NATE's Blue Button for Consumers (NBB4C) Trust Bundle

ONBOARDING APPLICATION

Main Point of Contact	
Name:	Organization:
Telephone Number:	Mobile:
Email:	
Physical Address:	

Overview of document

This document lays out the criteria for a consumer facing [1] application's (CFA) inclusion in the National Association for Trusted Exchange's (NATE) Blue Button Trust Bundle(s) for Consumers (NBB4C). All organizations operating consumer-facing applications wishing to participate in the NBB4C bundle must complete this form and supply the necessary information and evidence to be considered for inclusion[2]. Please create a new profile, if you do not already have one, and upload your completed application and materials on the NATE Bundles Administrator (NBA) tool (https//bundles.nate-trust.org). You will receive information on how to remit the required processing fee payable to the National Association for Trusted Exchange upon receipt, along with any feedback regarding the information you have provided.

The requirements for inclusion in NATE Trust Bundles are governed by the policies and procedures of NATE and are subject to change from time to time. In the event that changes to the

[1] For the purposes of this application and onboarding to NBB4C, we use the phrase "consumer facing application" to include any application that is patient controlled and uses Direct to receive protected health information from external systems. The application may be web-based, mobile or both. It includes what have been traditionally described as PHRs as well as more narrowly focused consumer controlled apps that use the Direct mode of exchange as a secure transport mechanism between the consumer and the sources of PHI about them, including their caregivers, payers and government entities.

[2] In addition to NBB4C, NATE and its partners operate the Blue Button Plus (BB+) Patient and Provider Bundles as a free service to the community at no charge. NATE was asked by members of the BB+ community and others to establish a bundle that includes the eligibility criteria established by NATE's crowdsourcing activities as opposed to the single criteria of the BB+ bundles (public display of a Notice of Privacy Practices via the candidate's external website).

inclusion requirements are approved by the NATE Board of Directors, each organization operating a CFA will be required to resubmit or otherwise demonstrate compliance with the criteria within a period of time decided upon by the Board, but not to be less than 30 days unless required by changes in applicable law. Onboarded entities always have the right to withdraw from a NATE operated bundle at any time.

In the event that your application does not meet or exceed the requirements for onboarding, you will receive information regarding any gaps identified. At the discretion of NATE, you may be required to resubmit an application; if the new application is not received within 30 days, an additional processing fee may be required to offset the additional cost incurred by NATE.

Once your application has been approved, you will be required to upload the following information on the NATE Bundles Administrator (https://bundles.nate-trust.org):

1. The technical point of contact (name and email address) for the person responsible for managing updates to trust anchors in the trust store[3].
2. The technical point of contact (name and email address) for the person responsible for transport (not content) testing, should it be different from (1) above.
3. The trust anchor certificate for the Direct HISP.

Certificates can be provided in any format. However, some formats and extensions are identified as a potential security threat by our email servers. Therefore, either (1) include the certificate in a ZIP file archive, or (2) change the extension to something harmless (such as "txt") and include the correct format/extension in the body of the email.

Related NATE documents:

- NATE Procedure 3 d 1
- NATE Policy 3 c 3 (NBB4C)

Questions regarding this form or the onboarding processes in general can be directed to Aaron Seib, NATE CEO, at aaron.seib@nate-trust.org.

[3] Since not all organizations have the ability to automatically poll https://bundles.nate-trust.org/nbb4c.p7c for updates to NBB4C, our procedures require the NATE Trust Bundle Coordinator to send an alert to all bundle participants whenever an update is made.

