Capital Rx remains agile and unconflicted, dedicated to delivering a clinical framework to manage costs and improve patient outcomes.



Prior Authorization Work Flow

STANDARD PROCESS		HIGH-TOUCH PROCESS	
Rx sent to pharmacy	PA Requirement Identified	Rx sent to pharmacy	The PA team monitors claims and pro-actively contacts providers to initiate the PA process
Rx rejected for PA		Rx rejected for PA	
Pharmacist informs member and provider		Pharmacist informs member and provider	
Member or Provider initiate the PA process	PA Initiation and Review	The clinical reviewer performs additional outreach to discuss treatment options and collect additional information if necessary	The clinical reviewer and provider agree on a decision
Additional information is obtained by the PA team from the provider's office if necessary		The coverage determination is communicated to the provider and member in real-time via a telephonic call and followed by a letter	
The PA is reviewed by the clinical reviewer and a coverage determination is made	PA Decision and Communication	The coverage determination is communicated to the provider and member in real-time via a telephonic call and followed by a letter	
The coverage determination is communicated to the provider and member via a letter			

Prior Authorization Management Approach

Prior Authorization (PA) Management Approach	Open	Managed	High-Touch
 <p>Description</p>	Benefit has no prior authorization review requirements	Benefit requires prior authorization review for select drugs	Benefit requires prior authorization review for select drugs Review process involves high-touch pro-active communication between the PBM, member and provider
 <p>Member/Provider Experience</p>	Prescription is dispensed without a PA rejection	Prescription rejects for PA review Member or provider initiates the PA review PA team only initiates outreach if additional information is required Coverage determination (and appeal rights) are communicated to both member and provider	Prescription rejects for PA review PA team monitors claims and initiates PA review via direct outreach Clinical reviewer initiates additional outreach if more information is required Clinical reviewer also actively engages the provider and shares recommendations on the most appropriate and cost-effective option Coverage determination (and appeal rights) are communicated to both member and provider in real-time
 <p>Pros</p>	check Mitigates delay of care concerns check Reduces administrative burden for member and provider	check Deploys key cost containment lever check Ensures ability to validate appropriateness of care	check Deploys key cost containment lever check Ensures ability to validate appropriateness of care check PA review process is initiated and triaged actively check High-touch service lowers administrative burden and mitigates delay of care
 <p>Cons</p>	Times Limits ability to validate the appropriateness of care Times Removes key cost containment lever	Times PA review process is initiated and triaged passively Times May delay care	



Powered by technology.
Inspired by humanity.

Human Capital Reporting turns human resources data into actionable strategies.

With our Human Capital Reporting solution, we're taking a data-driven approach to understanding the total cost of care by offering unmatched insights into health benefits and the effect on plan performance.

By combining pharmacy + medical + human resources data into one innovative platform, our advanced analytics derive relationships that offer a holistic view of healthcare utilization. Data integration allows our experts to recommend specific programs that measure ROI across the entire human resources budget and advance the health of the population.



MEDICAL DATA

PHARMACY DATA

TIME & ATTENDANCE DATA

SALARY & PAYROLL DATA



PHARMACY DATA

Cohort A	3,962 receive Flu Vaccine	= \$148,000
Cohort B	2,788 skip Flu Vaccine	= \$0



MEDICAL DATA

Cohort A	425 sick office visits	= \$132,000	(\$33 per employee)
Cohort B	401 sick office visits	= \$125,000	(\$44 per employee)



PAYROLL & SICK DAYS

Cohort A	8.2 sick days	= \$0	
Cohort B	9.1 sick days	= \$923,000	+0.9 sick days

Why data integration matters

Challenge: Healthcare costs are too high

- Client requested to limit flu vaccines for employees to stay under budget

Solution: Shift the mindset from cost to investment

- To illustrate the global impact for all employees to have a flu vaccine, we combined the client's medical, pharmacy and time & attendance data for analysis in our human capital platform

Impact: An enormous ROI

- The investment in flu vaccines was \$148,000, but it resulted in one less sick day for employees
- Gaining just one full day back of attendance delivered \$2.5 million in savings!



Letter of Certification

January 22, 2018

Magellan Health
14100 Magellan Plaza
Maryland Heights, MO 63043

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an approved HITRUST CSF Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST CSF Assurance Program, the following system and its supporting applications of the organization meet the HITRUST CSF v8.1 Certification Criteria:

Magellan Health – Pharmacy Services system and its supporting applications

The certification is valid for a period of two years assuming the following occurs:

- A monitoring program is in place to determine if the controls continue to operate effectively over time
- No data security breach reportable to a federal or state agency by law or regulation has occurred
- No significant changes in the business or security policies, practices, controls and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria
- Annual progress is being made on areas identified in the Corrective Action Plan (CAP)
- Timely completion of the interim review as defined in the HITRUST CSF Assurance Program Requirements

HITRUST performs a limited quality assurance review of the assessment to ensure that the scores are consistent with the testing performed by the HITRUST Assessor organization. Certification is specific to the maturity of the HITRUST CSF controls implemented to address the outcomes specified by the NIST CsF Subcategories.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information security tailored to the healthcare industry. With input from leading organizations within the industry, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For those HITRUST CSF control requirements that are not currently being met, the organization must have a CAP that outlines its plans for meeting such requirements.

A full copy of the certification report has also been issued to the organization listed above. This full report includes additional details on the scope of the assessment, a representation letter from management, testing results for those controls required for certification, a benchmark report comparing the organization's results to industry results, details on CAPs required for certification, as well as the completed questionnaire. If interested in obtaining a copy of the full report, you will need to contact the organization directly.



Additional information on the HITRUST CSF Certification program can be found at the HITRUST website: www.hitrustalliance.net.



HITRUST

1. Introduction

Capital Rx, Inc (“Capital Rx”) is committed to ensuring the confidentiality, privacy, integrity, and availability of all electronic protected health information (ePHI) it receives, maintains, processes and/or transmits on behalf of its Customers. As providers of compliant, hosted software used by health plans, health technology vendors, developers, designers, agencies, custom development shops, and enterprises, Capital Rx strives to maintain compliance, proactively address information security, mitigate risk for its Customers, and assure known breaches are completely and effectively communicated in a timely manner. The following documents address core policies used by Capital Rx to maintain compliance and assure the proper protections of infrastructure used to store, process, and transmit ePHI for Capital Rx Customers.

Capital Rx provides secure and compliant cloud-based software. This hosted software can generally be described as **Software as a Service (SaaS)**.

1.1 Software as a Service (SaaS)

Capital Rx utilizes the software it has developed as to provide services directly to Customers. In addition, Customers may use Capital Rx SaaS products directly. This software is run, managed, maintained, and under the full control of Capital Rx. No aspects of compliance relating the SaaS offering are inherited; all are the responsibility of Capital Rx.

1.2 Compliance Inheritance

Capital Rx provides compliant hosted software infrastructure for its Customers. Capital Rx is in the process of completing a HIPAA compliance audit by a national third-party compliance firm to validate and map organizational policies and technical controls to HIPAA rules. Capital Rx’s company policies, procedures, and technologies map to HITRUST Certified controls and Capital Rx will be initiating the HITRUST Certification process in the near future. Capital Rx’s service offerings are available on AWS.

1.3 Capital Rx Organizational Concepts

The physical infrastructure environment is hosted at Amazon Web Services (AWS). The network components and supporting network infrastructure are contained within the AWS infrastructures and managed by AWS. Capital Rx does not have physical access into the network components. The Capital Rx environment consists of AWS-managed services which Capital Rx utilizes in

accordance with Capital Rx's Business Associate Agreement with AWS and a very limited number of Capital Rx managed EC2 servers running Ubuntu Linux.

Within the Capital Rx Platform on AWS, all data transmission is encrypted and all hard drives are encrypted so data at rest is also encrypted; this applies to all servers - those hosting Docker containers, databases, APIs, log servers, etc. Capital Rx assumes all data *may* contain ePHI, even though our Risk Assessment does not indicate this is the case, and provides appropriate protections based on that assumption.

Data and network segmentation within AWS are achieved with AWS Accounts, VPCs, VPC subnets, subnet routing, and Security Groups as appropriate.

Additionally, security groups are used on each server for logical segmentation. Security Groups are configured to restrict access to only justified ports and protocols. Capital Rx has implemented strict logical access controls so that only authorized personnel are given access to the internal management servers.

Certain servers and services are directly accessible via the internet. These servers are necessary to allow the exchange of data with and enable connectivity to the outside world. For example, SFTP servers, bastion hosts, and API endpoints for public-facing services are accessible via the internet. All servers where ePHI resides are located on the internal Capital Rx network and can only be accessed indirectly via a public-facing server. Access to the internal database is restricted to a limited number of personnel and strictly controlled to only those personnel with a business-justified reason. Direct remote access to internal servers is not possible.

All software and operating systems are tested end-to-end for usability, security, and impact prior to deployment to production.

1.4 Requesting Audit and Compliance Reports

Capital Rx, at its sole discretion, shares audit reports, including its HITRUST reports and Corrective Action Plans (CAPs), with customers on a case by case basis. All audit reports are shared under explicit NDA in Capital Rx format between Capital Rx and party to receive materials. Audit reports can be requested by Capital Rx workforce members for Customers or directly by Capital Rx Customers.

The following process is used to request audit reports:

1. Email is sent to compliance@cap-rx.com. In the email, please specify the type of report being requested and any required timelines for the report.
2. Capital Rx staff will log an issue with the details of the request into the Capital Rx Quality Management System. The Capital Rx Quality Management System is used to track requests' status and outcomes.

3. Capital Rx will confirm if a current NDA is in place with the party requesting the audit report. If there is no NDA in place, Capital Rx will send one for execution.
4. Once it has been confirmed that an NDA is executed, Capital Rx staff will move the issue to “Under Review”.
5. The Capital Rx Security Officer or Privacy Officer must Approve or Reject the Issue. If the Issue is rejected, Capital Rx will notify the requesting party that we cannot share the requested report.
6. If the issue has been Approved, Capital Rx will send the customer the requested audit report and complete the Quality Management System issue for the request.

1.5 Version Control

Refer to the GitHub repository at <https://github.com/capitalrx/policies>.
capitalrx.com/ for the full version history of these policies.

2. HIPAA Inheritance

2.1 HIPAA Inheritance for SaaS Customers

Not applicable at this time.

2.2 HIPAA Inheritance for PaaS Customers

Not applicable at this time.

3. Policy Management Policy

Capital Rx implements policies and procedures to maintain compliance and integrity of data. The Security Officer and Privacy Officer are responsible for maintaining policies and procedures and assuring all Capital Rx workforce members, business associates, customers, and partners are adherent to all applicable policies. Previous versions of policies are retained to assure ease of finding policies at specific historic dates in time.

3.1 Applicable Standards

3.1.1 Applicable Standards from the HITRUST Common Security Framework

- 12.c - Developing and Implementing Continuity Plans Including Information Security

3.1.2 Applicable Standards from the HIPAA Security Rule

- 164.316(a) - Policies and Procedures
- 164.316(b)(1)(i) - Documentation

3.2 Maintenance of Policies

1. All policies are stored and updated to maintain Capital Rx compliance with HIPAA, HITRUST, NIST, and other relevant standards. Updates and version control are done similarly to source code control.
2. Policy update requests can be made by any workforce member at any time. Furthermore, all policies are reviewed annually by both the Security and Privacy Officer to assure they are accurate and up-to-date.
3. Capital Rx employees may request changes to policies using the following process:
4. The Capital Rx employee initiates a policy change request by creating an Issue in the Capital Rx Quality Management System. The change request may optionally include a GitHub pull request from a separate branch or repository containing the desired changes.
5. The Security Officer or the Privacy Officer is assigned to review the policy change request.
6. Once the review is completed, the Security Officer or Privacy Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
7. If the review is approved, the Security Officer or Privacy Officer then marks the Issue as Done, adding any pertinent notes required.

8. If the policy change requires technical modifications to production systems, those changes are carried out by authorized personnel using Capital Rx's change management process (§9.4).
9. All policies are made accessible to all Capital Rx workforce members. The current master policies are published internally via Capital Rx's Dropbox.
 - Changes are automatically communicated to all Capital Rx team members through integrations between GitHub and Slack that log all GitHub policy channels to a dedicated Capital Rx Slack Channel.
 - The Security Officer also communicates policy changes to all employees via email. These emails include a high-level description of the policy change using terminology appropriate for the target audience.
5. All policies, and associated documentation, are retained for 6 years from the date of its creation or the date when it last was in effect, whichever is later
6. Version history of all Capital Rx policies is done via GitHub.
7. Backup storage of all policies is done with Dropbox.
8. The policies and information security policies are reviewed and audited annually, or after significant changes occur to Capital Rx's organizational environment. Issues that come up as part of this process are reviewed by Capital Rx management to assure all risks and potential gaps are mitigated and/or fully addressed. The process for reviewing policies is outlined below:
9. The Security Officer initiates the policy review by creating an Issue in the Capital Rx Quality Management System.
10. The Security Officer or the Privacy Officer is assigned to review the current Capital Rx policies.
11. If changes are made, the above process is used. All changes are documented in the Issue.
12. Once the review is completed, the Security Officer or Privacy Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
13. If the review is approved, the Security Officer or Privacy Officer then marks the Issue as Done, adding any pertinent notes required.
14. Policy review is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.
15. Capital Rx utilizes the HITRUST MyCSF framework to track compliance with the HITRUST CSF on an annual basis. Capital Rx also tracks compliance with HIPAA. In order to track and measure adherence on an annual basis, Capital Rx uses the following process to track HITRUST audits, both full and interim:
 16. The Security Officer initiates the HITRUST audit activity by creating an Issue in the Capital Rx Quality Management System.
 17. The Security Officer or the Privacy Officer is assigned to own and manage the HITRUST activity.
 18. Once the HITRUST activity is completed, the Security Officer approves or rejects the Issue.

19. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
 20. Compliance with annual compliance assessments, utilizing the HITRUST CSF as a framework, is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.
- Additional documentation related to maintenance of policies is outlined in §5.3.1.

4. Risk Management Policy

This policy establishes the scope, objectives, and procedures of Capital Rx's information security risk management process. The risk management process is intended to support and protect the organization and its ability to fulfill its mission.

4.1 Applicable Standards

4.1.1 Applicable Standards from the HITRUST Common Security Framework

- 03.a - Risk Management Program Development
- 03.b - Performing Risk Assessments
- 03.c - Risk Mitigation

4.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308(a)(1)(ii)(A) - HIPAA Security Rule Risk Analysis
- 164.308(a)(1)(ii)(B) - HIPAA Security Rule Risk Management
- 164.308(a)(8) - HIPAA Security Rule Evaluation

4.2 Risk Management Policies

1. It is the policy of Capital Rx to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) (and other confidential and proprietary electronic information) it stores, transmits, and/or processes for its Customers and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the Capital Rx's information security program.
2. Risk analysis and risk management are recognized as important components of Capital Rx's corporate compliance program and information security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).
3. Risk assessments are done throughout product life cycles:
4. Before the integration of new system technologies and before changes are made to Capital Rx physical safeguards; and

- These changes do not include routine updates to existing systems, deployments of new systems created based on previously configured systems, deployments of new Customers, or new code developed for operations and management of the Capital Rx Platform.
5. While making changes to Capital Rx physical equipment and facilities that introduce new, untested configurations.
 6. Capital Rx performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI.
 7. Capital Rx implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
 8. Ensure the confidentiality, integrity, and availability of all ePHI Capital Rx receives, maintains, processes, and/or transmits for its Customers;
 9. Protect against any reasonably anticipated threats or hazards to the security or integrity of Customer ePHI;
 10. Protect against any reasonably anticipated uses or disclosures of Customer ePHI that are not permitted or required; and
 11. Ensure compliance by all workforce members.
 12. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the senior management and Capital Rx's Security Officer.
 13. All Capital Rx workforce members are expected to fully cooperate with all persons charged with doing risk management work, including contractors and audit personnel. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation, as outlined in the Capital Rx Roles Policy.
 14. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of Capital Rx's Security Officer (or other designated employee), and the identified Risk Management Team.
 15. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.
 16. The details of the Risk Management Process, including risk assessment, discovery, and mitigation, are outlined in detail below. The process is tracked, measured, and monitored using the following procedures:
 17. The Security Officer or the Privacy Officer initiates the Risk Management Procedures by creating an Issue in the Capital Rx Quality Management System.
 18. The Security Officer or the Privacy Officer is assigned to carry out the Risk Management Procedures.
 19. All findings are documented in an approved spreadsheet that is linked to the Issue.
 20. Once the Risk Management Procedures are complete, along with corresponding documentation, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.

21. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
22. The Risk Management Procedure is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.

