Introduction

Complete this *Information Security Questionnaire* with information about the proposed implementation of a new application (or new version of an existing application) at Town of Brookline ("BROOKLINE").

- If there is a Brookline application owner, he or she must review the completed form before submitting it to [WHO WITHIN BROOKLINE WILL BE RESPONSIBLE FOR VERIFYING SECURITY MATTERS RELATING TO NEW SOFTWARE AND TECHNOLOGIES???].
- Please complete **all tabs** in this workbook.
- Incomplete questionnaires will delay the Information Security review.

Application Information

Complete the following information about the application, vendor, Brookline application owner, and affected locations.

Application Information			
Application name:		Version #:	
List alternate names for this application:			
Is this an existing application, already in production?		Yes	No
Vendor Information			
Company name:			
Contact information	**Name:**		
	Phone:		
	Email:		

BROOKLINE'S Application Owner Information		
Business unit:		
Service line lead:		
Application owner	**Name:**	
	Phone:	
	Email:	
Completed by	**Name:**	
	Phone:	

	Email:
Date submitted:	

Application Usage Information
How many people are responsible for providing support for this product or service?
What is the general function or purpose of this application?

Locations affected (*select all that apply*)					
How many users will use this application?	Fewer than 10	Fewer than 100	Fewer than 500	Fewer than 1000	Over 1000
Town of Brookline					
Police Department					
Fire Department					
Public Works Department					
School Department					
Other:					

Personal Identification Information (PII) Identifiers	
Does the use case scenario for this application store, process, or transmit any of the following PII identifiers in this implementation?	
Bank / Credit Union account numbers	Home phone number
Biometrics (finger / face print)	IP Address
Birth certificate	Mother's maiden name
Citizenship	Name
Credit card expiration date	Other identity verification or authentication data
Credit card number	Passport number
Criminal records	Personal phone number
Date of birth	Personal e-mail address

Date of death	Photo
Death certificate number	Race or Ethnicity
Dependent information	Salary and bonus
Disability information	Social Security number
Driver's license number	Vehicle registration plate number
Financial data	Work eligibility
Home address	
None of the above or not applicable	

	User Accounts & Password Controls	
1	*Who is responsible for provisioning users for this application?*	Automated provisioning/de-provisioning Account Control Team / Help Desk BROOKLINE Application Owner Vendor
2	*How many users will use this application?*	Fewer than 10 Fewer than 100 Fewer than 500 Fewer than 1000 1000+
3	*How many locations will use this application?*	Town wide Multiple sites with independent controls One Department or site only
4	*Will the installation of this application authenticate users against Brookline's Active Directory (**AD**) infrastructure?*	Yes No, it is available, but not enabled No, it is not available from the vendor
5	Are there any shared or Generic User Accounts used? *(An account used by multiple users for the purpose of logging into an application)*	Yes Yes, for vendor support only No
	a) Can these accounts be disabled, to allow only individual named user accounts	Yes No
	b) Who is this account used by and for what purpose?	
6	*(An account used for predefined, scheduled tasks without user interaction. These do not include accounts used for*	Yes No
7	*Is this application called solely from another application?*	Yes, this application is only accessed via a service account from the parent application. 'Yes, this application is only accessed with the user's cached credentials from the parent application. Yes, the user must authenticate manually before accessing this application. No, this application is independent and the user must authenticate manually before accessing this application
8	*Upon termination or transfer, will the user's access be **disabled** or **deleted** within the application?*	Users are disabled, marked as inactive, etc. within the application. Users are deleted from the application No action is taken within the application.
9	*Is there a documented procedure for terminating users from the application?*	Yes In progress No
10	*What is the timeframe for terminating a user from this application?*	< 2 hours < 1 day < 2 days No restriction