A. General Obligations of the Consumer Facing Application (CFA)

Obligation	Method of Attestation	Provide a description of how this obligation is satisfied and attach any additional documentation or evidence as necessary.
1. The CFA shall comply with all applicable state and federal laws and regulations.	☐Self-Attestation alone	Applicant expects to remain compliant with all applicable laws and regulations within the states in which consumers access its offering.
2. The CFA shall display their Privacy Notice in an easily accessible location prior to sign up or use. Must include language on the application's data practices, including those areas addressed by the ONC Personal Health Record (PHR) Privacy Notice.	☐Self-Attestation with supporting materials submitted	Applicant should include links to its published privacy notices and a link to the home page of the application's service. For those applicants that offer smart phone applications only, text of their privacy policies or instructions on how a user is presented their privacy policy are sufficient alternatives. Applicant should also include a narrative response on how its approach to NPP materials echoes the information provided by the ONC's Personal Health Record (PHR) Privacy Notice.
3. The CFA shall notify its users and consumers of changes to its Privacy Notice per applicable law; when CFA is required to notify its users NATE shall be notified as well.	☐Self-Attestation with supporting materials submitted	Applicant should provide a narrative response on how its users are notified of changes and updates to any privacy policies. Applicant should describe how NATE is to be notified of updates to privacy policies. Failure to notify NATE of changes to a Privacy Policy may result in removal of your organization from the bundle.
4. The CFA shall conform to industry-accepted security practices and at a minimum maintain necessary safeguards for ensuring the privacy and security of personally identifiable health information.	☐Self-Attestation with supporting materials submitted	Please provide any information, including 3rd Party independent reports, that speaks to your offering's compliance with industry accepted security practices and safeguards that your organization has put in place along with your written attestation.

Obligation	Method of Attestation	Provide a description of how this obligation is satisfied and attach any additional documentation or evidence as necessary.
5. The CFA shall perform periodic Network Security Audits	☐Self-Attestation with supporting materials submitted ☐Not Applicable	The frequency with which Network Security Audits are performed and the outcomes of these audits are sensitive information the disclosure of which could tend to make a system less secure. The Community requires that the applicant acknowledge the value of having a defined approach to auditing Network Security and responding to their findings. By attesting to meeting this obligation the CFA acknowledges that it risk a finding of deceptive practices by enforcement agencies if it fails to meet this obligation.
6. The CFA shall perform regular Network Intrusion Detection	☐Self-Attestation with supporting materials submitted ☐Not Applicable	The frequency with which Network Intrusion Detection is performed and the outcomes of this test are sensitive information the disclosure of which could tend to make a system less secure. The Community requires that the applicant acknowledge the value of having a defined approach to Network Intrusion Detection and responding to their findings. By attesting to meeting this obligation the CFA acknowledges that it risk a finding of deceptive practices by enforcement agencies if it fails to meet this obligation.
7. The CFA shall conduct regular Web Application Security scanning/testing (for web-based PHR applications only)	☐Self-Attestation with supporting materials submitted ☐Not Applicable	The frequency with which Web Application Security tests are performed and the outcomes of these tests are sensitive information the disclosure of which could tend to make a system less secure. The Community requires that the applicant acknowledge the value of having a defined approach to tests and responding to their findings. By attesting to meeting this obligation the CFA acknowledges that it risk a finding of deceptive practices by enforcement agencies if it fails to meet this obligation.
8. The CFA shall conduct periodic third-party Penetration Testing	☐Self-Attestation alone ☐Not Applicable	The frequency with which Penetration Tests are performed and the outcomes of these tests are sensitive information the disclosure of which could tend to make a system less secure. The Community requires that the applicant acknowledge the value of having a defined approach to Penetration Testing and responding to their findings. By attesting to meeting this obligation the CFA acknowledges that it risk a finding of deceptive practices by enforcement agencies if it fails to meet this obligation.