4.3 Risk Management Procedures

4.3.1 Risk Assessment

The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

- Step 1. System Characterization
 - The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is received, maintained, processed, or transmitted. Using information-gathering techniques, the Capital Rx Platform boundaries are identified.
 - Output - Characterization of the Capital Rx Platform system assessed, a good picture of the Platform environment, and delineation of Platform boundaries.
- Step 2. Threat Identification
 - Potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. All potential threat-sources from historical incidents and data from intelligence agencies, the government, etc., are reviewed to help generate a list of potential threats.
 - Output - A threat list containing a list of threat-sources that could exploit Platform vulnerabilities.
- Step 3. Vulnerability Identification
 - Develop a list of technical and non-technical Platform vulnerabilities that could be exploited or triggered by potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network.
 - Output - A list of the Platform vulnerabilities (observations) that could be exercised by potential threat-sources.
- Step 4. Control Analysis

- Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by Capital Rx to minimize or eliminate the likelihood / probability of a threat-source exploiting a Platform vulnerability.
- Output - List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the Platform to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.
- Step 5. Likelihood Determination
- Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
- Output - Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- Step 6. Impact Analysis
- Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to Capital Rx's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.
- Output - Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- Step 7. Risk Determination
- Establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management must take for each risk level.
- Output - Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.
- Step 8. Control Recommendations
- Identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

- Output - Recommendation of control(s) and alternative solutions to mitigate risk.
- Step 9. Results Documentation
- Results of the risk assessment are documented in an official report, spreadsheet, or briefing and provided to senior management to make decisions on policy, procedure, budget, and Platform operational and management changes.
- Output - A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

4.3.2 Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the Risk Assessment process to ensure the confidentiality, integrity and availability of Capital Rx Platform ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

- Step 1. Prioritize Actions
 - Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources
 - Output - Actions ranked from high to low
- Step 2. Evaluate Recommended Control Options
 - Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.
 - Output - list of feasible controls
- Step 3. Conduct Cost-Benefit Analysis
 - Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner,

and prioritizing across all controls being considered, can greatly aid in the decision-making process.

- Output - Documented cost-benefit analysis of either implementing or not implementing each specific control
- Step 4. Select Control(s)
- Taking into account the information and results from previous steps, Capital Rx's mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
- Output - Selected control(s)
- Step 5. Assign Responsibility
- Identify the workforce members with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.
- Output - List of resources, responsible persons and their assignments
- Step 6. Develop Safeguard Implementation Plan
- Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
 - Each risk or vulnerability/threat pair and risk level;
 - Prioritized actions;
 - The recommended feasible control(s) for each identified risk;
 - Required resources for implementation of selected controls;
 - Team member responsible for implementation of each control;
 - Start date for implementation
 - Target date for completion of implementation;
 - Maintenance requirements.
- The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to Capital Rx Senior Management.
- Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations. Additionally, consider including

items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates and project requirements.

- Output - Safeguard Implementation Plan
- Step 7. Implement Selected Controls
- As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.
- Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.
- Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
- If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
- Output - Residual Risk documentation

4.3.3 Risk Management Schedule

The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of Capital Rx's information security program:

- Scheduled Basis - an overall risk assessment of Capital Rx's information system infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the corporate budgeting process.
- Throughout a System's Development Life Cycle - from the time that a need for a new, untested information system configuration and/or application is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
- As Needed - the Security Officer (or other designated employee) or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect Capital Rx's Platform.

4.4 Process Documentation

Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of six years.

5. Roles Policy

Capital Rx has a Security Officer [164.308(a)(2)] and Privacy Officer [164.308(a)(2)] appointed to assist in maintaining and enforcing safeguards towards compliance. The responsibilities associated with these roles are outlined below.

5.1 Applicable Standards

5.1.1 Applicable Standards from the HITRUST Common Security Framework

- 02.f - Disciplinary Process
- 06.d - Data Protection and Privacy of Covered Information
- 06.f - Prevention of Misuse of Information Assets
- 06.g - Compliance with Security Policies and Standards

5.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308(a)(2) - Assigned Security Responsibility
- 164.308(a)(5)(i) - Security Awareness and Training

5.2 Privacy Officer

The Privacy Officer is responsible for assisting with compliance and security training for workforce members, assuring organization remains in compliance with evolving compliance rules, and helping the Security Officer in his responsibilities.

1. Provides annual training to all workforce members of established policies and procedures as necessary and appropriate to carry out their job functions, and documents the training provided.
2. Assists in the administration and oversight of business associate agreements.
3. Manage relationships with customers and partners as those relationships affect security and compliance of ePHI.
4. Assist Security Officer as needed.

The current Capital Rx Privacy Officer is Ryan Kelly (ryan@cap-rx.com).

5.2.1 Workforce Training Responsibilities

1. The Privacy Officer facilitates the training of all workforce members as follows:
2. New workforce members within their first month of employment;

3. Existing workforce members annually;
4. Existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective;
5. Existing workforce members as needed due to changes in security and risk posture of Capital Rx.
6. The Security Officer or designee maintains documentation of the training session materials and attendees for a minimum of six years.
7. The training session focuses on, but is not limited to, the following subjects defined in Capital Rx's security policies and procedures:
8. HIPAA Privacy, Security, and Breach notification rules;
9. HITRUST Common Security Framework;
10. NIST Security Rules;
11. Risk Management procedures and documentation;
12. Auditing. Capital Rx may monitor access and activities of all users;
13. Workstations may only be used to perform assigned job responsibilities;
14. Users may not download software onto Capital Rx's workstations and/or systems without prior approval from the Security Officer;
15. Users are required to report malicious software to the Security Officer immediately;
16. Users are required to report unauthorized attempts, uses of, and theft of Capital Rx's systems and/or workstations;
17. Users are required to report unauthorized access to facilities
18. Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation);
19. Users may not alter ePHI maintained in a database, unless authorized to do so by a Capital Rx Customer;
20. Users are required to understand their role in Capital Rx's contingency plan;
21. Users may not share their user names nor passwords with anyone;
22. Requirements for users to create and change passwords;
23. Users must set all applications that contain or transmit ePHI to automatically log off after 15 minutes of inactivity;
24. Supervisors are required to report terminations of workforce members and other outside users;
25. Supervisors are required to report a change in a users title, role, department, and/or location;
26. Procedures to backup ePHI;
27. Procedures to move and record movement of hardware and electronic media containing ePHI;
28. Procedures to dispose of discs, CDs, hard drives, and other media containing ePHI;
29. Procedures to re-use electronic media containing ePHI;
30. SSH key and sensitive document encryption procedures.

5.3 Security Officer

The Security Officer is responsible for facilitating the training and supervision of all workforce members [164.308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any workforce member that is in violation of Capital Rx security policies and non-compliance with the security regulations [164.308(a)(1)(ii)(c)], and writing, implementing, and maintaining all policies, procedures, and documentation related to efforts toward security and compliance [164.316(a-b)].

The current Capital Rx Security Officer is Ryan Kelly (ryan@cap-rx.com).

5.3.1 Organizational Responsibilities

The Security Officer, in collaboration with the Privacy Officer, is responsible for facilitating the development, testing, implementation, training, and oversight of all activities pertaining to Capital Rx's efforts to be compliant with the HIPAA Security Regulations, HITRUST CSF, and any other security and compliance frameworks. The intent of the Security Officer Responsibilities is to maintain the confidentiality, integrity, and availability of ePHI. The Security Officer is appointed by and reports to the Board of Directors and the CEO.

These organizational responsibilities include, but are not limited to the following:

1. Oversees and enforces all activities necessary to maintain compliance and verifies the activities are in alignment with the requirements.
2. Helps to establish and maintain written policies and procedures to comply with the Security rule and maintains them for six years from the date of creation or date it was last in effect, whichever is later.
3. Reviews and updates policies and procedures as necessary and appropriate to maintain compliance and maintains changes made for six years from the date of creation or date it was last in effect, whichever is later.
4. Facilitates audits to validate compliance efforts throughout the organization.
5. Documents all activities and assessments completed to maintain compliance and maintains documentation for six years from the date of creation or date it was last in effect, whichever is later.
6. Provides copies of the policies and procedures to management, customers, and partners, and has them available to review by all other workforce members to which they apply.
7. Annually, and as necessary, reviews and updates documentation to respond to environmental or operational changes affecting the security and risk posture of ePHI stored, transmitted, or processed within Capital Rx infrastructure.
8. Develops and provides periodic security updates and reminder communications for all workforce members.

9. Implements procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it may be accessed.
10. Maintains a program promoting workforce members to report non-compliance with policies and procedures.
 - Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.
 - Applies consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Capital Rx.
 - Mitigates, to the extent practicable, any harmful effect known to Capital Rx of a use or disclosure of ePHI in violation of Capital Rx's policies and procedures, even if the effect is the result of actions of Capital Rx business associates, customers, and/or partners.
11. Reports security efforts and incidents to administration immediately upon discovery. Responsibilities in the case of a known ePHI breach are documented in the Capital Rx Breach Policy.
12. The Security Officer facilitates the communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:
 - Latest malicious software or virus alerts;
 - Capital Rx's requirement to report unauthorized attempts to access ePHI;
 - Changes in creating or changing passwords;
 - Additional security-focused training is provided to all workforce members by the Security Officer. This training includes, but is not limited to:
 - Data backup plans;
 - System auditing procedures;
 - Redundancy procedures;
 - Contingency plans;
 - Virus protection;
 - Patch management;
 - Media Disposal and/or Re-use;
 - Documentation requirements.
13. The Security Officer works with the COO to ensure that any security objectives have appropriate consideration during the budgeting process.
 - In general, security and compliance are core to Capital Rx's technology and service offerings; in most cases this means security-related objectives cannot be split out to separate budget line items.
 - For cases that *can* be split out into discrete items, such as licenses for commercial tooling, the Security Officer follows Capital Rx's standard corporate budgeting process.
 - At the beginning of every fiscal year, the COO contacts the Security Officer to plan for the upcoming year's expenses.
 - The Security Officer works with the COO to forecast spending needs

based on the previous year's level, along with changes for the upcoming year such as additional staff hires.

- During the year, if an unforeseen security-related expense arises that was not in the budget forecast, the Security Officer works with the COO to reallocate any resources as necessary to cover this expense.

5.3.2 Supervision of Workforce Responsibilities

Although the Security Officer is responsible for implementing and overseeing all activities related to maintaining compliance, it is the responsibility of all workforce members (i.e. team leaders, supervisors, managers, directors, co-workers, etc.) to supervise all workforce members and any other user of Capital Rx's systems, applications, servers, workstations, etc. that contain ePHI.

1. Monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.
2. Assist the Security and Privacy Officers to ensure appropriate role-based access is provided to all users.
3. Take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and Capital Rx's security policies and procedures.

5.3.3 Sanctions of Workforce Responsibilities

All workforce members report non-compliance of Capital Rx's policies and procedures to the Security Officer or other individual as assigned by the Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

1. The Security Officer promptly facilitates a thorough investigation of all reported violations of Capital Rx's security policies and procedures. The Security Officer may request the assistance from others.
 - Complete an audit trail/log to identify and verify the violation and sequence of events.
 - Interview any individual that may be aware of or involved in the incident.
 - All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
 - Provide individuals suspected of non-compliance of the Security rule and/or Capital Rx's policies and procedures the opportunity to explain their actions.
 - The investigator thoroughly documents the investigation as the investigation occurs. This documentation must include a list of all employees involved in the violation.

2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
 - A violation resulting in a breach of confidentiality (i.e. release of PHI to an unauthorized individual), change of the integrity of any ePHI, or inability to access any ePHI by other users, requires immediate termination of the workforce member from Capital Rx.
3. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).
4. In the case of an insider threat, the Security Officer and Privacy Officer are to set up a team to investigate and mitigate the risk of insider malicious activity. Capital Rx workforce members are encouraged to come forward with information about insider threats, and can do so anonymously.
5. The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.

6. Data Management Policy

Capital Rx has procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI) stored in conjunction with the Capital Rx Platform. The policy and procedures will assure that complete, accurate, retrievable, and tested backups are available for all systems used by Capital Rx.

Data backup is an important part of the day-to-day operations of Capital Rx. To protect the confidentiality, integrity, and availability of ePHI, both for Capital Rx and Capital Rx Customers, complete backups are done at least daily to assure that data remains available when it needed and in case of a disaster.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.

6.1 Applicable Standards

6.1.1 Applicable Standards from the HITRUST Common Security Framework

- 01.v - Information Access Restriction

6.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308(a)(7)(ii)(A) - Data Backup Plan
- 164.310(d)(2)(iii) - Accountability
- 164.310(d)(2)(iv) - Data Backup and Storage

6.2 Backup Policy and Procedures

1. Perform daily snapshot backups of all systems that process, store, or transmit ePHI for Capital Rx Customers.
2. The Capital Rx Infrastructure Team is designated to be in charge of backups.
3. Infrastructure Team members are trained and assigned to complete backups and manage the backup media.
4. Document backups
 - Name of the system
 - Date & time of backup
 - Where backup stored (or to whom it was provided)
5. Securely encrypt stored backups in a manner that protects them from loss or environmental damage.

6. Test backups annually and document that files have been completely and accurately restored from the backup media.

7. System Access Policy

Access to Capital Rx systems and applications is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, and consultants. Access by any other entity is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems. These safeguards have been established to address the HIPAA Security regulations including the following:

7.1 Applicable Standards

7.1.1 Applicable Standards from the HITRUST Common Security Framework

- 01.d - User Password Management
- 01.f - Password Use
- 01.r - Password Management System
- 01.a - Access Control Policy
- 01.b - User Registration
- 01.h - Clear Desk and Clear Screen Policy
- 01.j - User Authentication for External Connections
- 01.q - User Identification and Authentication
- 01.v - Information Access Restriction
- 02.i - Removal of Access Rights
- 06.e - Prevention of Misuse of Information Assets

7.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308a4iiC Access Establishment and Modification
- 164.308a3iiB Workforce Clearance Procedures
- 164.308a4iiB Access Authorization
- 164.312d Person or Entity Authentication
- 164.312a2i Unique User Identification
- 164.308a5iiD Password Management
- 164.312a2iii Automatic Logoff
- 164.310b Workstation Use
- 164.310c Workstation Security
- 164.308a3iiC Termination Procedures

7.2 Access Establishment and Modification

1. Requests for access to Capital Rx Platform systems and applications is made formally using the following process:
2. A Capital Rx workforce member initiates the access request by creating an Issue in the Capital Rx Quality Management System.
 - User identities must be verified prior to granting access to new accounts.
 - Identity verification must be done in person where possible; for remote employees, identities must be verified over the phone.
 - For new accounts, the method used to verify the user's identity must be recorded on the Issue.
3. The Security Officer or Privacy Officer will grant access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
4. Once the review is completed, the Security Officer or Privacy Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
5. If the review is approved, the Security Officer or Privacy Officer then marks the Issue as Done, adding any pertinent notes required. The Security Officer or Privacy Officer then grants requested access.
 - New accounts will be created with a temporary secure password that meets all requirements from §7.12, which must be changed on the initial login.
 - All password exchanges must occur over an authenticated channel.
 - For production systems, access grants are accomplished by adding the appropriate IAM policies and roles to the user account.
 - For non-production systems, access grants are accomplished by leveraging the access control mechanisms built into those systems. Account management for non-production systems may be delegated to a Capital Rx employee at the discretion of the Security Officer or Privacy Officer.
6. Access is not granted until receipt, review, and approval by the Capital Rx Security Officer or Privacy Officer;
7. The request for access is retained for future reference.
8. All access to Capital Rx systems and services is reviewed and updated on a bi-annual basis to ensure proper authorizations are in place commensurate with job functions. The process for conducting reviews is outlined below:
9. The Security Officer initiates the review of user access by creating an Issue in the Capital Rx Quality Management System.
10. The Security Officer is assigned to review levels of access for each Capital Rx workforce member.
11. If user access is found during review that is not in line with the least

privilege principle, the process below is used to modify user access and notify the user of access changes. Once those steps are completed, the Issue is then reviewed again.

12. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
13. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
14. Review of user access is monitored on an annual basis using the Quality Management System reporting to assess compliance with above policy.
15. Any Capital Rx workforce member can request change of access using the process outlined in §7.2 paragraph 1.
16. Access to production systems is controlled using standardized user management and authentication.
17. Temporary accounts are not used unless absolutely necessary for business purposes.
 - Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily.
 - Accounts that are inactive for over 90 days are removed.
8. In the case of non-personal information, such as generic educational content, identification and authentication may not be required.
9. Privileged users should first access systems using standard, unique user accounts before switching to privileged users and performing privileged tasks, when functionality is available.
 - For production systems running Linux servers, this is enforced by creating non-privileged user accounts that must invoke `sudo` to perform privileged tasks.
 - Rights for privileged accounts are granted by the Security Officer or Privacy Officer using the process outlined in §7.2 paragraph 1.
10. All application to application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
11. Generic accounts are not allowed on Capital Rx systems.
12. Access is granted through encrypted, secure portals that utilize two-factor authentication.
 - Two-factor authentication is accomplished using a Time-based One-Time Password (TOTP) as the second factor when possible or Text Message based One-Time Password if the former is unavailable.
 - SSH connections use 256-bit AES 256 encryption, or equivalent or stronger.
13. In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security and Privacy Officer to limit access and reduce risk of unauthorized access.
14. Direct system to system, system to application, and application to applica-

tion authentication and authorization are limited and controlled to restrict access.

7.3 Workforce Clearance

1. The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
2. All access requests are treated on a "least-access principle."
3. Capital Rx maintains a minimum necessary approach to access to Customer data.

7.4 Access Authorization

1. Role based access categories for each Capital Rx system and application are pre-approved by the Security Officer, or an authorized delegate of the Security Officer.
2. Capital Rx utilizes hardware and software firewalls to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.

7.5 Person or Entity Authentication

1. Each workforce member has and uses a unique user ID and password that identifies him/her as the user of the information system.
 2. Each Customer and Partner has and uses a unique user ID and password that identifies him/her as the user of the information system.
 3. All Customer support desk interactions must be verified before Capital Rx support personnel will satisfy any request having information security implications.
- Capital Rx's current support desk software, Jira, requires users to authenticate before submitting support tickets.
 - Support issues submitted via Capital Rx's dashboard require that users authenticate with their Capital Rx account before submitting support tickets.
 - Support issues submitted by email must be verified by Capital Rx personnel using a phone number that has been registered with the corresponding account.

7.6 Unique User Identification

1. Access to the Capital Rx Platform systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
2. Passwords requirements mandate strong password controls (see below).
3. Passwords are not displayed at any time and are not transmitted or stored in plain text.
4. Shared accounts are not allowed within Capital Rx systems or networks.