	Application Controls	
A	Will this application be void of PII data?	Yes No
1	Are users assigned **ROLES** (**Role Based Access)** within the application?	Yes No, role based access controls are not available from the vendor No, role based access controls are disabled.
	a) Roles are established such that: **(select all that apply)**	Some users only have **View only** access Some users have **Create, Modify, Delete** access Only some users are **Application Administrators** **All** users have access to **all** data Users are grouped by title, dept, job desc, etc. Users are grouped per department or site Users are grouped per facility or location Users can access only select patients Restrictions are imposed on IT staff Restrictions are imposed on vendor staff Other (Please list on the Notes Tab)
2	What is the Application Inactivity Timeout value?	30 minutes or less over 30 minutes currently disabled Not available from the vendor
3	Does the application restrict access to printing?	Yes This is a web application, printing is a function of the browser No
4	Is the application version under an active support contract?	Yes No
5	Does the application owner review application security patches and apply where needed within 60 days of release?	Yes No, but within 6 months No
6	What is the back-end database type?	None, no database used Oracle MS SQL mysql Other: *{please explain on **Notes** tab}*
7	Does this solution require anti-virus scanning exceptions on the server or endpoint device (*such as directory exclusions*)? *(Please explain in the **Notes** tab or provide vendor documentation)*	Yes No
8	(*A medical device is an instrument, apparatus, implant, in vitro reagent, or similar or related article that is used to diagnose, prevent, or treat disease or other conditions, and does not achieve its purposes through chemical action within*	Yes No
9	Will users be provided training in the use of this application?	Yes No
10	Is the necessity for protecting PHI reinforced during training of this application?	Yes No
11	Will users be provided training regarding the application's security features?	Yes No

	Audit Logging & Monitoring	
1	Are log-on activities recorded in the audit trail?	Yes Not Applicable Not Logged
2	Are log-off activities recorded in the audit trail?	Yes Not Applicable Not Logged
3	Are failed log-in attempts recorded in the audit trail?	Yes Not Applicable Not Logged
4	Are view access activities recorded in the audit trail?	Yes Not Applicable Not Logged
5	Are create/modify/delete activities recorded in the audit trail?	Yes Not Applicable Not Logged
6	Is printing of PII or screen printing of PII, recorded in the audit trail?	Printing is not available Yes Application is browser based No, printing is not logged
7	Are audit logs searchable & extractible per user?	Yes Yes, By request of vendor only No

8	Are audit logs searchable and extractible per patient or object?	Yes Yes, But by request of vendor only No
9	Are the application logs retained for six(6) or more years?	Yes No
10	Are the security & audit logs reviewed?	Monthly or less Log Monitoring application (SIEM) is used Quarterly Only when requested Never
11	Who reviews the security & audit Logs?	

	Encryption & Remote Access Security
1	Is Database Encryption available from the vendor?
	a) Can and will database encryption be enabled?
2	Will the PII data reside on an encrypted storage volume?
3	Does the application support full hard disk encryption of the client pc or laptop?
4	Are there constraints in place to ensure data integrity of the database? {*e.g. entity integrity, referential integrity, domain integrity, etc.*}
5	Are there integrity checks in place to ensure file based data integrity? {*e.g. checksum verification, CRC, parity, mirroring, etc.*}
6	Does the application support USB encryption?
7	Does the use case scenario limit application users to inside the US only?

8	Does the vendor's staff that will have access to BROOKLINE data or the infrastructure that supports it, reside solely in the United States?	
	a) From what country or countries will the staff connect from?	
9	Does this application use a Publicly Accessible web site?	
10	Will confidential data be saved to the user's local pc or laptop?	
	(select all that apply)	
11	Does the use case scenario include the use of mobile phones or tablets?	
	a) Is the application accessed via a browser or a mobile app? (select all that apply)	
	b) Will confidential data be sent or saved to the users' mobile phone or tablet?	
	c) What security and privacy controls are required of the users' devices by the application? *(select all that apply)*	
12	Is PII data transferred to or received from other systems?	