Obligation	Method of Attestation	Provide a description of how this obligation is satisfied and attach any additional documentation or evidence as necessary.
9. The CFA shall only transmit data as directed or approved by the consumer.	☐Self-Attestation with reference to location in Policies submitted ☐ Not applicable	Applicant should supply a statement of attestation and/or inclusion of reference to the applicable consumer facing policy statement or similar policy artifact. If you indicate not applicable please describe why this is not applicable to your offering. For example, by design the way you have architected your application only the end user ever has the ability to share data once delivered to a device controlled solely by the consumer.
10. The CFA shall communicate in its consumer facing materials that the offering is not intended for use by a HIPAA Covered Entity in place of an EMR or similar application.	☐Self-Attestation with reference to location in Policies submitted.	Applicant should supply a statement of attestation and inclusion of reference to the applicable consumer facing policy statement or similar policy artifact.
11. CFA shall ensure that an End-user is able to extract all of their structured data captured in the CFA and be able transport it to another location via Direct or another secure transport method.	☐Self-Attestation with reference to location in Policies submitted and outline of how a consumer can export standard data to a secure end-point.	The community being established by this bundle is intended to enable consumer choice and prevent vendor lock-in where the consumer's PHI is trapped in a CFA.

Obligation	Method of Attestation	Provide a description of how this obligation is satisfied and attach any additional documentation or evidence as necessary.
12. CFA shall ensure that an End-user is able to terminate their participation in the CFA and be able to request that their data be expunged in its entirety from the application and any data stores controlled by the CFA that may contain the End-users PHI.	☐Self-Attestation with reference to location in policies submitted and outline of how a consumer requests that the Consumer's PHI be expunged from the CFA's data stores. ☐Not Applicable	The community being established by this bundle is intended to ensure that the consumer has control over how its PHI is used including how it is used after termination of the consumer's use of the application.

B. Eligibility Criteria for Direct

Obligation	Method of Attestation	Provide a description of how this obligation is satisfied and attach any additional documentation or evidence as necessary.
1. Conform to Direct Project's *Applicability Statement for Secure Health Transport, version 1.1*.	☐Self-Attestation indicating expectation that applicant will complete testing successfully as part of onboarding process.	Applicant should provide attestation and/or narrative description of its compliance with the Applicability Statement. Applicants with certification demonstrating compliance or similar evidence may submit such evidence as part of application process. All applicants must complete the confirmation tests required during the onboarding process as described in NATE Procedure 3.d.1
2. Encrypt all edge protocol communications (last mile exchange).	☐Self-Attestation with supporting materials.	Applicant should provide a description of how edge protocols are secured.
3. Have a documented process for the provisioning and management of digital certificates	☐Self-Attestation with supporting materials.	Applicant should include a copy of applicable certificate policy & Certificate Practice Statement or supply the rationale for why this item is not applicable. Note: NATE does not permit multi-tenant certificates to be used in any NATE Trust Bundle.
4. The NATE-QE POC shall notify the Trust Bundle Coordinator when trust anchors/public keys should be removed or replaced due to any reason (including expiration of trust anchors) and supply new trust anchors in a timely fashion.	☐Self-Attestation with supporting materials.	Applicant should provide attestation of compliance, including the name and title of who is responsible for notifications and certificate management.
5. Ensure that at any given time, only unique Direct addresses are active. Once a Direct address is inactivated it may never be reused again.	☐Self-Attestation with reference to location in Policies submitted in response to item 4.A	Applicant should provide written attestation of compliance and reference to location in written policies where this requirement is documented.

In addition to the required materials to be submitted by an applicant, NATE encourages all applicants to provide:

- Any third-party audit or accreditation information applicable to the CFA. Audit and/or accreditation examples include SOC2, EHNAC or similar verifiable evidence.
- A Statement of Principles in support of FIPPs

NATE will make this information discoverable by relying parties in the future as supporting standards emerge to enable computable use of such third party information.

My signature below affirms that the above information is true, complete and accurate, and that I am authorized to execute this CFA Onboarding Form on behalf of the designated organization. I understand that 'self-attestation' to the obligations may or may not be further verified by NATE and any discovery of contradiction to attested statements will result in immediate removal from the bundle. Further, law enforcement agencies may find attestation to these facts without sufficient evidence to support such an attestation as a deceptive or unfair practice.

Printed Name	**Title and Organization**
Signature	**Date**