7.7 Automatic Logoff

1. Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).
2. The Security Officer pre-approves exceptions to automatic log off requirements.

7.8 Employee Workstation Use

All workstations at Capital Rx are company owned, and all are laptop Apple products running Mac OSX or Linux.

1. Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
2. Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization's system.
3. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
4. Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
5. Transmitted messages may not contain material that criticizes the organization, its providers, its employees, or others.
6. Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
7. Workstation hard drives will be encrypted using FileVault 2.0 or equivalent.

8. All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.

7.9 Wireless Access Use

1. Capital Rx production systems are not accessible directly over wireless channels.
2. Wireless access is disabled on all production systems.
3. When accessing production systems via remote wireless connections, the same system access policies and procedures apply to wireless as all other connections, including wired.
4. Wireless networks managed by Capital Rx within Capital Rx non-production facilities (offices, etc.) are secured with the following configurations:
 - All data in transit over wireless is encrypted using WPA2 encryption;
 - Passwords are rotated on a regular basis, presently quarterly. This process is managed by the Capital Rx Security Officer.

7.10 Employee Termination Procedures

1. The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".
2. The Human Resources Department, users, and supervisors are required to notify the Security Officer to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
 - The user has been using their access rights inappropriately;
 - A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
 - An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
3. The Security Officer will terminate users' access rights immediately upon notification, and will coordinate with the appropriate Capital Rx employees to terminate access to any non-production systems managed by those employees.
4. The Security Officer may audit and may terminate access of users that have not logged into organization's information systems/applications for

an extended period of time.

7.11 Paper Records

Capital Rx does not use paper records for any sensitive information. Use of paper for recording and storing sensitive data is against Capital Rx policies.

7.12 Password Management

Capital Rx provides all employees with enterprise-grade password management tools. Such tools allow unique passwords to be used on all systems and managed effectively, limiting password re-use or the use of algorithmically related or derived passwords.

1. User IDs and passwords are used to control access to Capital Rx systems and may not be disclosed to anyone for any reason.
2. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
3. On all production systems and applications in the Capital Rx environment, password configurations are set when possible to require:
 - a minimum length of 8 characters;
 - a mix of upper case characters, lower case characters, and numbers or special characters;
 - lockout after an excessive number of failed attempts;
 - the use of a second factor.
4. All system and application passwords must be stored and transmitted securely.
 - Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or equivalent).
 - Passwords that must be stored in non-hashed format must be encrypted at rest pursuant to the requirements in §17.8.
 - Transmitted passwords must be encrypted in flight pursuant to the requirements in §17.9.
5. Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the ePHI contained within the network, system, application, and/or database.
6. Passwords are inactivated immediately upon an employee's termination (refer to the Employee Termination Procedures in §7.10).
7. All default system, application, and Partner passwords are changed before deployment to production.

8. Upon initial login, users must change any passwords that were automatically generated for them.
9. Password change methods should use a confirmation method to correct for user input errors.
10. All passwords used in configuration scripts are secured and encrypted.
11. If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security Office.
12. In cases where a user has forgotten their password, the following procedure is used to reset the password.
 - The user submits a password reset request to password-reset@cap-rx.com. The request should include the system to which the user has lost access and needs the password reset.
 - An administrator with password reset privileges is notified and connects directly with the user requesting the password reset.
 - The administrator verifies the identity of the user either in-person or through a separate communication channel such as phone or Slack.
 - Once verified, the administrator resets the password.

The password-reset email inbox is used to track and store password reset requests. The Security Officer is the owner of this group and modifies membership as needed.

Counter-productive password management techniques, such as frequent changes, are known to provide minimal additional security benefit but are highly burdensome for users 1 2 and are not implemented unless otherwise required.

7.13 Access to ePHI

1. Employees should not download ePHI to any workstations used to connect to production systems.

7.14 SaaS Customer Access to Systems

Capital Rx grants SaaS customer secure system access via HTTPS or SSH connections. This access is only to Customer-specific systems, no other systems in the environment. These connections are setup at customer deployment. These connections are secured and encrypted and the only method for customers to connect to Capital Rx hosted systems.

In the case of data migration, Capital Rx does, on a case by case basis, support customers in importing data. In these cases Capital Rx requires that all data is secured and encrypted in transit, such as by using SFTP or SCP for transferring files.

In the case of an investigation, Capital Rx will assist customers, at Capital Rx's discretion, and law enforcement in forensics.

8. Auditing Policy

Capital Rx shall audit access and activity of electronic protected health information (ePHI) applications and systems in order to ensure compliance. The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Audit activities may be limited by application, system, and/or network auditing capabilities and resources. Capital Rx shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing that is consistent with available resources.

It is the policy of Capital Rx to safeguard the confidentiality, integrity, and availability of applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, Capital Rx shall audit access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusions;
- Breaches in confidentiality and security of patient protected health information;
- Performance problems and flaws in applications;
- Improper alteration or destruction of ePHI;
- Out of date software and/or software known to have vulnerabilities.

This policy applies to all Capital Rx systems that store, transmit, or process ePHI.

8.1 Applicable Standards

8.1.1 Applicable Standards from the HITRUST Common Security Framework

- 0.a Information Security Management Program
- 01.a Access Control Policy
- 01.b User Registration
- 01.c Privilege Management
- 09.aa Audit Logging
- 09.ac Protection of Log Information
- 09.ab - Monitoring System Use
- 06.e - Prevention of Misuse of Information

8.1.2 Applicable Standards from the HIPAA Security Rule

- 45 CFR §164.308(a)(1)(ii)(D) - Information System Activity Review

- 45 CFR §164.308(a)(5)(ii)(B) & (C) - Protection from Malicious Software & Log-in Monitoring
- 45 CFR §164.308(a)(2) - HIPAA Security Rule Periodic Evaluation
- 45 CFR §164.312(b) - Audit Controls
- 45 CFR §164.312(c)(2) - Mechanism to Authenticate ePHI
- 45 CFR §164.312(e)(2)(i) - Integrity Controls

8.2 Auditing Policies

1. Responsibility for auditing information system access and activity is assigned to Capital Rx's Security Officer. The Security Officer shall:
 - Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network, or any other individual determined to be appropriate for the task;
 - Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task;
 - Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).
 - All connections to Capital Rx are monitored. Access is limited to certain services, ports, and destinations. Exceptions to these rules, if created, are reviewed on an annual basis.
2. Capital Rx's auditing processes shall address access and activity at the following levels listed below. Auditing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.
 - User: User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.
 - Application: Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.
 - System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions. Capital Rx utilizes file system monitoring to assure the integrity of file system data, if any.
 - Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.
3. Capital Rx shall log all incoming and outgoing traffic to into and out of its environment. This includes all successful and failed attempts at data access and editing. Data associated with this data will include origin, destination, time, and other relevant details that are available to Capital Rx.

4. Capital Rx utilizes OSSEC to scan all systems for malicious and unauthorized software every 2 hours and at reboot of systems.
5. Capital Rx leverages process monitoring tools throughout its environment.
6. Capital Rx logs all access to AWS-managed or -hosted services using AWS CloudTrail.
7. Capital Rx uses OSSEC to monitor the integrity of log files by utilizing OSSEC System Integrity Checking capabilities.
8. Capital Rx shall identify “trigger events” or criteria that raise awareness of questionable conditions of viewing of confidential information. The “events” may be applied to the entire Capital Rx Platform or may be specific to a Customer, partner, business associate, Platform or application (See Listing of Potential Trigger Events below).
9. In addition to trigger events, Capital Rx utilizes OSSEC log correlation functionality to proactively identify and enable alerts based on log data.
10. Logs are reviewed weekly by the Security Officer.
11. Capital Rx’s Security Officer and Privacy Officer are authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are explicitly prohibited by others, including Customers and Partners, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:
 - Scanning tools and devices;
 - Password cracking utilities;
 - Network “sniffers.”
 - Passive and active intrusion detection systems.
12. The process for review of audit logs, trails, and reports shall include:
 - Description of the activity as well as rationale for performing the audit.
 - Identification of which Capital Rx workforce members will be responsible for review (workforce members shall not review audit logs that pertain to their own system activity).
 - Frequency of the auditing process.
 - Determination of significant events requiring further review and follow-up.
 - Identification of appropriate reporting channels for audit results and required follow-up.
13. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.
 - Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services - separation of duties).
 - Testing shall be done on a routine basis, currently annually.

14. Software patches and updates will be applied to all systems in a timely manner.

8.3 Audit Requests

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Privacy Officer, Security Officer, Customer, Partner, or an Application owner or application user.
2. A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by Capital Rx's Privacy or Security Officer.
3. A request for an audit must be approved by Capital Rx's Privacy Officer and/or Security Officer before proceeding. Under no circumstances shall detailed audit information be shared with parties without proper permissions and access to see such data.
 - Should the audit disclose that a workforce member has accessed ePHI inappropriately, the minimum necessary/least privileged information shall be shared with Capital Rx's Security Officer to determine appropriate sanction/corrective disciplinary action.
 - Only de-identified information shall be shared with Customer or Partner regarding the results of the investigative audit process. This information will be communicated to the appropriate personnel by Capital Rx's Privacy Officer or designee. Prior to communicating with customers and partners regarding an audit, it is recommended that Capital Rx consider seeking risk management and/or legal counsel.

8.4 Review and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner, currently annually, by the responsible workforce member(s). On an annual basis, logs are reviewed to assure the proper data is being captured and retained. The following process details how log reviews are done at Capital Rx:
2. The Security Officer initiates the log review by creating an Issue in the Capital Rx Quality Management System.
3. The Security Officer, or a Capital Rx Security Engineer assigned by the Security Officer, is assigned to review the logs.
4. Relevant audit log findings are added to the Issue; these findings are investigated in a later step. Once those steps are completed, the Issue is then reviewed again.
5. Once the review is completed, the Security Officer approves or rejects the Issue. Relevant findings are reviewed at this stage. If the Issue is rejected,

it goes back for further review and documentation. The communications protocol around specific findings are outlined below.

6. If the Issue is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
7. The reporting process shall allow for meaningful communication of the audit findings to those workforce members, Customers, or Partners requesting the audit.
 - Significant findings shall be reported immediately in a written format. Capital Rx's security incident response form may be utilized to report a single event.
 - Routine findings shall be reported to the sponsoring leadership structure in a written report format.
3. Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
4. Security audits constitute an internal, confidential monitoring practice that may be included in Capital Rx's performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative level oversight structures only and that information which may further expose organizational risk is shared with extreme caution. Generic security audit information may be included in organizational reports (individually-identifiable ePHI shall not be included in the reports).
5. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members, Customers, and/or Partners.
6. Log review activity is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.

8.5 Auditing Customer and Partner Activity

1. Periodic monitoring of Customer and Partner activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between Capital Rx and the 3rd party. Capital Rx will make every effort to assure Customers and Partners do not gain access to data outside of their own Environments.
2. If it is determined that the Customer or Partner has exceeded the scope of access privileges, Capital Rx's leadership must remedy the problem immediately.
3. If it is determined that a Customer or Partner has violated the terms of the HIPAA business associate agreement or any terms within the HIPAA regulations, Capital Rx must take immediate action to remediate the

situation. Continued violations may result in discontinuation of the business relationship.

8.6 Audit Log Security Controls and Backup

1. Audit logs shall be protected from unauthorized access or modification, so the information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
2. All audit logs are protected in transit and encrypted at rest to control access to the content of the logs.
3. Audit logs shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails by those with system administrator privileges.
 - Separate systems are used to apply the security principle of “separation of duties” to protect audit trails from hackers.
 - Capital Rx logging is handled by AWS CloudWatch.

8.7 Workforce Training, Education, Awareness and Responsibilities

1. Capital Rx workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and ePHI. Capital Rx’s commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. Capital Rx workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member’s failure to comply with organizational policies.
2. Capital Rx Customers are provided with necessary information to understand Capital Rx auditing capabilities, and PaaS Customers can choose the level of logging and auditing that Capital Rx will implement on their behalf.

8.8 External Audits of Information Access and Activity

1. Prior to contracting with an external audit firm, Capital Rx shall:
 - Outline the audit responsibility, authority, and accountability;
 - Choose an audit firm that is independent of other organizational operations;
 - Ensure technical competence of the audit firm staff;

- Require the audit firm’s adherence to applicable codes of professional ethics;
- Obtain a signed HIPAA business associate agreement;
- Assign organizational responsibility for supervision of the external audit firm.

8.9 Retention of Audit Data

1. Audit logs shall be maintained based on organizational needs. There is no standard or law addressing the retention of audit log/trail information. Retention of this information shall be based on:
 - Organizational history and experience.
 - Available storage space.
2. Reports summarizing audit activities shall be retained for a period of six years.
3. Audit log data is retained in AWS CloudWatch for a currently unrestricted period of time.

8.10 Potential Trigger Events

- High risk or problem prone incidents or events.
- Business associate, customer, or partner complaints.
- Known security vulnerabilities.
- Atypical patterns of activity.
- Failed authentication attempts.
- Remote access use and activity.
- Activity post termination.
- Random audits.

9. Configuration Management Policy

Capital Rx standardizes and automates configuration management through the use of Salt and Terraform scripts as well as documentation of all changes to production systems and networks. Salt and Terraform automatically configure all Capital Rx systems according to established and tested policies, and are used as part of our Disaster Recovery plan and process.

9.1 Applicable Standards

9.1.1 Applicable Standards from the HITRUST Common Security Framework

- 06 - Configuration Management

9.1.2 Applicable Standards from the HIPAA Security Rule

- 164.310(a)(2)(iii) Access Control & Validation Procedures

9.2 Configuration Management Policies

1. Salt and Terraform are used to standardize and automate configuration management.
 2. No new systems are deployed into Capital Rx environments without approval of the Capital Rx CTO.
 3. All changes to production systems, network devices, and firewalls are approved by the Capital Rx CTO before they are implemented to assure they comply with business and security requirements.
 4. All changes to production systems are tested before they are implemented in production.
 5. Implementation of approved changes are only performed by authorized personnel.
 6. Tooling to generate an up-to-date inventory of systems, including corresponding architecture diagrams for related products and services, is provided by AWS.
- All systems are categorized as production and utility to differentiate based on criticality.
 - These scripts are used to generate the diagrams and asset lists required by the Risk Assessment phase of Capital Rx's Risk Management procedures (§4.3.1).
 - After every use of these scripts, the Security Officer will verify their accuracy by reconciling their output with recent changes to production systems. The

Security Officer will address any discrepancies immediately with changes to the scripts.

7. All frontend functionality (developer dashboards and portals) is separated from backend (database and app servers) systems by being deployed on separate servers, containers, or AWS-managed systems.
8. All software and systems are tested using either unit tests, end to end tests, or both.
9. All committed code is reviewed using pull requests to assure software code quality and proactively detect potential security issues in development.
10. Capital Rx utilizes staging and acceptance environments that mirror production to assure proper function.
11. Capital Rx also deploys environments locally using the same scripts to assure functionality before moving to staging, acceptance, or production.
12. All formal change requests require unique ID and authentication.
13. Capital Rx uses the Security Technical Implementation Guides (STIGs) published by the Defense Information Systems Agency as a baseline for hardening systems.
 - Linux-based systems use a Red Hat Enterprise Linux STIG which has been adapted for Ubuntu and improved based on the results of subsequent vulnerability scans and risk assessments.
14. Clocks are continuously synchronized to an authoritative source across all systems using NTP or a platform-specific equivalent. Modifying time data on systems is restricted.

9.3 Provisioning Production Systems

1. Before provisioning any systems, infrastructure team members must file a request in the Capital Rx Quality Management System.
 - Quality Management System access requires authenticated users.
 - The CTO grants access to the Quality Management System following the procedures covered in the Access Establishment and Modification section.
2. The CTO, or an authorized delegate of the CTO, must approve the provisioning request before any new system can be provisioned.
3. Once provisioning has been approved, the ops team member must configure the new system according to the standard baseline chosen for the system's role.
4. If the system will be used to house production data (ePHI), the infrastructure team must ensure that any systems used are covered by the AWS BAA and utilize encrypted storage and communication.
5. Once the system has been provisioned, the infrastructure team member must contact the security team to inspect the new system. A member of the security team will verify that the secure baseline has been applied to the new system, including (but not limited to) verifying the following

items:

- Network configuration for system.
 - Data volume encryption settings.
 - Intrusion detection and virus scanning software installed.
 - All items listed below in the operating system-specific subsections below.
6. Once the security team member has verified the new system is correctly configured, the team member must verify that system is being monitored by AWS Inspector security scanner configuration.
 7. The new system may be rotated into production once the CTO verifies all the provisioning steps listed above have been correctly followed and has marked the Issue with the Approved state.

9.3.1 Provisioning Linux Systems

1. Linux systems have their baseline security configuration applied via Salt states. These baseline Salt states cover:
 - Ensuring that the machine is up-to-date with security patches and is configured to apply patches in accordance with our policies.
 - Stopping and disabling any unnecessary OS services.
 - Installing and configuring the OSSEC IDS agent.
 - Configuring 15-minute session inactivity timeouts.
 - Installing and configuring the ClamAV virus scanner.
 - Installing and configuring the NTP daemon, including ensuring that modifying system time cannot be performed by unprivileged users.
 - Configuring LUKS volumes for providers that do not have native support for encrypted data volumes, including ensuring that encryption keys are protected from unauthorized access.
 - Configuring authentication to the centralized LDAP servers.
 - Configuring audit logging as described in the Auditing Policy section.
2. Any additional Salt states applied to the Linux system must be clearly documented by the ops team member in the DT request by specifying the purpose of the new system.