	ASP Specific IT Security Controls	
	Vendor Selection Controls	
1	Is data stored outside of BROOKLINE's datacenters? [DOES BROOKLINE HAVE A DATA CENTER???] *(if **No**, skip this section.* *If **Yes**, answer the following questions with regard to the hosting facility)*	
	a) Are the servers located in a datacenter?	
	b) Are the servers located at a BROOKLINE property?	
2	Provide the entity name and address where the servers and computer equipment are located.	Þ Þ Þ
3	Does your organization outsource any IT functions?	
4	Will BROOKLINE's data be stored off-shore?	
5	Are Backups encrypted?	
6	Have any of the following certifications or reviews of the data center site(s) been performed?	
	a. Can and will the cover sheet from the certification company be attached to this review?	
7	Has your organization developed and is it maintaining an information risk management program to manage information security risks to an acceptable level?	
8	Does your organization perform risk assessments to identify and quantify risks; and communicate the results to the affected parties and to management?	
	Vendor Staff & Third Party Controls	
9	Data Center(s) are staffed and monitored 24x7x365?	
10	Approximately, how many support staff will have access to the application, database, or infrastructure containing BROOKLINE's data?	
11	What application or service does your organization use to authenticate IT staff user accounts?	
12	Does your organization's staff utilize unique named accounts?	
13	How often are passwords changed for your staff with access to BROOKLINE's data?	
14	Does your organization have a procedure in place for the provisioning, monitoring and management of privileged accounts?	
15	Are entitlement reviews performed for access to information systems (e.g. applications, systems and devices)?	
16	Does the web application support Security Assertion Markup Language (SAML) for exchanging authentication and authorization data?	
17	Do the hosting facility's staff members or contractors have remote access capabilities to their datacenter?	
	a) Is multi-factor authentication (for example, token, smart card, or One-Time-Password) required or supported?	
	b) Are their remote sessions terminated if idle for **15 minutes** or less?	
	Vendor Infrastructure Controls **Interfaces and Networking**	
18	Network hardware & software are under support and monitored?	
19	Vendor maintains appropriate anti-virus and patch levels?	
20	Do other parties have access to BROOKLINE data?	
21	Are logins to infrastructure devices logged and audited?	
22	Are default passwords changed before being put into production	
	Disposal of ePHI and Personally Identifiable Information	
23	Does BROOKLINE own the data stored at this facility?	
24	Is there an established process for wiping or destroying data at termination?	
25	How will BROOKLINE data be removed from the data stores at the end of the contract?	
26	How will BROOKLINE data residing on backup media be handled at the end of the contract?	
	Vendor Infrastructure Controls **Interfaces and Networking**	
27	Are client connections restricted to a dedicated circuit, VPN, or https?	
28	Are there controls in place to prevent unapproved copying of BROOKLINE data?	
	Administrative Controls and Logging	
29	Have manufacturer's default passwords been changed? This includes network devices, databases, applications, etc.	
30	Is there an enterprise Patch Management System in place for servers and endpoint devices (e.g. workstations, laptops, and smartphones)?	
31	Are application patches applied so version numbers are within two (2) releases of current?	
32	Are critical and important operating system (OS) patches applied so version numbers are within sixty (60) days of release date?	
33	Are third party applications updated so version numbers are within two (2) releases of current?	
34	Are the Service Provider's staff activities logged when accessing or querying BROOKLINE data?	
35	Are vendor staff activities logged and monitored for successful logins?	
36	Are vendor staff activities logged and monitored for failed login attempts?	
37	What are the retention periods of the vendor's activity logs?	
38	Does your organization have controls in place to ensure logging systems and log information are protected from tampering and unauthorized access?	
	Network and Endpoint Security Controls	
39	Will multiple copies of BROOKLINE data or databases be maintained? *(excluding backup media)*	
40	Have access roles been provisioned with administrative rights instead of assigning administrative rights to individual users on the network devices?	
41	How often are administrative passwords changed on the network devices?	
42	Was an external vulnerability scan performed within the last 2 years?	
43	Was an internal vulnerability scan performed within the last 2 years?	
	Was remediation completed?	

44	Are all network hardware devices (such as firewalls, routers and switches) under maintenance, support, and within two (2) versions of the current manufacturer's release?	
45	Is there an intrusion prevention system (IPS) in place?	
46	Is there an intrusion detection system (IDS) in place?	
47	Is outbound internet traffic monitored for data loss prevention?	
48	Are there anti-virus, anti-spam, and anti-malware systems in place?	
49	Are there a Security Incident and Event Monitoring (SIEM) systems in place?	
	Vendor Policies	
50	Does your organization have policies for the following topics?	
	a. Computer Use Policy	
	This policy establishes rules and guidelines for the use of all computing devices, including desktops, laptops, smartphones, handheld devices and any other network enabled devices.	
	b. Password Policy	
	This policy establishes a list of requirements for the development and use of passwords that control access to computer systems and networks to protect data.	
	c. Mobile Device Policy	
	This policy establishes guidelines for using cellular/Smartphone devices (for example, BlackBerry, iPhone, iPad, iPod Touch, Air Cards, Android based devices, and cell phones).	
	d. Incident Response Policy	
	This policy establishes procedures for defining, documenting, and responding to information security incidents.	
	e. Sanction Policy	
	This policy establishes corrective actions for employees not following approved corporate policies.	
	f. Change Management Policy	
	This policy establishes a consistent and systematic approach is used for modifying the IT resources of the approved vendor. The intent is to streamline processes while mitigating security vulnerabilities and potential loss due to system outages. Modifications to IT resources require serious forethought, testing, appropriate communication and post-change evaluation.	
	g. Business Continuity and Disaster Recovery Policy	
	This policy establishes strategies for recovering key systems, business processes and data in the event of an emergency situation or other significant occurrence which disrupts critical business operations. The goal is to ensure the vendor has key data and processes identified prior to an event occurrence to minimize potential impact.	
	h. Email Usage Policy	
	The policy must address information security related to the exchange of data between users via email and address safeguards against unauthorized access, monitoring to help prevent security breaches, and maintain confidentiality of data. The policy must define the authorized and appropriate use of the vendor's email system.	
	i. Encryption Policy	
	This policy establishes encryption safeguards to ensure data authenticity and integrity where reasonable and appropriate, and in accordance with applicable laws and regulations.	
51	Are written security policies provided to staff?	
52	Are the information security policies reviewed at least annually; or if significant changes occur in the organizational environment, business circumstances, legal conditions, or technical environment to ensure its continuing adequacy and effectiveness?	
53	Does your organization monitor and review the services, reports and records provided by third parties and are audits carried out regularly to govern and maintain compliance with the service delivery agreements?	