9.3.2 Provisioning Windows Systems

Not applicable.

9.3.3 Provisioning Management Systems

1. Provisioning management systems such as Salt servers, LDAP servers, or VPN appliances follows the same procedure as provisioning a production system.

2. Provisioning the first Salt server for a production pod requires bootstrapping Salt. An authorized member of the infrastructure team will oversee provisioning a new Salt server.
 - Once the Salt server has been bootstrapped, the ops team member will apply the baseline configuration to the Salt server by performing a `highstate` operation as usual.
3. Critical infrastructure services such as logging, monitoring, LDAP servers, or Windows Domain Controllers must be configured with appropriate Salt states.
 - These Salt states have been approved by the CTO, or an authorized delegate of the CTO, to be in accordance with all Capital Rx policies, including setting appropriate:
 - Audit logging requirements.
 - Password size, strength, and expiration requirements.
 - Transmission encryption requirements.
 - Network connectivity timeouts.
4. Critical infrastructure roles applied to new systems must be clearly documented by the ops team member in the DT request.

9.4 Changing Existing Systems

1. Subsequent changes to already-provisioned systems are unconditionally handled by one of the following methods:
 - Changes to Salt states or pillar values.
 - Changes to Terraform configuration.
 - For configuration changes that cannot be handled by Salt or Terraform, a runbook describing exactly what changes will be made and by whom.
2. Configuration changes to Salt states or Terraform configurations must be initiated by creating a Merge Request in GitHub.
 - The infrastructure team member will create a feature branch and make their changes on that branch.
 - The infrastructure team member must test their configuration change locally when possible, or on a development and/or staging sandbox otherwise.
 - At least one other infrastructure team member must review the Salt or Terraform change before merging the change into the main branch.
3. In all cases, before rolling out the change to production, the infrastructure team member must file an Issue in the project describing the change. This Issue must link to the reviewed Merge Request and/or include a link to the runbook.

4. Once the request has been approved by the CTO, the infrastructure team member may roll out the change into production environments.

9.5 Patch Management Procedures

1. Capital Rx uses automated tooling to ensure systems are up-to-date with the latest security patches.
2. On Ubuntu Linux systems, the unattended-upgrades tool is used to apply security patches in phases.
 - Patches for critical kernel security vulnerabilities may be applied to production systems using hot-patching tools at the discretion of the Security Officer. These patches must follow the same phased testing process used for non-kernel security patches; this process may be expedited for severe vulnerabilities.

9.6 Software Development Procedures

1. All development uses feature branches based on the main branch used for the current release. Any changes required for a new feature or defect fix are committed to that feature branch.
 - These changes should be covered under 1) a unit test where possible, or 2) integration tests.
 - Integration tests may be required if unit tests cannot reliably exercise all facets of the change.
2. Developers are encouraged to follow the commit message conventions suggested by GitHub.
 - Commit messages should be wrapped to 72 characters.
 - Commit messages should be written in the present tense. This convention matches up with commit messages generated by commands like `git merge` and `git revert`.
3. Once the feature and corresponding tests are complete, a pull request will be created using the GitHub web interface. The pull request should indicate which feature or defect is being addressed and should provide a high-level description of the changes made.
4. Code reviews are performed as part of the pull request procedure. Once a change is ready for review, the author(s) will notify other engineers using an appropriate mechanism.
 - Other engineers will review the changes, using the guidelines above.
 - Engineers should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.

5. If the feature or defect interacts with ePHI, or controls access to data potentially containing ePHI, the code changes must be reviewed by a member of Capital Rx's security team before the feature is marked as complete.
 - The security team member will provide a security analysis of features to ensure they satisfy Capital Rx's compliance and security commitments.
 - This review must include a security analysis for potential vulnerabilities such as those listed in the OWASP Top 10 or the CWE top 25.
 - This review must also verify that any actions performed by authenticated users will generate appropriate audit log entries.
 - Security team members are required to undergo annual training on identifying the most common software vulnerabilities and will receive ongoing training on Capital Rx's compliance and security requirements.
6. Once the review process finishes, each reviewer should leave a comment on the pull request saying "looks good to me" (often abbreviated as "LGTM"), at which point the original author(s) may merge their change into the release branch.

9.7 Software Release Procedures

1. Software releases are treated as changes to existing systems and thus follow the procedure described in §9.4.

10. Facility Access Policy

Capital Rx works with Subcontractors to assure restriction of physical access to systems used as part of the Capital Rx Platform. Capital Rx and its Subcontractors control access to the physical buildings/facilities that house these systems/applications, or in which Capital Rx workforce members operate, in accordance to the HIPAA Security Rule 164.310 and its implementation specifications. Physical Access to all of Capital Rx facilities is limited to only those authorized in this policy. In an effort to safeguard ePHi from unauthorized access, tampering, and theft, access is allowed to areas only to those persons authorized to be in them and with escorts for unauthorized persons. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Capital Rx's facility.

Capital Rx does not physically house any systems used by its Platform in Capital Rx facilities. Physical security of our Platform servers is outlined in §1.4.

10.1 Applicable Standards

10.1.1 Applicable Standards from the HITRUST Common Security Framework

- 08.b - Physical Entry Controls
- 08.d - Protecting Against External and Environmental Threats
- 08.j - Equipment Maintenance
- 08.l - Secure Disposal or Re-Use of Equipment
- 09.p - Disposal of Media

10.1.2 Applicable Standards from the HIPAA Security Rule

- 164.310(a)(2)(ii) Facility Security Plan
- 164.310(a)(2)(iii) Access Control & Validation Procedures
- 164.310(b-c) Workstation Use & Security

10.2 Capital Rx-controlled Facility Access Policies

1. Visitor and third party support access is recorded and supervised. All visitors are escorted.
2. Repairs are documented and the documentation is retained.
3. Fire extinguishers and detectors are installed according to applicable laws and regulations.

4. Maintenance is controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organization's maintenance program.
5. Electronic and physical media containing covered information is securely destroyed (or the information securely removed) prior to disposal.
6. The organization securely disposes media with sensitive information.
7. Physical access is restricted using smart locks that track all access.
 - Restricted areas and facilities are locked when unattended (where feasible).
 - Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
 - Access and keys are revoked upon termination of workforce members.
 - Workforce members must report a lost and/or stolen key(s) to the Security Officer.
 - The Security Officer facilitates the changing of the lock(s) within 7 days of a key being reported lost/stolen
8. Enforcement of Facility Access Policies
 - Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
 - Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
 - Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Capital Rx.
9. Workstation Security
 - Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
 - All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
 - All workstations purchased by Capital Rx are the property of Capital Rx and are distributed to users by the company.

11. Incident Response Policy

Capital Rx implements an information security incident response process to consistently detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

The incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders

Note: These policies were adapted from work by the HIPAA Collaborative of Wisconsin Security Networking Group. Refer to the linked document for additional copyright information.

11.1 Applicable Standards

11.1.1 Applicable Standards from the HITRUST Common Security Framework

- 11.a - Reporting Information Security Events
- 11.c - Responsibilities and Procedures

11.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308(a)(5)(i) - Security Awareness and Training
- 164.308(a)(6) - Security Incident Procedures

11.2 Incident Management Policies

The Capital Rx incident response process follows the process recommended by SANS, an industry leader in security. Process flows are a direct representation of the SANS process which can be found in this document.

Capital Rx's incident response classifies security-related events into the following categories:

- **Events** - Any observable computer security-related occurrence in a system or network with a negative consequence. Examples:
 - Hardware component failing causing service outages.
 - Software error causing service outages.
 - General network or system instability.
- **Precursors** - A sign that an incident may occur in the future. Examples:
 - Monitoring system showing unusual behavior.
 - Audit log alerts indicated several failed login attempts.
 - Suspicious emails targeting specific Capital Rx staff members with administrative access to production systems.
- **Indications** - A sign that an incident may have occurred or may be occurring at the present time. Examples:
 - IDS alerts for modified system files or unusual system accesses.
 - Antivirus alerts for infected files.
 - Excessive network traffic directed at unexpected geographic locations.
- **Incidents** - A violation of computer security policies or acceptable use policies, often resulting in data breaches. Examples:
 - Unauthorized disclosure of ePHI.
 - Unauthorized change or destruction of ePHI.
 - A data breach accomplished by an internal or external entity.
 - A Denial-of-Service (DoS) attack causing a critical service to become unreachable.

Capital Rx employees must report any unauthorized or suspicious activity seen on production systems or associated with related communication systems (such as email or Slack). In practice this means keeping an eye out for security events, and letting the Security Officer know about any observed precursors or indications as soon as they are discovered.

11.2.1 Identification Phase

1. Immediately upon observation Capital Rx members report suspected and known Events, Precursors, Indications, and Incidents in one of the following ways:
 2. Direct report to management, the Security Officer, Privacy Officer, or other;
 3. Email;
 4. Phone call;
 5. Secure Chat.
 6. Anonymously through workforce members desired channels.
 7. The individual receiving the report facilitates completion of an Incident Identification form and notifies the Security Officer (if not already done).
 8. The Security Officer determines if the issue is an Event, Precursor, Indication, or Incident.
 9. If the issue is an event, indication, or precursor the Security Officer forwards

it to the appropriate resource for resolution.

1. Non-Technical Event (minor infringement): the Security Officer completes a SIR Form and investigates the incident.
 2. Technical Event: Assign the issue to an IT resource for resolution. This resource may also be a contractor or outsourced technical resource, in the event of a small office or lack of expertise in the area.
10. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies senior management.
1. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
 2. Once the investigation is completed, progress to Phase V, Follow-up.
 3. If the issue is a technical security incident, commence to Phase II: Containment.
 4. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.
 5. Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.
 6. The lead member of the SIRT team facilitates initiation of a SIR Form or an Incident Survey Form. The intent of the SIR form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.
11. The Security Officer, Privacy Officer, or Capital Rx representative appointed notifies any affected Customers and Partners. If no Customers and Partners are affected, notification is at the discretion of the Security and Privacy Officer.
12. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal to Capital Rx and potentially external.

11.2.2 Containment Phase (Technical)

In this Phase, Capital Rx's IT department attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

1. The SIRT reviews any information that has been collected by the Security Officer or any other individual investigating the security incident.
2. The SIRT secures the network perimeter.
3. The IT department performs the following:
4. Securely connect to the affected system over a trusted connection.
5. Retrieve any volatile data from the affected system.

6. Determine the relative integrity and the appropriateness of backing the system up.
7. If appropriate, back up the system.
8. Change the password(s) to the affected system(s).
9. Determine whether it is safe to continue operations with the affected system(s).
10. If it is safe, allow the system to continue to function;
 1. Complete any documentation relative to the security incident on the SIR Form.
 2. Move to Phase V, Follow-up.
11. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.
12. The individual completing this phase provides written communication to the SIRT.
13. Continuously apprise Senior Management of progress.
14. Continue to notify affected Customers and Partners with relevant updates as needed

11.2.3 Eradication Phase (Technical)

The Eradication Phase represents the SIRT's effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

1. Determine symptoms and cause related to the affected system(s).
2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:
 3. An increase in network perimeter defenses.
 4. An increase in system monitoring defenses.
 5. Remediation ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques.
 6. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.
 7. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
 8. Complete the Eradication Form.
 9. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
10. Apprise Senior Management of the progress.
11. Continue to notify affected Customers and Partners with relevant updates as needed.
12. Move to Phase IV, Recovery.

11.2.4 Recovery Phase (Technical)

The Recovery Phase represents the SIRT's effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected.

1. The technical team determines if the affected system(s) have been changed in any way.
2. If they have, the technical team restores the system to its proper, intended functioning ("last known good").
3. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
4. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
5. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
6. Update the documentation with the detail that was determined during this phase.
7. Apprise Senior Management of progress.
8. Continue to notify affected Customers and Partners with relevant updates as needed.
9. Move to Phase V, Follow-up.

11.2.5 Follow-up Phase (Technical and Non-Technical)

The Follow-up Phase represents the review of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.

1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident.
2. Create a "lessons learned" document and attach it to the completed SIR Form.
3. Evaluate the cost and impact of the security incident to Capital Rx using the documents provided by the SIRT and the technical security resource.
4. Determine what could be improved.
5. Communicate these findings to Senior Management for approval and for implementation of any recommendations made post-review of the security incident.

6. Carry out recommendations approved by Senior Management; sufficient budget, time and resources should be committed to this activity.
7. Close the security incident.

11.2.6 Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding Capital Rx's expectation for them, relative to security responsibilities. The incident response plan is tested annually.

11.3 Security Incident Response Team (SIRT)

Current members of the Capital Rx SIRT:

- Security Officer
- Privacy Officer

12. Breach Policy

To provide guidance for breach notification when impressive or unauthorized access, acquisition, use and/or disclosure of the ePHI occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities and business associates may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009 (pending publication HHS regulations).

In the case of a breach, Capital Rx shall notify all affected Customers and individuals.

12.1 Applicable Standards

12.1.1 Applicable Standards from the HITRUST Common Security Framework

- 11.a Reporting Information Security Events
- 11.c Responsibilities and Procedures

12.1.2 Applicable Standards from the HIPAA Security Rule

- Security Incident Procedures - 164.308(a)(6)(i)
- HITECH Notification in the Case of Breach - 13402(a) and 13402(b)
- HITECH Timeliness of Notification - 13402(d)(1)
- HITECH Content of Notification - 13402(f)(1)

12.2 Capital Rx Breach Policy

1. Discovery of Breach: A breach of ePHI shall be treated as “discovered” as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to Capital Rx (includes breaches by the organization’s Customers, Partners, or subcontractors). Capital Rx shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or Partner of the organization. Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response) immediately, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each Customer affected by the breach. Capital Rx shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)
2. Breach Investigation: The Capital Rx Security Officer shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years. A template breach log is located here.
3. Risk Assessment: For an acquisition, access, use or disclosure of ePHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. A use or disclosure of ePHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of ePHI constitutes a breach and requires further notification, the organization will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications to appropriate Customers or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the

need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

- Consideration of who impermissibly used or to whom the information was impermissibly disclosed;
 - The type and amount of ePHI involved;
 - The cause of the breach, and the entity responsible for the breach, either Customer, Capital Rx, or Partner.
 - The potential for significant risk of financial, reputational, or other harm.
4. Timeliness of Notification: Upon discovery of a breach, notice shall be made to the affected Capital Rx Customers no later than 4 hours after the discovery of the breach. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.
5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:
- If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
 - If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.
6. Content of the Notice: The notice shall be written in plain language and must contain the following information:
- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 - A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known;
 - Any steps the Customer should take to protect Customer data from potential harm resulting from the breach.
 - A brief description of what Capital Rx is doing to investigate the breach, to mitigate harm to individuals and Customers, and to protect against further breaches.
 - Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number, an e-mail address, a web site, or postal address.
7. Methods of Notification: Capital Rx Customers will be notified via email and phone within the timeframe for reporting breaches, as outlined above.

8. **Maintenance of Breach Information/Log:** As described above and in addition to the reports created for each incident, Capital Rx shall maintain a process to record or log all breaches of unsecured ePHI regardless of the number of records and Customers affected. The following information should be collected/logged for each breach (see sample Breach Notification Log):
 - A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers affected, if known.
 - A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.), if known.
 - A description of the action taken with regard to notification of patients regarding the breach.
 - Resolution steps taken to mitigate the breach and prevent future occurrences.
10. **Workforce Training:** Capital Rx shall train all members of its workforce on the policies and procedures with respect to ePHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.
11. **Complaints:** Capital Rx must provide a process for individuals to make complaints concerning the organization's patient privacy policies and procedures or its compliance with such policies and procedures.
12. **Sanctions:** The organization shall have in place and apply appropriate sanctions against members of its workforce, Customers, and Partners who fail to comply with privacy policies and procedures.
13. **Retaliation/Waiver:** Capital Rx may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

12.3 Capital Rx Platform Customer Responsibilities

1. The Capital Rx Customer that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured ePHI shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify Capital Rx of such breach. The Customer shall provide Capital Rx with the following information:
 - A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers

affected, if known.

- A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.), if known.
 - A description of the action taken with regard to notification of patients regarding the breach.
 - Resolution steps taken to mitigate the breach and prevent future occurrences.
2. Notice to Media: Capital Rx Customers are responsible for providing notice to prominent media outlets at the Customer's discretion.
 3. Notice to Secretary of HHS: Capital Rx Customers are responsible for providing notice to the Secretary of HHS at the Customer's discretion.

12.4 Sample Letter to Customers in Case of Breach

[Date]

[Name][Name of Customer] [Address 1][Address 2] [City, State Zip Code]

Dear [Name of Customer]:

I am writing to you from Capital Rx, Inc., with important information about a recent breach that affects your account with us. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known.
- Any steps the Customer should take to protect themselves from potential harm resulting from the breach.
- A brief description of what Capital Rx is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, web site, or postal address.

Other Optional Considerations:

- Recommendations to assist customer in remedying the breach.

We will assist you in remedying the situation.

Sincerely,

A.J. Loiacono CEO - Capital Rx, Inc.
aj@cap-rx.com
(917) 379-5317

13. Disaster Recovery Policy

The Capital Rx Contingency Plan establishes procedures to recover Capital Rx following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the Capital Rx Security Officer and Privacy Officer.

The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
 - *Notification/Activation phase* to detect and assess damage and to activate the plan;
 - *Recovery phase* to restore temporary IT operations and recover damage done to the original system;
 - *Reconstitution phase* to restore IT system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out Capital Rx processing requirements during prolonged interruptions to normal operations.
3. Identify and define the impact of interruptions to Capital Rx systems.
4. Assign responsibilities to designated personnel and provide guidance for recovering Capital Rx during prolonged periods of interruption to normal operations.
5. Ensure coordination with other Capital Rx staff who will participate in the contingency planning strategies.
6. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

This Capital Rx Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a)(7), which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

This Capital Rx Contingency Plan is created under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems" dated June 2002.

The Capital Rx Contingency Plan also complies with the following federal and departmental policies:

- The Computer Security Act of 1987;

- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000;
- Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999;
- Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998;
- PDD 63, Critical Infrastructure Protection, May 1998;
- Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999;
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, “Government Information Security Reform,” October 30, 2000

Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, internal malicious activities.

Capital Rx defined two categories of systems from a disaster recovery perspective.

1. *Critical Systems*. These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.
2. *Non-critical Systems*. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

13.1 Applicable Standards

13.1.1 Applicable Standards from the HITRUST Common Security Framework

- 12.c - Developing and Implementing Continuity Plans Including Information Security

13.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308(a)(7)(i) - Contingency Plan

13.2 Line of Succession

The following order of succession to ensure that decision-making authority for the Capital Rx Contingency Plan is uninterrupted. The Chief Technology Officer (CTO) is responsible for ensuring the safety of personnel and the execution of procedures documented within this Capital Rx Contingency Plan. If the CTO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the CEO or COO shall function as that authority. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below.

- Ryan Kelly, CTO: (845) 222-5529, ryan@cap-rx.com
- Joe Alexander, COO: (615) 294-0538, joe@cap-rx.com

13.3 Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

1. The **Infrastructure Team** is responsible for recovery of the Capital Rx hosted environment, network devices, and all servers. Members of the team include personnel who are also responsible for the daily operations and maintenance of Capital Rx. The team leader is the CTO and directs the Infrastructure Team.
2. The **Services Team** is responsible for assuring all application servers, web services, and platform add-ons are working. It is also responsible for testing redeployments and assessing damage to the environment. The team leader is the CTO and directs the Services Team.

Members of the Infrastructure and Services teams must maintain local copies of the contact information from §13.2. Additionally, the CTO must maintain a local copy of this policy in the event Internet access is not available during a disaster scenario.

13.4 Testing and Maintenance

The CTO shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

13.4.1 Tabletop Testing

Tabletop Testing is conducted in accordance with the the CMS Risk Management Handbook, Volume 2. The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

13.4.2 Technical Testing

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch compute and storage resources to alternate processing site.

13.5 Disaster Recovery Procedures

13.5.1 Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Capital Rx. Based on the assessment of the Event, sometimes according to the Capital Rx Incident Response Policy, the Contingency Plan may be activated by either the CTO or the COO.

The notification sequence is listed below:

- The first responder is to notify the CTO. All known information must be relayed to the CTO.
- The CTO is to contact the Services Team and inform them of the event. The CTO is to to begin assessment procedures.
- The CTO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CTO is to following the steps below.
- Damage Assessment Procedures:
- The CTO is to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.
- Alternate Assessment Procedures:

- Upon notification, the CTO is to follow the procedures for damage assessment with combined Infrastructure and Services Teams.
- The Capital Rx Contingency Plan is to be activated if one or more of the following criteria are met:
 - Capital Rx will be unavailable for more than 48 hours.
 - Hosting facility is damaged and will be unavailable for more than 24 hours.
 - Other criteria, as appropriate and as defined by Capital Rx.
- If the plan is to be activated, the CTO is to notify and inform team members of the details of the event and if relocation is required.
- Upon notification from the CTO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The CTO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
- The CTO is to notify remaining personnel and executive leadership on the general status of the incident.
- Notification can be message, email, or phone.

13.5.2 Recovery Phase

This section provides procedures for recovering the application at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the Capital Rx infrastructure at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild Capital Rx infrastructure to a production state.

The tasks outlines below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected - Services
2. Assess damage to the environment - Services
3. Begin replication of new environment using automated and tested scripts, currently Salt and Terraform, and following the procedures provided in a runbook or other documentation. - Infrastructure
4. Test new environment using pre-written tests - Services
5. Test logging, security, and alerting functionality - Infrastructure
6. Assure systems are appropriately patched and up to date. - Infrastructure
7. Deploy environment to production - Services
8. Update DNS to new environment. - Infrastructure

13.5.3 Reconstitution Phase

This section discusses activities necessary for restoring Capital Rx operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. When the hosted data center at the original or new site has been restored, Capital Rx operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

1. Original or New Site Restoration

- Begin replication of new environment using automated and tested scripts, currently Salt and Terraform, and following the procedures provided in a runbook or other documentation. - Infrastructure
- Test new environment using pre-written tests. - Services
- Test logging, security, and alerting functionality. - Infrastructure
- Deploy environment to production - Services
- Assure systems are appropriately patched and up to date. - Infrastructure
- Update DNS to new environment. - Infrastructure

2. Plan Deactivation

- If the Capital Rx environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the Capital Rx Media Disposal Policy.

14. Disposable Media Policy

Capital Rx recognizes that media containing ePHI may be reused when appropriate steps are taken to ensure that all stored ePHI has been effectively rendered inaccessible. Destruction/disposal of ePHI shall be carried out in accordance with federal and state law. The schedule for destruction/disposal shall be suspended for ePHI involved in any open investigation, audit, or litigation.

Capital Rx utilizes dedicated hardware from Subcontractors. All data stores utilized by Capital Rx and Capital Rx Customers are encrypted. Capital Rx does not use, own, or manage any removable hard drives, SD cards, or tapes that have access to ePHI.

14.1 Applicable Standards

14.1.1 Applicable Standards from the HITRUST Common Security Framework

- 0.9o - Management of Removable Media

14.1.2 Applicable Standards from the HIPAA Security Rule

- 164.310(d)(1) - Device and Media Controls

14.2 Disposable Media Policy

1. All removable media is restricted, audited, and is encrypted.
2. Capital Rx assumes all disposable media in its Platform may contain ePHI, so it treats all disposable media with the same protections and disposal policies.
3. All destruction/disposal of ePHI media will be done in accordance with federal and state laws and regulations and pursuant to the Capital Rx's written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
4. Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.

5. Before reuse of any media, for example all ePHI is rendered inaccessible, cleaned, or scrubbed. All media is formatted to restrict future access.
6. All Capital Rx Subcontractors provide that, upon termination of the contract, they will return or destroy/dispose of all patient health information. In cases where the return or destruction/disposal is not feasible, the contract limits the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
7. Any media containing ePHI is disposed using a method that ensures the ePHI could not be readily recovered or reconstructed.
8. The methods of destruction, disposal, and reuse are reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.
9. In the cases of a Capital Rx Customer terminating a contract with Capital Rx and no longer utilizing Capital Rx Services, the following actions will be taken depending on the Capital Rx Services in use. In all cases it is solely the responsibility of the Capital Rx Customer to maintain the safeguards required of HIPAA once the data is transmitted out of Capital Rx Systems.

15. IDS Policy

In order to preserve the integrity of data that Capital Rx stores, processes, or transmits for Customers, Capital Rx implements strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access. Capital Rx currently utilizes OSSEC to track file system integrity, monitor log data, and detect rootkit access.

15.1 Applicable Standards

15.1.1 Applicable Standards from the HITRUST Common Security Framework

- 09.ab - Monitoring System Use
- 06.e - Prevention of Misuse of Information
- 10.h - Control of Operational Software

15.1.2 Applicable Standards from the HIPAA Security Rule

- 164.312(b) - Audit Controls

15.2 Intrusion Detection Policy

1. OSSEC is used to monitor and correlate log data from different systems on an ongoing basis. Reports generated by OSSEC are reviewed by the Security Officer on a monthly basis.
2. OSSEC generates alerts to analyze and investigate suspicious activity or suspected violations.
3. OSSEC monitors file system integrity and sends real time alerts when suspicious changes are made to the file system.
4. Automatic monitoring is done to identify patterns that might signify the lack of availability of certain services and systems (DoS attacks).
5. Capital Rx firewalls monitor all incoming traffic to detect potential denial of service attacks. Suspected attack sources are blocked automatically. Additionally, our hosting provider actively monitors its network to detect denial of services attacks.
6. All new firewall rules and configuration changes are tested before being pushed into production. All firewall and router rules are reviewed every quarter.
7. Capital Rx utilizes redundant firewall on network perimeters.

16. Vulnerability Scanning Policy

Capital Rx is proactive about information security and understands that vulnerabilities need to be monitored on an ongoing basis. Capital Rx utilizes AWS Inspector to consistently scan, identify, and address vulnerabilities on our systems. We also utilize OSSEC on all systems, including logs, for file integrity checking and intrusion detection.

16.1 Applicable Standards

16.1.1 Applicable Standards from the HITRUST Common Security Framework

- 10.m - Control of Technical Vulnerabilities

16.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308(a)(8) - Evaluation

16.2 Vulnerability Scanning Policy

1. AWS Inspector management is performed by the Capital Rx Security Officer, or an authorized delegate of the Security Officer.
2. AWS Inspector is used to monitor all long running services (servers, VMs, containers, etc) on Capital Rx networks.
3. AWS Inspector continuously monitors hosts.
4. Reviewing AWS Inspector reports and findings, as well as any further investigation into discovered vulnerabilities, is the responsibility of the Capital Rx Security Officer. The process for reviewing such reports is outlined below:
5. The Security Officer initiates the review of an AWS Inspector report by creating an Issue in the Capital Rx Quality Management System.
6. The Security Officer, or a delegate assigned by the Security Officer, is assigned to review the report.
7. If new vulnerabilities are found during review, the process outlined below is used to test those vulnerabilities. Once those steps are completed, the Issue is then reviewed again.
8. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review.
9. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
10. In the case of new vulnerabilities, the following steps are taken:

- All new vulnerabilities are verified manually to assure they are repeatable. Those not found to be repeatable are manually tested after the next vulnerability scan, regardless of if the specific vulnerability is discovered again.
 - Vulnerabilities that are repeatable manually are documented and reviewed by the Security Officer and Privacy Officer to see if they are part of the current risk assessment performed by Capital Rx.
 - Those that are a part of the current risk assessment are checked for mitigations.
 - Those that are not part of the current risk assessment trigger a new risk assessment, and this process is outlined in detail in the Capital Rx Risk Assessment Policy.
6. All vulnerability scanning reports are retained for 6 years by Capital Rx. Vulnerability report review is monitored on a quarterly basis using the Quality Management System reporting to assess compliance with above policy.
 7. Penetration testing is performed regularly as part of the Capital Rx vulnerability management policy.
 - External penetration testing is performed annually by a third party.
 - Internal penetration testing is performed quarterly. Below is the process used to conduct internal penetration tests.
 1. The Security Officer initiates the penetration test by creating an Issue in the Capital Rx Quality Management System.
 2. The Security Officer, or a Capital Rx Security Engineer assigned by the Security Officer, is assigned to conduct the penetration test.
 3. Gaps and vulnerabilities identified during penetration testing are reviewed, with plans for correction and/or mitigation, by the Capital Rx Security Officer before the Issue can move to be approved.
 4. Once the testing is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further testing and review.
 5. If the Issue is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
 - Penetration tests results are retained for 6 years by Capital Rx.
 - Internal penetration testing is monitored on an annual basis using the Quality Management System reporting to assess compliance with above policy.
 8. This vulnerability policy is reviewed on a quarterly basis by the Security Officer and Privacy Officer.

17. Data Integrity Policy

Capital Rx takes data integrity very seriously. As stewards and partners of Capital Rx Customers, we strive to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical settings in support of the Capital Rx mission of data protection.

Production systems that create, receive, store, or transmit Customer data (hereafter “production systems”) must follow the guidelines described in this section.

17.1 Applicable Standards

17.1.1 Applicable Standards from the HITRUST Common Security Framework

- 10.b - Input Data Validation

17.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308(a)(8) - Evaluation

17.2 Disabling Non-Essential Services

1. All production systems must disable services that are not required to achieve the business purpose or function of the system.

17.3 Monitoring Log-in Attempts

1. All access to production systems must be logged. This is done following the Capital Rx Auditing Policy.

17.4 Prevention of Malware on Production Systems

1. All Capital Rx managed production systems must have OSSEC running, and set to scan system every 2 hours and at reboot to assure not malware is present. Detected malware is evaluated and removed.
 2. Virus scanning software is run on all Capital Rx managed production systems for anti-virus protection.
- Hosts are scanned daily for malicious binaries in critical system paths.

- The malware signature database is checked hourly and automatically updated if new signatures are available.
 - Logs of virus scans are maintained according to the requirements outlined in §8.6.
3. All Capital Rx managed production systems are to only be used for Capital Rx business needs.

17.5 Patch Management

1. Software patches and updates will be applied to all systems in a timely manner. In the case of routine updates, they will be applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within 30 days from testing and all security patches are applied within 90 days after testing.
2. Administrators subscribe to mailing lists to ensure that they are using current versions of all Capital Rx-managed software on production systems.

17.6 Intrusion Detection and Vulnerability Scanning

1. Capital Rx managed production systems are monitored using IDS systems. Suspicious activity is logged and alerts are generated.
2. Vulnerability scanning of Capital Rx managed production systems must occur on a predetermined, regular basis, no less than annually. Currently it is weekly. Scans are reviewed by Security Officer, with defined steps for risk mitigation, and retained for future reference.

17.7 Production System Security

1. System, network, and server security is managed and maintained by the Security Officer in conjunction with the Infrastructure team.
2. Up to date system lists and architecture diagrams are kept for all production environments.
3. Access to Capital Rx managed production systems is controlled using centralized tools and two-factor authentication.

17.8 Production Data Security

1. Reduce the risk of compromise of Production Data.
2. Implement and/or review controls designed to protect Production Data from improper alteration or destruction.

3. Ensure that confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
4. Ensure Capital Rx Customer Production Data is segmented and only accessible to Customers authorized to access data.
5. All Production Data at rest is encrypted. Encryption at rest is ensured through the use of automated deployment scripts referenced in the Configuration Management Policy.
6. Volume encryption keys and machines that generate volume encryption keys are protected from unauthorized access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
7. Encrypted volumes use AES encryption with a minimum of 256-bit keys, or keys and ciphers of equivalent or higher cryptographic strength.

17.9 Transmission Security

1. All data transmission is encrypted end to end. Encryption is not terminated at the network end point, and is carried through to the application.
2. Transmission encryption keys and machines that generate keys are protected from unauthorized access. Transmission encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
3. Transmission encryption keys use a minimum of 4096-bit RSA keys, or keys and ciphers of equivalent or higher cryptographic strength (e.g., 256-bit AES session keys in the case of IPsec encryption).
4. Transmission encryption keys are limited to use for one year and then must be regenerated.
5. In the case of Capital Rx provided APIs, provide mechanisms to assure person sending or receiving data is authorized to send and save data.
6. System logs of all transmissions of Production Data access. These logs must be available for audit.

18. Data Retention Policy

Despite not being a requirement within HIPAA, Capital Rx understands and appreciates the importance of health data retention. Acting as a subcontractor, and at times a business associate, Capital Rx is not directly responsible for health and medical records retention as set forth by each state. Despite this, Capital Rx has created and implemented the following policy to make it easier for Capital Rx Customers to support data retention laws.

18.1 State Medical Record Laws

- Listing of state requirements for medical record retention

18.2 Data Retention Policy

- Current Capital Rx Customers have data stored by Capital Rx as a part of the Capital Rx Service.
- Once a Customer ceases to be a Customer, as defined below, the following steps are
 1. Customer is sent a notice via email of change of standing, and given the option to reinstate account.
 2. If no response to notice in #1 above within 7 days, or if Customer responds they do not want to reinstate account, Customer is sent directions for how to download their data from Capital Rx and/or to have Capital Rx continue to store the data at a rate of \$25/month for up to 100GB. If there is more than 100GB of data, Capital Rx will work with Customer to determine storage costs.
 3. If Customer downloads data or does not respond to notices from Capital Rx within 30 days, Capital Rx will remove data from Capital Rx systems and Customer is sent notice of removal of data.

19. Employees Policy

Capital Rx is committed to ensuring all workforce members actively address security and compliance in their roles at Capital Rx. As such, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

19.1 Applicable Standards

19.1.1 Applicable Standards from the HITRUST Common Security Framework

- 02.e - Information Security Awareness, Education, and Training
- 06.e - Prevention of Misuse of Information Assets
- 07.c - Acceptable Use of Assets
- 09.j - Controls Against Malicious Code
- 01.y - Teleworking

19.1.2 Applicable Standards from the HIPAA Security Rule

- 164.308(a)(5)(i) - Security Awareness and Training

19.2 Employment Policies

1. All new workforce members, including contractors, are given training on security policies and procedures, including operations security, within 30 days of employment.
 - Records of training are kept for all workforce members.
 - Employees must complete this training before accessing production systems containing ePHI.
2. All workforce members are granted access to formal organizational policies, which include the sanction policy for security violations.
3. The Capital Rx Employee Handbook clearly states the responsibilities and acceptable behavior regarding information system usage, including rules for email, Internet, mobile devices, and social media usage.
 - Workforce members are required to sign an agreement stating that they have read and will abide by all terms outlined in the Capital Rx Employee Handbook, along with all policies and processes described in this document.
 - A Human Resources representative will provide the agreement to new employees during their onboarding process.