		Weight	high score	high weight	criteria score	radio value	score	Weighted Score { C*H }	
	BCP / DR Controls								
	Business Requirements								
1	If this application were unavailable, what would be the public safety/service or business/financial impact?	3	5	15	5 3 1	**3**	1	**3**	**Public safety/service** Severely impacted Moderately impacted Little to no impact
		3	5	15	5 3 1	**3**	1	**3**	**Business/Financial** Severely impacted Moderately impacted Little to no impact
2	What does this application most closely support? Select the most appropriate category. Select <u>one (1)</u> choice only	0	3	0	3 3 2 2 2 2 1 1 1 1	**3**	2	0	**A**. Underlying backbone or core infrastructure layer services. **B**. Core public safety. **C**. Electronic enterprise communication tool critical for public safety **D**. Ancillary public services. **E**. Critical Printing services **F**. Critical Business or Financial application (non-public service) **G**. Non-Critical Business application for standalone departments **H**. Non-Critical Infrastructure Utility **I**. Used for Historical Data only **J**. Other minor discretionary service or business process.
3	How long could the business operate if the application is unavailable due to a hardware or software issue?	0	5	0	5 3 1 1	**4**	1	0	**A**. < 1 hour **B**. > 1 hour to < 12 hours **C**. > 12 hours to < 24 hours **D**. > 24 hours
4	Is data stored outside of BROOKLINE's datacenters?	3	1	3	1 0	**1**	1	**3**	Yes No
		9	**19**	**33**	**27.27%**			**9**	
	General BCP / DR Strategy								**Date Approved/Embedded Approval**
	The Service Provider should complete the following section.								
	General BCP / DR Strategy								
5	Do you have documented plans for Business Continuity and IT Disaster Recovery (DR)?	5	3	15	1 3	1	1	**5**	Yes No
6	Do your plans include the following information?								
	a) Activation plan for your Alternate Backup Site	0	3	0	1 3	1	1	**0**	Yes No
	b) Crisis Communication Plan	0	3	0	1 3	**1**	1	**0**	Yes No
	c) Resource Mobilization Plan for recovery activities	0	3	0	1 3	**1**	1	**0**	Yes No
	d) Step-by-Step Failover Procedures (detailed tasks, roles/responsibilities, resources and estimated task timeframe)	0	3	0	1 3	**1**	1	**0**	Yes No
	e) Emergency Mode Operations Plan	0	3	0	1 3	**1**	1	**0**	Yes No
	f) Data Backup Plan	0	3	0	1 3	**1**	1	**0**	Yes No
7	Is your Business Continuity and IT Disaster Recovery program regulated and/or audited by a Regulatory Agency?	1	2	2	1	**2**	2	**2**	Yes