4. Capital Rx does not allow mobile devices to connect directly to any of its production networks.
5. All workforce members are educated about the approved set of tools to be installed on workstations.
6. All new workforce members are given HIPAA training within 30 days of beginning employment. Training includes HIPAA reporting requirements, including the ability to anonymously report security incidents, and the levels of compliance and obligations for Capital Rx and its Customers and Partners.
7. All remote (teleworking) workforce members are trained on the risks, the controls implemented, their responsibilities, and sanctions associated with violation of policies. Additionally, remote security is maintained through the use of secure links for all access to production systems with access to ePHI data.
8. Employees may only use Capital Rx-purchased and -owned workstations for accessing production systems with access to ePHI data.
 - Any workstations used to access production systems must be configured as prescribed in §7.8.
 - Any workstations used to access production systems must have virus protection software installed, configured, and enabled.
 - Capital Rx may monitor access and activities of all users on workstations and production systems in order to meet auditing policy requirements (§8).
9. Access to internal Capital Rx systems can be requested using the procedures outlined in §7.2. All requests for access must be granted by the Capital Rx Security Officer.
10. Request for modifications of access for any Capital Rx employee can be made using the procedures outlined in §7.2.
11. Employees are required to cooperate with federal and state investigations.
 - Employees must not interfere with investigations through willful misrepresentation, omission of facts, or by the use of threats against any person.
 - Employees found to be in violation of this policy will be subject to sanctions as described in §5.3.3.

19.3 Issue Escalation

Capital Rx workforce members are to escalate issues using the procedures outlined in the Employee Handbook. Issues that are brought to the Escalation Team are assigned an owner. The membership of the Escalation Team is maintained by the Chief Executive Officer.

Security incidents, particularly those involving ePHI, are handled using the process described in §11.2. If the incident involves a breach of ePHI, the Security Officer will manage the incident using the process described in §12.2. Refer to

§11.2 for a list of sample items that can trigger Capital Rx's incident response procedures; if you are unsure whether the issue is a security incident, contact the Security Officer immediately.

It is the duty of that owner to follow the process outlined below:

1. Create an Issue in the Capital Rx Quality Management System.
2. The Issue is investigated, documented, and, when a conclusion or remediation is reached, it is moved to Review.
3. The Issue is reviewed by another member of the Escalation Team. If the Issue is rejected, it goes back for further evaluation and review.
4. If the Issue is approved, it is marked as Done, adding any pertinent notes required.
5. The workforce member that initiated the process is notified of the outcome via email.

20. Approved Tools Policy

Capital Rx utilizes a suite of approved software tools for internal use by workforce members. These software tools are either self-hosted, with security managed by Capital Rx, or they are hosted by a Subcontractor with appropriate business associate agreements in place to preserve data integrity. Use of other tools requires approval from Capital Rx leadership.

20.1 List of Approved Tools

- **GitHub.** GitHub is a fully-managed platform built on top of Git, the version control platform. It is utilized for storage of configuration scripts and other infrastructure automation tools, as well as for source and version control of application code used by Capital Rx.
- **Dropbox.** Dropbox is used for storage of files and sharing of files with Partners and Customers.
- **Office 365.** Office 365 is used for email and document collaboration.
- **Slack.** Slack is an office workplace chat tool.
- **JIRA.** JIRA is used for the implementation of Capital Rx's Quality Management System.
- **PyCharm.** Pycharm is an IDE used for writing code.
- **Visual Studio Code.** VS Code is an IDE used for writing code.
- **Sublime.** Sublime is a text editor used for writing code.
- **Postman.** Postman is a collaboration platform for API Development.

- **Zoom.** Zoom is a video conferencing tool.
- **BlueJeans.** BlueJeans is a video conferencing tool.

21. 3rd Party Policy

Capital Rx makes every effort to assure all 3rd party organizations are compliant and do not compromise the integrity, security, and privacy of Capital Rx or Capital Rx Customer data. 3rd Parties include Customers, Partners, Subcontractors, and Contracted Developers.

21.1 Applicable Standards

21.1.1 Applicable Standards from the HITRUST Common Security Framework

- 05.i - Identification of Risks Related to External Parties
- 05.k - Addressing Security in Third Party Agreements
- 09.e - Service Delivery
- 09.f - Monitoring and Review of Third Party Services
- 09.g - Managing Changes to Third Party Services
- 10.1 - Outsourced Software Development

21.1.2 Applicable Standards from the HIPAA Security Rule

- 164.314(a)(1)(i) - Business Associate Contracts or Other Arrangements

21.2 Policies to Assure 3rd Parties Support Capital Rx Compliance

1. Capital Rx does not allow 3rd party access to production systems containing ePHI.
 2. All connections and data in transit between the Capital Rx Platform and 3rd parties are encrypted end to end.
 3. A standard business associate agreement with Customers and Partners is defined and includes the required security controls in accordance with the organization's security policies. Additionally, responsibility is assigned in these agreements.
 4. Capital Rx has Service Level Agreements (SLAs) with Subcontractors with an agreed service arrangement addressing liability, service definitions, security controls, and aspects of services management.
- Subcontractors must coordinate, manage, and communicate any changes to services provided to Capital Rx.
 - Changes to 3rd party services are classified as configuration management changes and thus are subject to the policies and procedures described in

- §9; substantial changes to services provided by 3rd parties will invoke a Risk Assessment as described in §4.2.
- Capital Rx utilizes monitoring tools to regularly evaluate Subcontractors against relevant SLAs.
5. No Capital Rx Customers or Partners have access outside of their own environment, meaning they cannot access, modify, or delete anything related to other 3rd parties.
 6. Capital Rx may outsource software development; however, all development occurs according to the policies and procedures described in §9.
 7. Capital Rx maintains and annually reviews a list all current Partners and Subcontractors.
 - The list of current Partners and Subcontractors is maintained by the Capital Rx Privacy Officer, includes details on all provided services (along with contact information), and is recorded in §1.4.
 - The annual review of Partners and Subcontractors is conducted as a part of the security, compliance, and SLA review referenced below.
 8. Capital Rx assesses security, compliance, and SLA requirements and considerations with all Partners and Subcontractors. This includes annual assessment of SOC2 reports for all Capital Rx infrastructure partners.
 - Capital Rx leverages recurring calendar invites to assure reviews of all 3rd party services are performed annually. These reviews are performed by the Capital Rx Security Officer and Privacy Officer. The process for reviewing 3rd party services is outlined below:
 1. The Security Officer initiates the SLA review by creating an Issue in the Capital Rx Quality Management System.
 2. The Security Officer, or Privacy Officer, is assigned to review the SLA and performance of 3rd parties. The list of current 3rd parties, including contact information, is also reviewed to assure it is up to date and complete.
 3. SLA, security, and compliance performance is documented in the Issue.
 4. Once the review is completed and documented, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.
 9. Regular review is conducted as required by SLAs to assure security and compliance. These reviews include reports, audit trails, security events, operational issues, failures and disruptions, and identified issues are investigated and resolved in a reasonable and timely manner.
 10. Any changes to Partner and Subcontractor services and systems are reviewed before implementation.
 11. For all partners, Capital Rx reviews activity annually to assure partners are in line with SLAs in contracts with Capital Rx.
 12. SLA review is monitored on a quarterly basis using the Quality Management

System reporting to assess compliance with above policy.

13. The 3rd Party Assurance process is reviewed annually and updated to include any necessary changes.
14. Changes to the 3rd Party Assurance process will also be made on an ad-hoc basis in cases where operational changes require it or if the process is found lacking.

22. Key Definitions

- *Application*: An application hosted by Capital Rx, either maintained and created by Capital Rx, or maintained and created by a Customer or Partner.
- *Application Level*: Controls and security associated with an Application.
- *Audit*: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing.
- *Audit Controls*: Technical mechanisms that track and record computer/system activities.
- *Audit Logs*: Encrypted records of activity maintained by the system which provide: 1) date and time of activity; 2) origin of activity (app); 3) identification of user doing activity; and 4) data accessed as part of activity.
- *Access*: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.
- *Backup*: The process of making an electronic copy of data stored in a computer system. This can either be complete, meaning all data and programs, or incremental, including just the data that changed from the previous backup.
- *Backup Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Offered with all Capital Rx Add-ons and as an option for PaaS Customers.
- *Breach*: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, “compromises the security or privacy of the PHI” means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI. Breach excludes:
 1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
 2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates,

and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

3. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
 - *Business Associate*: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
 - *Covered Entity*: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.
 - *De-identification*: The process of removing identifiable information so that data is rendered to not be PHI.
 - *Disaster Recovery*: The ability to recover a system and data after being made unavailable.
 - *Disclosure*: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.
 - *Customers*: Contractually bound users of Capital Rx Platform.
 - *Electronic Protected Health Information (ePHI)*: Any individually identifiable health information protected by HIPAA that is transmitted by, processed in some way, or stored in electronic media.
 - *Environment*: The overall technical environment, including all servers, network devices, and applications.
 - *Event*: An event is defined as an occurrence that does not constitute a serious adverse effect on Capital Rx, its operations, or its Customers, though it may be less than optimal. Examples of events may include, but are not limited to:
 - A hard drive malfunction that requires replacement;
 - Systems become unavailable due to power outage that is non-hostile in nature, with redundancy to assure ongoing availability of data;
 - Accidental lockout of an account due to incorrectly entering a password multiple times.
 - *Hardware (or hard drive)*: Any computing device able to create and store ePHI.
 - *Health and Human Services (HHS)*: The government body that maintains HIPAA.
 - *Individually Identifiable Health Information*: That information that is a subset of health information, including demographic information collected

from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

- *Indication*: A sign that an Incident may have occurred or may be occurring at the present time. Examples of indications include:
 - The network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS “hits” are also false positives and are neither an event nor an incident;
 - The antivirus software alerts when it detects that a host is infected with a worm;
 - Users complain of slow access to hosts on the Internet;
 - The system administrator sees a filename with unusual characteristics;
 - Automated alerts of activity from log monitors like OSSEC;
 - An alert from OSSEC about file system integrity issues.
- *Intrusion Detection System (IDS)*: A software tool use to automatically detect and notify in the event of possible unauthorized network and/or system access.
- *IDS Service*: An Intrusion Detection Service for providing IDS notification to customers in the case of suspicious activity. Offered with all Capital Rx Add-ons and as an option for PaaS Customers.
- *Law Enforcement Official*: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- *Logging Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Offered with all Capital Rx Add-ons and as an option for PaaS Customers.
- *Messaging*: API-based services to deliver and receive SMS messages.
- *Minimum Necessary Information*: Protected health information that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The “minimum necessary” standard applies to all protected health information in any form.

- *Off-Site*: For the purpose of storage of Backup media, off-site is defined as any location separate from the building in which the backup was created. It must be physically separate from the creating site.
- *Organization*: For the purposes of this policy, the term “organization” shall mean Capital Rx.
- *Partner* : Contractual bound 3rd party vendor with integration with the Capital Rx Platform. May offer Add-on services.
- *Platform*: The overall technical environment of Capital Rx.
- *Protected Health Information (PHI)*: Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
 - Past, present or future physical or mental health or condition of an individual.
 - The provision of health care to an individual.
 - The past, present, or future payment for the provision of health care to an individual.
- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *Sanitization*: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.
- *Trigger Event*: Activities that may be indicative of a security breach that require further investigation (See Appendix).
- *Restricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is stored, utilized, or accessible at any time.
- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *Precursor* : A sign that an Incident may occur in the future. Examples of precursors include:
 - Suspicious network and host-based IDS events/attacks;
 - Alerts as a result of detecting malicious code at the network and host levels;
 - Alerts from file integrity checking software;

- Audit log alerts.
- *Risk*: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.
- *Risk Management Team*: Individuals who are knowledgeable about the Organization's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below.
- *Risk Assessment*: (Referred to as Risk Analysis in the HIPAA Security Rule); the process:
 - Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
 - Prioritizes risks; and
 - Results in recommended possible actions/controls that could reduce or offset the determined risk.
- *Risk Management*: Within this policy, it refers to two major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).
- *Risk Mitigation*: Referred to as Risk Management in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.
- *Security Incident* (or just Incident): A security incident is an occurrence that exercises a significant adverse effect on people, process, technology, or data. Security incidents include, but are not limited to:
 - A system or network breach accomplished by an internal or external entity; this breach can be inadvertent or malicious;
 - Unauthorized disclosure;
 - Unauthorized change or destruction of ePHI (i.e. delete dictation, data alterations not following Capital Rx's procedures);
 - Denial of service not attributable to identifiable physical, environmental, human or technology causes;
 - Disaster or enacted threat to business continuity;

- **Information Security Incident:** A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples of information security incidents may include, but are not limited to, the following:
 - **Denial of Service:** An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources;
 - **Malicious Code:** A virus, worm, Trojan horse, or other code-based malicious entity that infects a host;
 - **Unauthorized Access/System Hijacking:** A person gains logical or physical access without permission to a network, system, application, data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations;
 - **Inappropriate Usage:** A person violates acceptable computing use policies;
 - **Other examples of observable information security incidents may include, but are not limited to:**
 - Use of another person’s individual password and/or account to login to a system;
 - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment);
 - Installation of unauthorized software;
 - Terminated workforce member accessing applications, systems, or network.
- **Threat:** The potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:
 - **Environmental** - external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
 - **Human** - hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
 - **Natural** - fires, floods, electrical storms, tornados, etc.
 - **Technological** - server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
 - **Other** - explosions, medical emergencies, misuse or resources, etc.
- **Threat Source:** Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization’s ability to protect ePHI.

- *Threat Action*: The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).
 - *Unrestricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is not stored or is not utilized or is not accessible there on a regular basis.
 - *Unsecured Protected Health Information*: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.
1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
 2. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
 3. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
 4. The media on which the PHI is stored or recorded has been destroyed in the following ways:
 5. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
 6. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.
- *Vendors*: Persons from other organizations marketing or selling products or services, or providing services to Capital Rx.
 - *Vulnerability*: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

- *Workstation*: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), tablet PCs, and other handheld devices. For the purposes of this policy, “workstation” also includes the combination of hardware, operating system, application software, and network connection.
- *Workforce*: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Health Action Council & Cooperative Council of Governments RFP #2020.03.19 for PBM Services

Attachment B: Cost Proposal

Excelsior Solutions

Signature Tab

Pricing Requirements - Traditional Bids Tab

Pricing Requirements - Pass-Through Bids Tab

Other Credits and Fees Tab

Med Rx Alignment Credit Tab

Clinical Program Fees Tab

Pricing Scenarios Tabs

Lists Requested



2100 Ross Ave, Ste. 1200
Dallas, TX 75201

www.lockton.com
smartin@lockton.com
816-489-2545



Bidder Signature Page

The bidder must include this signature page in the Attachment B RFP response under Signature Tab.
Please sign in **BLUE INK**.

Company:

Bidder Name:

Bidder Signature :

Bidder Primary Contact Name/email:

Date of Bid Submission :

CAPITAL EX
ANTHONY J. BARRETT
Anthony J. Barrett
BARRETT@CAP-EX.COM
4/23/20

Pricing Requirements - Pass Through Bids

Question #	QUESTIONS - Please indicate YES/NO as applicable.	Bidder Response	Point Value	Comments to Bidders	Comments from Bidders
1	Bidder agrees that all answers in this document are binding and supersede any pricing supplement provided as an Appendix. Pricing supplements may be provided if you wish to provide more details but there is no guarantee it will be reviewed by the Proposal Team.	Yes	4		
Discounts					
	Bidder agrees the proposed "effective" generic discount and the generic discount guarantee calculation INCLUDES the following:			In addition to point value, valuation of the bids will be adjusted accordingly if this is not confirmed.	
2	MAC Generics	Yes	5		Capital Rx's Clearinghouse Model guarantees that each claim, without exclusions or exceptions, will be adjudicated according to the Clearinghouse logic outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> .
3	Non-MAC Generics	Yes	5		Please refer to explanation for 2 above.
4	Single Source Generics	Yes	5		Please refer to explanation for 2 above.
5	Multi-Source Generics	Yes	5		Please refer to explanation for 2 above.
6	Generics in their FDA-granted exclusivity period	Yes	5		Please refer to explanation for 2 above.
7	Generics launched at risk	Yes	5		Please refer to explanation for 2 above.
8	Patent litigated claims	Yes	5		Please refer to explanation for 2 above.
9	Generics with limited supply	Yes	5		Please refer to explanation for 2 above.
10	Generic medications prescribed and/or dispensed in conjunction with a specialty medication	Yes	5		Please refer to explanation for 2 above.
	Bidder agrees all proposed "effective" discounts and the discount guarantee calculation, dispensing fees and dispensing fee guarantee calculation EXCLUDES the following:			In addition to point value, valuation of the bids will be adjusted accordingly if this is not confirmed.	
11	U&C Claims	No	5		Capital Rx's Clearinghouse Model guarantees that each claim, without exclusions or exceptions, will be adjudicated according to the Clearinghouse logic outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> .
12	Reversed/Rejected Claims	No	5		Please refer to explanation for 11 above.
13	Compound Claims	No	5		Please refer to explanation for 11 above.
14	340B claims	No	5		Please refer to explanation for 11 above.
15	OTC claims (except insulin and diabetic test strips)	No	5		Please refer to explanation for 11 above.
16	Member Submitted Claims	No	1		Please refer to explanation for 11 above.
17	Bidder agrees that all claims filed in all states and Puerto Rico are INCLUDED in discount guarantees.	Yes	1		Please refer to explanation for 11 above.
18	Bidder agrees that all claims filed in rural pharmacies are INCLUDED in discount guarantees.	Yes	1		Please refer to explanation for 11 above.
19	Bidder agrees that 100% Member Paid Claims (Zero Balance Due Claims) will be INCLUDED in discount guarantees, with discounts calculated based on the ingredient cost before the subtraction of member paid amount.	Yes	10		Please refer to explanation for 11 above.
Calculations/Definitions					
	Bidder agrees to all the following calculations/definitions				
	Average Wholesale Price (AWP) must be based on ALL of the following criteria:				
20	Provided by Medi-Span	Yes	10		
21	Actual date that the drug is dispensed	Yes	10		
22	Actual package size used for dispensing: PBM will not charge a higher AWP price based on repackaged products. This applies at retail, mail service and specialty.	Yes	10		
23	AWP used to calculate the claim (and quoted in pricing in this RFP) is the current, post-settlement AWP.	Yes	10		
24	U&C is defined as the retail price charged by a retail pharmacy for the particular NDC-11 dispensed on the date the drug was dispensed.	Yes	2		
25	Bidder agrees when HAC or the designated auditor or consultant is completing the annual pricing reconciliation, U&C claims will be identified and treated as U&C claims if the ingredient cost is equal to the U&C amount and the dispensing fee is \$0, OR ingredient cost plus dispensing fee equal the U&C amount provided in the claims file.	Yes	2		
	Ingredient Cost (including member share) is defined as the lesser of the following:				
26	AWP-Discount %	Yes	5		Capital Rx's Clearinghouse Model guarantees that each claim, without exclusions or exceptions, will be adjudicated according to the Clearinghouse logic outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> .
27	MAC Price	No	5		Please see comments for 26 above.
28	Usual & Customary Price	Yes	5		Please see comments for 26 above.
29	Discount will always be calculated using this formula (all claims, including ZBDs): (1- [Ingredient Cost]/[AWP Price]) * 100.	Yes	5		Not applicable to Capital Rx's Clearinghouse Model, as we do not provide category-level average annual discount guarantees.
30	Gross Cost is defined as [Ingredient Cost] + [Dispensing Fee] + [Sales Tax].	Yes	5		
31	Gross Cost for vaccines is defined as [Ingredient Cost] + [Dispensing Fee] + [Sales Tax] + [Vaccine Fee].	Yes	1		