	regulated and/or audited by a Regulatory Agency?	1	2	2	2	2	2	2	No
8	Do you have a dedicated team of professionals focused on the continuity and recovery of your service capabilities?	3	3	9	1 3	**1**	1	**3**	Yes No
	If yes, list the service provider's name on the notes page.								
9	Have you ever activated your DR Plan? *If yes, explain on the notes page.*	0	3	0	1 3	**2**	3	**0**	Yes No
10	Does your recovery plan require services of other third party service providers? *If yes, explain on the notes page.*	3	3	9	3 0	**1**	3	**9**	Yes No
11	At what point would you formally declare a disaster during a significant operational disruptive event?	5	5	25	1 2 3 5	**3**	3	**15**	15-30 minutes < 1 hour < 4 hour Other, explain on notes page
12	Who has the decision making authority to declare a disaster?	5	3	15	1 3 2	**3**	2	**10**	BROOKLINE Service Provider Both
13	Specify the Recovery Time Objective (RTO) you are contractually capable of providing to BROOKLINE at your alternate data center.	3	5	15	1 2 3 4 5	**3**	3	**9**	15-30 minutes < 1 hour < 4 hour < 24 hours Other, explain on notes page
14	Specify (in hours) what Recovery Point Objective (RPO) you are contractually capable of delivering to BROOKLINE.	3	5	15	1 1 1 3 5	**3**	1	**3**	Zero Data Loss < 1 hour < 4 hour < 24 hours Other, explain on notes page
15	Can you meet the Data Backup and Data Retention requirements specified in question **3**? *Please explain your answer on the notes page.*	3	5	15	1 5	**1**	1	**3**	Yes No
16	Are backups encrypted?	3	5	15	1 1 5	**1**	1	**3**	Hardware Encryption Software Encryption Not Encrypted
17	If data were lost, are you able to recreate it? *(If yes, please explain on the Notes page: How this would be done and how far back would you be able to do this?)*	3	5	15	1 5	**1**	1	**3**	Yes No
18	Can you provide BROOKLINE with a physical tour of your Primary or Alternate Data Center if requested? *If no, explain on the notes page)*	1	3	3	1 3	**1**	1	**1**	Yes No
		41	**71**	**162**	**46.30%**			**75**	
	Data Center Information								
	The Service Provider should complete the following section.								
	Primary Data Center								
19	Do you operate and maintain your own Primary Data Center	5	5	25	1 5	**2**	5	**25**	Yes No
	a) Do you use an external service provider for your Primary Data Center?	5	5	25	1	**1**	1	**5**	Yes

	Data Center?	5	5	25	5	1	1	5	No
20	b) Provide the name and address of the Primary Data Center.								Þ 0 Þ 0 Þ
21	What is the Tier rating (as defined by the Uptime Institute) of the Primary Data Center?	3	5	15	4 3 2 1 5	3	2	9	Tier 1 (99.671%) Tier 2 (99.741%) Tier 3 (99.982%) Tier 4 (99.995%) None. Explain on the notes page
22	Do you maintain an encrypted copy of all primary production data off site?	5	5	25	1 5	2	5	25	Yes No
23	Do you maintain an application image for recovery purposes?	5	5	25	1 5	1	1	5	Yes No
24	Are your backups routinely verified and tested for recovery purposes?	5	3	15	1 3	1	1	5	Yes No
25	Is your primary data center staffed and monitored 24x7x365?	3	5	15	1 5	1	1	3	Yes No
26	Are there servers located in physically secured and environmentally controlled rooms? *If yes, explain on the notes page.*	5	5	25	1 5	1	1	5	Yes No
26	Are there systems in place to prevent theft of physical data stores?	5	3	15	1 3	1	1	5	Yes No
27	Do you have multiple network carriers for redundancy supporting your Primary Data Center with separate points of ingress and egress?	5	5	25	1 5	1	1	5	Yes No
28	Do other companies or organizations use computing resources that reside in the same location as the Primary Data Center	1	3	3	3 1	1	3	3	Yes No
29	Will BROOKLINE data be located in a shared database or one separated from other clients of the vendor? If shared, explain how BROOKLINE data and access to it are separated from other customers' data.	2	3	6	1 3	1	1	2	Standalone Shared
30	What fire detection and suppression system is used in your Primary Data Center?	3	3	9	1 1 1		0	0	FM 200 Gas Pre-action Dry Pipe Other, explain on the notes page
31	What types of physical security and currently in place at your Primary Data Center?	3	4	12	1 1 1 1		0	0	Key card Bio-metrics CCTY/Security Cameras Other, explain on the notes page
		55	59	240	40.42%			97	
	Alternate Data Center								
32	Do you operate and maintain your own Alternate Data Center?	3	5	15	1 5	2	5	15	Yes No
	a) Do you use an external service provider for your Alternate Data Center?	3	5	15	1 5	1	1	3	Yes No
33	b) Provide the name and address of the Alternate Data Center.								Þ Þ