32	Any OTC exclusions do NOT apply to insulin or diabetic test strips.	Yes	1		Capital Rx's Clearinghouse Model guarantees that each claim, without exclusions or exceptions, will be adjudicated according to the Clearinghouse logic outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> .
33	Biosimilars will be included in specialty brand discount guarantees and specialty rebate guarantees.	Yes	5	If not, quote separate pricing in appropriate tabs.	Capital Rx's Clearinghouse Model guarantees that each claim, without exclusions or exceptions, will be adjudicated according to the Clearinghouse logic outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> .
34	Any manufacturer coupons will be excluded from ingredient cost calculations.	Yes	5		
35	Bidder agrees that a specialty generic medication is defined as any NDC with a Medispan indication of Y and the GPI 14 is on the Bidder's or individual Participating Group's specialty drug list.	Yes	1		Capital Rx agrees to this definition for the purposes of determining cost share in accordance with the plan sponsor's plan design. However, it is important to note that brand/generic classification is not applicable to the Clearinghouse pricing logic.
36	Please confirm that brand and generic definitions are based on indicators found in Medi-Span.	Yes	5		Capital Rx confirms adherence to this definition for the purposes of determining cost share in accordance with the plan sponsor's plan design. However, it is important to note that brand/generic classification is not applicable to the Clearinghouse pricing logic.
37	If not, Please specify brand/generic indicator source:		1		Not applicable
Guarantees					
38	Bidder agrees to apply individual Participating Group-specific guarantees to all pricing components: discounts, rebates, admin fees, dispensing fees	No	20	If not in all situations, indicate size threshold or other exceptions in comments.	For our proposed admin fee structure, please refer to attachment <i>Capital Rx - Pricing Guarantees</i> .
40	Bidder agrees to reimburse individual Participating Group or HAC 100% of the shortfalls resulting from the guarantees on a dollar-for-dollar basis. Shortfalls may not be limited in any way.	Yes	20		
41	Bidder agrees that all guarantees will be evaluated separately and performance from one guarantee may not be used to offset other guarantee performance within the proposal.	Yes	10		
42	During the contract term, Bidder agrees that the guarantees will not change.	No	10		
43	If not confirmed, please specifically explain the ONLY conditions upon which guarantees may change during the contract term.		10	Higher points will be awarded to bidders with fewest exceptions.	Capital Rx's Clearinghouse Model eliminates average annual discount guarantees. We guarantee that the minimum PMPM rebate guarantee will not change for the life of the contract unless the plan sponsor implements a plan change that is projected to have a material impact on the rebates received. It is important to note that Capital Rx passes through 100% of rebates received to the plan sponsor.
At a minimum, the Bidder agrees that the following financial guarantees will be reconciled and paid on an annual basis 90 days after the end of each contract year. If the Bidder is willing to reconcile quarterly, please indicate in comments.					
44	Discounts	Yes	20	If not, indicate timing in the comments for partial points.	Capital Rx's Clearinghouse Model guarantees that ingredient cost for every claim will be determined in accordance with the Clearinghouse logic outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> . It is important to note that we disclose all pricing sources to plan sponsors as part of our PBM Services Agreement. We also agree to provide reconciliation reporting to plan sponsors upon request.
45	Dispensing Fees	Yes	20	If not, indicate timing in the comments for partial points.	Capital Rx's Clearinghouse Model guarantees that dispensing fees will apply by claim according to network dispensing fee schedule by pharmacy chain code as part of our PBM services agreement with the plan sponsor. We agree to provide reconciliation reporting to plan sponsors upon request.
46	Admin Fees	Yes	20	If not, indicate timing in the comments for partial points.	
Claims Adjudication					
47	Bidder agrees that individual Participating Group will pay Bidder for claims based on this equation: Ingredient cost + dispensing fee (when applicable) + sales tax (when applicable) - member copayment.	Yes	20		
Bidder agrees that Members will always pay based on the logic below:					
48	Retail - lowest of the U&C price, plan copayments/coinsurance, or discounted AWP (including MAC price)	Yes	10		Capital Rx guarantees that members will pay the lower of U&C price, copayment/coinsurance, or ingredient cost + dispensing fee as determined by the Clearinghouse Pricing logic outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> .
49	Bidder agrees that if the individual Participating Group plan design includes minimum copayments the member would pay the lower of U&C, Discounted Ingredient Price, MAC or copayment (including minimum copay in a coinsurance plan design)	Yes	10		Please refer to comments for 48 above.
50	Mail Order - lower of plan copayments/coinsurance or discounted AWP (including MAC price)	Yes	5		Please refer to comments for 48 above.
51	Bidder agrees there will be no price floors for amount paid on any claims.	Yes	5		

52	Bidder agrees to apply its most comprehensive, lowest-cost MAC list to individual Participating Group's prescription drug program throughout the term of the contract.	Yes	5		While Capital Rx does not utilize MAC lists, we maintain competitive negotiated unit price lists with our mail order and specialty partners. Additionally, we leverage CMS's publically published NADAC database in determination of ingredient cost at retail. All pricing sources at retail, mail order and specialty are fully-disclosed to the plan sponsor as part of our PBM Services Agreement.
53	Bidder agrees to provide HAC a copy of the current MAC file upon request.	Yes	1		Please see explanation for 52 above.
54	Bidder agrees to proactively notify individual Participating Group of a material MAC change equal to or greater than 10%.	No	1		Please see explanation for 52 above.
55	Bidder agrees there will not be a minimum number of manufacturers of the generic product in order for a DAW penalty to apply if the individual Participating Group has implemented a DAW policy.	Yes	1		
56	Bidder confirms its contracts with retail network pharmacies mandates that any pharmacy retail program charges (i.e. \$4 generic program for select medications) are submitted as the pharmacy's Usual and Customary charge to the Bidder.	Yes	1		

57	Bidder confirms its contract with retail network pharmacies mandates submission of all pharmacy related claims to the PBM if the member has pharmacy benefit coverage.	Yes	1		
Rebates				Certain questions below are not applicable to reinvested rebates, and bidders will not be penalized on the reinvested rebate portion of their quotes for indicating "Not Confirmed"	
58	Bidder agrees that Rebates mean formulary discounts and pharmaceutical administrative fee rebates, market share rebates and access rebates, inflation price protection and/or other arrangements in which Bidder receives value which are paid to or received by Bidder and/or its subsidiaries pursuant to the terms of a contract or other arrangement with a pharmaceutical company, and are directly or indirectly attributable to the utilization of certain pharmaceuticals by participants, or monies or value received by Bidder and/or its subsidiaries where individual Participating Group's prescription or participant information is used in obtaining in part, or in its entirety, as a result of Bidder administering individual Participating Group's pharmacy benefit. Bidder also agrees that rebates received on OTC or other excluded claims are shared in their entirety with individual Participating Groups	Yes	40		
59	Bidder agrees that discount guarantees quoted must not include the impact of rebates. Rebates may not be included in the discount calculation when reconciling against a discount guarantee. This includes specialty drug discounts. For example, the guaranteed specialty discount must be based on the ingredient cost before any rebates are netted out.	Yes	20		Not applicable. Capital Rx's Clearinghouse Model eliminates the use of average annual discount guarantees.
Rebates will be paid at the greater of the following:					
60	Minimum Dollar Guarantee	Yes	20		
61	100% of Rebate dollars received by PBM for the individual Participating Group's claims	Yes	20		
Bidder to indicate what sources of pharmaceutical manufacturer revenue Bidder receives and if Bidder is including that source in the 100% share passed to individual Participating Group. Y = Bidder receives revenue and is passing through to the individual Participating Group N= Bidder receives revenue but Bidder is NOT passing through to the individual Participating Group N/A = revenue is not received by the bidder					
62	Formulary Rebates	Yes	10		
63	Incentive Rebates	Yes	1		
64	Specialty Drug Rebates	Yes	10		
65	Data Fees	Yes	1		
66	Price protection rebates or guarantees	Yes	5		
67	Manufacturer Administration Fees	Yes	5		
68	Market Share Rebates	Yes	5		
69	Promotional Grants	Yes	1		
70	Compliance Funding-Traditional Drugs	Yes	1		
71	Compliance Funding-Specialty Drugs	Yes	1		
72	Funding for Therapeutic Switching	Yes	1		
73	Other Funding Sources	Yes	1		
74	Bidder agrees that contract rebate guarantees are not subject to change as a result of known brand patent expirations and introductions of their biosimilars or generics into the market.	Yes	20		
75	Bidder agrees it will not block any generic medications in favor of brand medications without providing proof to individual Participating Group it provides them the lowest net cost on that drug.	Yes	10		
76	Bidder agrees all brand drugs, including multi-source, single-source and biosimilars are included in the rebate pricing offer.	Yes	20		Capital Rx provides minimum rebate guarantees on a PMPM basis. We believe this provides a more transparent financial guarantee by eliminating the opportunity for reclassification and exclusions-driven optics.
77	Bidder agrees that Zero-Balance Due Claims (100% paid by member) will be included in the rebate guarantees. This includes claims that are 100% paid by the member solely due to the member being in the deductible period of a HDHP. ZBD claims are included in the guarantee prior to the application of plan participant cost sharing.	Yes	10	If not confirmed, bid valuation will be adjusted according to response below.	Capital Rx provides minimum rebate guarantees on a PMPM basis and thus exclusions do not apply. We believe this provides a more transparent financial guarantee by eliminating the opportunity for reclassification and exclusions-driven optics.

78	If not confirmed, what is the minimum % of gross cost that must be paid by the plan on an individual claim in order for it to be included in rebate guarantees?				
79	Bidder agrees that minimum rebate guarantees are paid regardless if that exceeds total rebate collected.	Yes	50		
80	Bidder agrees rebates will be paid on a quarterly basis 60 days after the close of each quarter.	No	10	If not, indicate timing in comments. More points will be awarded for shorter pay outs.	Capital Rx guarantees that rebates will be paid on a quarterly basis, 90 days after the close of each quarter.
81	Bidder agrees true up of any additional money owed to individual Plan Sponsor for 100% of the rebates received by the Bidder will be reconciled within 180 days of the end of the year.	Yes	5		
82	Bidder agrees the rebates quoted on each tab are consistent with the formulary quoted on the applicable tab.	Yes	1		
83	Bidder agree the rebates quoted on per claim guarantee, will be paid per claim, and will not be contingent on a days supply (i.e. if the days supply is less than 30, but the drug is a brand medication, the quoted rebate will be paid without any proration).	Yes	20		Not applicable. Capital Rx provides minimum rebate guarantees on a PMPM basis. We believe this provides a more transparent financial guarantee by eliminating the opportunity for reclassification and exclusions-driven optics.
84	Bidder agrees it can administer Point of Sale Rebates if requested by individual Plan Sponsor.	Yes	20		Capital Rx's POS rebate program is currently under development. We anticipate this program being fully-functional by Q2 2021.
85	Bidder agrees if rebates are no longer available in the market that the Bidder will work in good faith with the individual Participating Group and their Designee to establish a fair and equitable adjustment based on market conditions.	Yes	20		
Mail Order					
86	Bidder agrees a MAC list will be in place at mail order.		10		Capital Rx's Clearinghouse Model does not utilize MAC lists. Instead, our mail order adjudication logic incorporates our competitive negotiated unit cost schedule with our mail order partner, Walmart. Our mail order unit price schedule is disclosed to the plan sponsor as a component of our PBM Services Agreement. For more information on pricing at mail order, please refer to attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> .
87	Bidder agrees the MAC list used at mail order will be either equivalent in price or more favorable than the MAC list used at retail at a drug level.		10		Please refer to comments for 86 above.
88	Bidder agrees they will not pass any increases in mailing/postage fees to individual Participating Group during the contract term.	Yes	1		
89	Bidder agrees it will not use NDC's of licensed repackagers as a cost basis for calculating AWP discounts and charging for mail service pharmacy discounts.	Yes	1		
90	Bidder agrees that all proposed mail service pricing guarantees (administration fees, discounts, dispensing fees, rebates) would apply to all mail service prescriptions, regardless of days supply.	Yes	1		
HDHP					
91	Bidder agrees all Discount and Dispensing Fee guarantees provided will also apply to claims filled through the HDHP plan.	Yes	20		it is important to note that Capital Rx's Clearinghouse Model eliminates the use of average annual discounts.
92	If rebate guarantees vary for HDHPs and PPO plans, both sets of guarantees are provided in the pricing on the 3 Year Pricing Proposal tabs.	Yes	5		
93	Bidder agrees that any UM requirements still apply to drugs listed on the preventive drug list.	Yes	1		
Specialty Medications					
94	Bidder will be providing individual Participating Group specialty guarantees for each category on the pricing tab. Note that if the specialty guarantees are not provided, Bidder's specialty drugs will be valued at a 10% discount off of AWP.	Yes	5		
95	Bidder agrees the Specialty guarantees and rebates provided include Limited Distribution Drugs.	Yes	5		
	If answer is no, the bidder will input a separate discount guarantee for Limited Distribution Drugs on the pricing tab.				
96	Bidder agrees to provide a list of LDD drugs.	Yes	5		
97	If this offer is drug specific (with or without an overall guarantee) the Bidder agrees to provide the guarantee at an NDC level as an attachment.	Yes	5		
98	Bidder agrees that the Specialty guarantees provided will include new Specialty drugs introduced to the market.	Yes	5		
99	Bidder agrees that the Specialty drug discounts provided are discounts off of AWP with discounts calculated based on Ingredient Cost before subtraction of member paid amounts, manufacturer coupons, rebate amounts, or any other offset amounts.	Yes	20		Capital Rx agrees to this term for those drugs without a negotiated unit price, which default to the lower of U&C and AWP - 10%.
100	The Bidder agrees the individual Participating Group or it's Participating Groups reserve the right to purchase specialty products from other sources with no impact to non-specialty guarantees. Please provide any fees for this scenario on the pricing tab.	Yes	5		Not applicable. Capital Rx's Clearinghouse Model does not employ category-level average annual guarantees. Prior to implementation of such a program, Capital Rx will perform a financial analysis to assess the potential impact to the provided minimum PMPM rebate guarantee. It is important to note that Capital Rx passes through 100% of rebates received to the plan sponsor, and therefore our minimum rebate guarantee will only be adjusted if a material decrease in rebates received is expected. As always, our PMPM guarantee represents the floor, and all over-performance against this minimum guarantee is fully-realized by the plan sponsor.
OTHER					
1	Bidder agrees that rebates received on OTC or other excluded claims are shared in their entirety with individual Participating Group.	Yes	20		
Total Possible Points			820		

Other Credits and Fees

Maximum Point Value is 100 Points. Points will be awarded based on estimated total credits less estimated total fees, adjusted down for any caveats around credit utilization, at the discretion of the Proposal Team.

Implementation Credits	Amount	Basis
What implementation credit is being offered?	[REDACTED]	
Bidder agrees individual Participating Group can use any remaining implementation credits during the life of the contract.	No	
How can the implementation credit be used?	The implementation credit can be used to offset any Capital Rx services related to implementation, such as member welcome packets. ID card production, provider communications, etc.	
When will it be paid and what type of documentation is required?	The implementation credit will be applied to desired Capital Rx services as a credit toward the applicable monthly invoice.	