									Þ
34	What is the Tier rating (as defined by the Uptime Institute) of the Primary Data Center?	3	5	15	4 3 2 1 5	**3**	2	**9**	Tier 1 (99.671%) Tier 2 (99.741%) Tier 3 (99.982%) Tier 4 (99.995%) None, explain on the notes page
35	What is the approximate physical distance between your Primary Data Center and your Alternate Data Center?	5	3	15	3 2 1 5	**3**	1	**5**	< 5 miles 5-25 miles > 25 miles Not applicable
36	How is your organization's Alternate Data Center configured to provide redundant data services to BROOKLINE?	3	3	9	1 2 3	**2**	2	**6**	Active/Active Active/Passive Other, specify on the notes page
37	What methodology is in place to support data replication to the Alternate Data Center?	3	3	9	1 2 3	**2**	2	**6**	Synchronous Asynchronous Other:
38	Do you have multiple network carriers for redundancy supporting your Alternate Data Center?	3	5	15	1 5	**1**	1	**3**	Yes No
39	Is the processing capacity of your alternate Data Center equivalent to support the BROOKLINE production needs? *If no, explain the limitations on the notes page.*	5	3	15	1 3	**1**	1	**5**	Yes No
40	How long can you support full processing capacities from your Alternate Data Center?	5	5	25	5 3 2 1	**4**	1	**5**	< 1 week < 4 weeks 1-3 months > 3 months
41	Is your Alternate Data Center staffed and monitored 24x7x365?	3	5	15	0 5	**1**	0	**0**	Yes No
42	Are the servers located in physically secured and environmentally controlled rooms? *If yes, explain on the notes page.*	3	5	15	1 5	**1**	1	**3**	Yes No
43	Are the systems in place to prevent theft of physical servers or data? *If yes, explain on the notes page.*	3	3	9	1 3	**1**	1	**3**	Yes No
44	What types of physical security are currently in place at your Alternate Data Center?	3	4	12	1 1 1 1		0	**0**	Key card Bio-metrics CCTV/Security Cameras Other, explain on the notes page
		45	**54**	**184**	**34.24%**			**63**	
	Testing Options								
	The Service Provider should complete the following section.								
	Testing								
45	Can you support a recovery exercise - conducted jointly with BROOKLINE- of the contracted services at your alternate data center?	1	3	3	1 3	**1**	1	**1**	Yes No
	a) How often will exercises be conducted?	0	0	0	1 1 0	**1**	1	**0**	Annually Semi-Annually Quarterly
46	What types of exercises can be conducted jointly with NorthBROOKLINEwell?								

	a) **Tabletop Exercise** - *to review written Recovery Documentation including the recovery scripts.*	1	3	3	1 3	**1**	1	**1**	Yes No
	b) **Functional Exercise** - *to restore or recover the system on alternate hardware to validate application functionality in parallel to production.*	2	3	6	1 3	**1**	1	**2**	Yes No
	c) **Full Redundancy Failover/Failback** - *to restore or recover the system to alternate hardware and failover production processing. Failback production processing to the production hardware after system functionality and interoperability are validated*	3	3	9	1 3	**1**	1	**3**	Yes No
47	How many hours annually will be available to BROOKLINE for testing?	3	5	15	1 2 3 4 5	**1**	1	**3**	> 48 24-48 hours 12-23 hours < 12 hours No hours planned or blocked out.
		10	**17**	**36**	**27.78%**			**10**	
		160	**220**	**655**	**38.78%**			**254**	

What privacy regulations must be addressed for the use cases supported?

What privacy controls or frameworks are employed?

What notices are given and when are they given in the process of collecting information?

Are there specific notices related to personal information?

Are there specific notices related to an individual's privacy or data rights or actions?

Are there specific policies in the case of children?

Are there policies for other special conditions, such as automated processing, health information or other special data categories?

Is the process opt in or opt out?

Does any tracking take place before notice is given or consent obtained?

Is a privacy point of contact provided?

How is the privacy policy reviewed and maintained?

Are privacy controls included in any internal or third party audits?

Are privacy controls included in logging?

BROOKLINE Business Sponsor	**0**
Vendor Company	**0**
Application & Version #	**0**

Notes & Comments