General Credits or "Ongoing Management Credits"		
What general or ongoing management credit is being offered?	[REDACTED]	
Is the credit provided each year or one time credit for the life of the contract?	Capital Rx is offering a \$[REDACTED] ongoing credit for each year of the contract.	
Bidder agrees the credit can be used for services including but not limited to, offsetting clinical program fees, ad hoc reporting, coding, audits and consulting fees. If there are any caveats, please explain.	Ongoing Management Credits can be used to offset costs associated with all services listed, with the exception of audits and consulting fees.	
Bidder agrees the credit can be used to pay for outside third-party care management programs or point solutions. If there are any caveats, please explain.	Confirmed	
Will outstanding balance at the end of the year be an offset on the Participating Group's invoice?	No	

Pharmacy Network Access	Yes/No	Percentage & Approximate amount PMPY
Bidder agrees to pass through a percentage of the pharmacy network access they receive to Client	Yes	100.00%

Other Items with Separate Fees	Fee
D Cards	
Paper Claims	[REDACTED]
Manual Claims	[REDACTED]
Manual Eligibility	
E-prescribing	
Member Welcome Packets	
Member & Provider Communications	
Other	

Non-Financial Performance Guarantees	
What is the total annual amount at risk for a Participating Group for the annual Performance Guarantees listed in Attachment A?	Please see comment in response box
What is the total one-time amount at risk for a Participating Group for the Implementation Performance Guarantees listed in Attachment A?	Please see comment in response box

Total Possible Points	100
------------------------------	------------

Alignment Credit

The Health Action Council and CCOG are requesting PBM bidders offer an alignment credit, preferably as a PMPM or PEPM, to Participating Groups who select an aligned medical carrier, if applicable. (Examples: OptumRx and UHC, ESI and Cigna, CVS and Aetna, Anthem and Ingenio). To show the value of integration or alignment, please indicate the credit you will offer if a Participating Group selects the medical carrier you are aligned with. Please note: The Proposal Team is not requesting integrated PBM/medical quotes or credits. The quoted credits would apply assumed a carved our pharmacy benefit, but selection of your aligned medical carrier.

As explained in Attachment F, more points will be awarded to bidders who are willing to provide a medical/pharmacy alignment credit. More points will be awarded for higher credits and fewer caveats. Bidders who are independent from any medical carrier can explain the advantages of their position in the area provided and will not be penalized for not providing a credit on this tab.

POINT VALUE: Maximum point value is 150 points.

Alignment Credit	Amount	Basis
What Alignment Credit is being offered?		
What medical vendor(s) must a Participating Group select to receive the credit?		
How can the alignment credit be used?	N/A	

Synchronization Credit or Savings Guarantee

The Health Action Council and CCOG are requesting PBM bidders offer a synchronization credit or savings guarantee to Participating Groups who select an aligned medical carrier, if applicable. (Examples: OptumRx and UHC, ESI and Cigna, CVS and Aetna, Anthem and Ingenio). To show the value of integration or alignment, please indicate a credit or savings guarantee for the Client, including how it is calculated, if a Participating Group selects the medical carrier you are aligned with. Please note: The Proposal Team is not requesting integrated PBM/medical quotes or credits. The quoted credits would apply assumed a carved our pharmacy benefit, but selection of your aligned medical carrier.

As explained in Attachment F, more points will be awarded to bidders who are willing to provide a medical/pharmacy synchronization credit or savings guarantee. More points will be awarded for higher credits or savings guarantee, with a meaningful formula, and fewer caveats. Bidders who are independent from any medical carrier can explain the advantages of their position in the area provided and will not be penalized for not providing a credit on this tab.

POINT VALUE: Maximum point value is 50 points.

Synchronization Credit	Amount	Basis
What Synchronization Credit is being offered?		
What medical vendor(s) must a Participating Group select to receive the credit?		
How can the synchronization credit be used?	N/A	

Total Possible Points	200
------------------------------	------------

Clinical Program Fees

Maximum point value is 100 points.

Indicate fee amount and basis (Example: \$0.10 PMPM, \$10 per intervention, etc.) and a brief description of the program, including your product name if applicable.

Program	Fee	Description	ROI Guarantees Offered?
Concurrent DUR (Drug Utilization Review)	Included in base admin fee	In order to detect and address quality and safety issues, we employ our DUR programs, which consist of more than 4,000 clinical edits and drug-specific interventions targeting multiple utilization cases such as duplicate therapies, drug-drug interactions, inappropriate drug dosing or duration of therapy, drug-allergy contraindications, age or gender-related edits, and overutilization and underutilization edits. Through DUR, we help clients identify outlier members and prescribers who may warrant a direct intervention, which may include personalized letters, educational materials, prescriber reports, and more.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Retrospective DUR (Drug Utilization Review)	Included in base admin fee	Please see above for cDUR	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Prior Authorization	Administrative PA Included in base admin fee Pharmacist-mediated PA [REDACTED] Incidence	Capital Rx's standard clinical prior authorization programs ensure appropriate and cost-effective utilization for target traditional and specialty disease states.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Quantity Limits	Included in base admin fee	Capital Rx's standard quantity limit programs ensure appropriate and cost-effective utilization for target traditional and specialty disease states.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Step Therapy	Included in base admin fee	Capital Rx's standard step therapy programs ensure appropriate and cost-effective utilization for target traditional and specialty disease states.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Specialty Enhanced UM	[REDACTED]	Capital Rx's High Touch Prior Authorization Program reimagines the role of administrator in the authorization workflow. By incorporating near real-time, proactive intervention, we take the burden off the member and physician to submit complete documentation required to support a thorough clinical review. Through this high-touch approach, Capital Rx provides superior member service as well as lower administrative burden and faster turnaround times. For additional information, please see Capital Rx_High Touch PA Overview	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Pharmacogenomics	Quoted upon request, varies by utilization	Capital Rx offers pharmacogenomic assays, including follow-up with member and provider education to prevent current or future inappropriate and/or unsafe drug utilization identified based on member pharmacogenomic profiles.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Specialty Copay Assistance True Accumulator Program	N/A	N/A	N/A
Specialty Copay Assistance Variable Copay Program	[REDACTED]	Our ValueMax Program connects members with manufacturer copay assistance programs for ~60 of the most commonly prescribed specialty medications. Proprietary algorithms optimize value of assistance programs to prevent copay disruption and maximize savings, including withholding from out-of-pocket (OOP) accumulators. Similarly, our Tier 5 Program connects members with manufacturer copay assistance programs for ~75 medications used to treat ultra-orphan conditions. Proprietary algorithms optimize value of assistance programs to prevent copay disruption and maximize savings, including withholding from out-of-pocket (OOP) accumulators.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Specialty Guideline Management	Included in base admin fee		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Appeals - Level 1	[REDACTED]		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Appeals - Level 2 or IRO	[REDACTED]		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Standard Opioid Management	Included in base admin fee		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Enhanced Opioid Management 1	[REDACTED]	Management and utilization strategies to reduce opioid overutilization risk. Services include New Start programs, drug disposal education, and 24/7 helpline support.	N/A
Enhanced Opioid Management 2	N/A	N/A	N/A
Diabetes Management Program 1	[REDACTED]	Our Live Vibrantly Diabetes case managers work with providers, pharmacies, and members to educate, prevent gaps in care, and improve adherence.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Diabetes Management Program 2	N/A	N/A	N/A
Fraud, Waste, and Abuse	Included in base admin fee	Capital Rx uses advanced real-time audit (RTA) system to perform statistical analysis on 100% of claims in real time at no additional cost to our clients. Our standard FWA programs also conduct regular desk and on-site audits that cover at least 5% of our retail network annually.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Compound Management	Included in base admin fee		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
CDI/HDP Fee	Included in base admin fee		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Rare Conditions Management Program	Quoted upon request, varies by disease state		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Gaps in Care Program Utilizing Rx Data Only	[REDACTED]	Our interventional disease management programs eliminates gaps in care and improves adherence by identifying and engaging with at risk members and their providers. Members receive educational tools and personalized care from a team of nurses, pharmacists, and other clinical professionals. Provider intervention is carried out via provider outreach as well as web-based information available regarding drugs that can improve care while minimizing costs. Video-taped materials are available on our member and provider portal and a 1-800 help line is available 24 hours/7 days a week for assistance.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Gaps in Care Program Utilizing Medical & Rx Data	[REDACTED]	Please see above	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Pharmacy Advisor	Included in base admin fee		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Clinical Alerts	Included in base admin fee		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Dermatology UM Bundle 1	Included in base admin fee		We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Dermatology UM Bundle 2	N/A		N/A
Enhanced FWA - COPS	[REDACTED]	In addition, Capital Rx offers the option to employ Cluster Optics Process (COPS), a highly sophisticated machine learning system leveraging principles of criminology to detect fraud in health care claims. After discovery of specific problems using the COPS algorithms, auditors recover from mis-paid claims through a comprehensive desk audit process. In most cases, the funds are recovered through a reversal of payments to the pharmacy. The cost to implement COPS is zero to the Sponsor, but COPS retains 20% of savings recovered. In some cases (less than 5% of cases audited), further investigative work is required. Trained investigators can pursue on-site investigations to prepare for litigation and restitution.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Human Capital Reporting	Included in base admin fee	Capital Rx standardly offers our Human Capital Reporting platform services at \$2.00 PMPM. However, we would like to offer a credit in full for this service to all HAC Participating Groups services by Capital Rx, as a commitment to our strategic partnership. Through our innovative Human Capital Reporting platform, we make it clear to Plan Sponsors that healthcare is an investment, not a cost. By combining pharmacy, medical, and payroll data into a unified reporting suite, Sponsors are provided with an unmatched, global view into the performance of their benefits. This level of insight gives Sponsors the power to track outcomes, measure the impact of plan design decisions across benefit liabilities (or budgets) and, most importantly, to constantly assess their most important asset- human capital.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Therapeutic Interchange Program	[REDACTED]	Capital Rx offers two levels of Therapeutic Interchange Programs Level One: Targets utilization of "low clinical value" or "low cost-effectiveness" for therapeutic substitution. Common targets include multi-source brand and "me too" brand utilization; common interventions include print, digital and telephonic member and physician engagement. Level Two: Target non-preferred brand utilization to maximize formulary compliance and drive cost savings	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Capital Rx Cares	Included in base admin fee	Members with specialty conditions are automatically enrolled in the Capital Rx Cares program. The program is a one-on-one clinical coaching program that provides a dedicated registered nurse, educated in the field of motivational interviewing and behavioral change psychology. This unique approach drives significantly higher medication adherence rates, which translates to more effective clinical care and improved health outcomes, productivity and quality of life for members.	We would be happy to discuss ROI guarantees with HAC based on your strategic priorities.
Other			
Other			
Other			
Other			
Other			
Other			
Total Possible Points		100	

Pricing Alt1: NADAC or Acquisition Cost Based Model

The Health Action Council is considering adding an alternative pricing model. Please describe your acquisition cost based model below by answers the questions and adding a further description and pricing as needed.

POINT VALUE: This model is optional for bidders. Bidders offering this model will be compared and scored relative to each other based on the below.

Questions	Complete below
Is the only source of income the dispensing fees?	Capital Rx's sole source of revenue is our admin fee. We do not retain any portion of the dispensing fees charged by our network pharmacy partners.
Is there an admin fee in addition to the dispensing fee?	Confirmed. Capital Rx's sole source of revenue is its admin fee. For the admin fee structure proposed, please refer to attachment <i>Capital Rx - Pricing Guarantees</i> .
How are specialty drugs priced?	Without exception or exclusion, all drugs are priced according to the Clearinghouse Model pricing terms outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> .
What acquisition cost metric is utilized? (NADAC, etc.)	Our Clearinghouse Model pricing terms incorporate NADAC at retail and negotiated unit price lists at mail and specialty. All pricing lists are fully-disclosed to the plan sponsor as part of our PBM Services Agreement.
Are you able to offer any pricing guarantees?	Yes, Capital Rx guarantees that every claim, without exception or exclusion, will be priced according to the Clearinghouse Model pricing terms outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i> . Upon request, Capital Rx will provide reconciliation reporting supporting our adherence to these pricing terms. Additionally, Capital Rx offers minimum rebate guarantees on a PMPM basis. We believe this provides a more transparent financial guarantee by eliminating the opportunity for reclassification and exclusions-driven optics.
How many commercial clients (non-health plan) do you have using this model?	As of 1/1/2021, all Capital Rx clients will utilize this model.
How many lives (non-health plan) do you have using this model?	450,000 lives
Please provide a complete description of your pricing proposal:	<p>Ingredient Cost Capital Rx's Clearinghouse Model establishes drug price by NDC-11 for all claims, without exception or exclusion and irrespective of classification, according to the pricing terms outlined in attachment <i>Capital Rx - Clearinghouse Adjudication Logic</i>. In addition, we have provided a claim-level repricing example of this logic in attachment <i>Capital Rx - Clearinghouse Pricing Explainer</i>. Please note that this attachment also includes illustrative "crosswalked" AWP discounts to facilitate evaluation of our model.</p> <p>Dispensing Fees Dispensing fees (where applicable) are determined according to our network dispensing fee schedule by pharmacy chain code, which is fully-disclosed to the plan sponsor as part of our PBM Services Agreement.</p> <p>Rebates Capital Rx provides minimum rebate guarantees on a PMPM basis. We believe this provides a more transparent financial guarantee by eliminating the opportunity for reclassification and exclusions-driven optics. It is important to note that Capital Rx passed through 100% of all rebates earned to the plan sponsor, and thus our PMPM rebate guarantee represent the guaranteed "floor". All overperformance against our minimum PMPM guarantees is realized in full by the plan sponsor. Capital Rx has provided our minimum PMPM rebate guarantees within the [Rebates] tab of attachment <i>Capital Rx - Pricing Guarantees</i>.</p> <p>Admin Fees Capital Rx's sole source of revenue is our admin fee. We do not participate in spread pricing practices, nor do we retain any manufacturer-derived revenue earned on behalf of the plan sponsor. Additionally, we do not own our mail order or specialty pharmacy facilities and therefore do not earn revenue on fulfillment. These practices allow Capital Rx to remain a truly unconflicted partner to our plan sponsors. Capital Rx has provided our admin fee structure within the [Admin Fee] tab of attachment <i>Capital Rx - Pricing Guarantees</i>.</p>

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

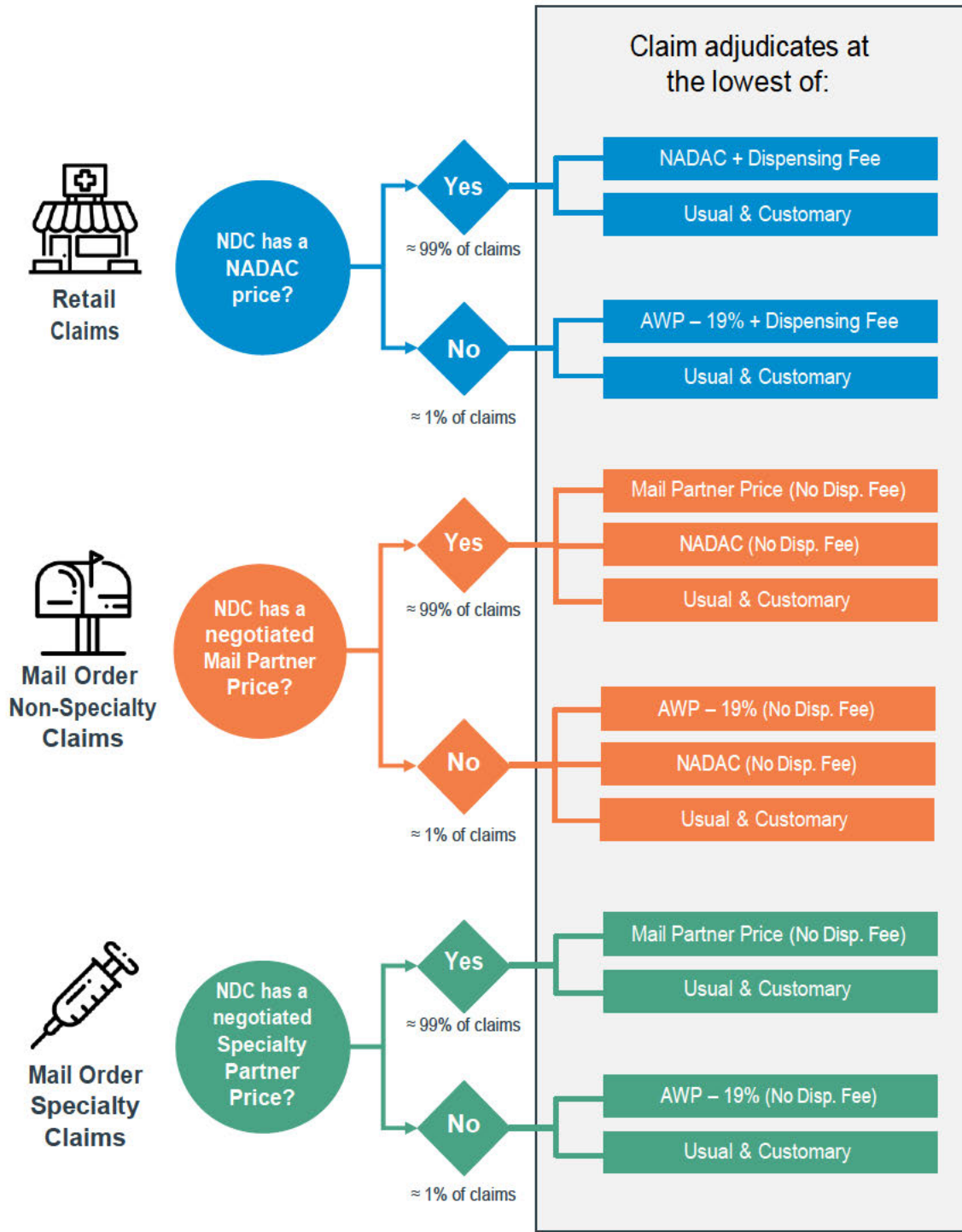
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





Notes:

- NADAC is available for download from the CMS website at no charge at <https://bit.ly/2VFeQ1B>.
- Mail/Specialty Partner Prices are documented in Capital Rx's Clearinghouse Price Lists, which are fully disclosed to the client at any time and auditable by a third party.
- Dispensing Fees for retail claims vary by pharmacy chain code. These fees are also disclosed to the client and auditable.
- In the rare event that the retail pharmacy's Submitted Cost is lower than their Usual & Customary price, Submitted Cost will be used.