MOBSF

ANDROID STATIC ANALYSIS REPORT

NYU Langone Health (2.12.3)

File Name:	org.nyulmc.clinical.mychart_158.apk
Package Name:	org.nyulmc.clinical.mychart
Scan Date:	Sept. 1, 2025, 4:08 p.m.
App Security Score:	42/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	16	1	0	1

FILE INFORMATION

File Name: org.nyulmc.clinical.mychart_158.apk
Size: 70.57MB
MD5: db945ee5c6b56e34a2547b0797026adf
SHA1: 9be43b5e74cf0d1c82edfe64d4a6cba7440a0c3e
SHA256: 809f0d79885e0b8e68de8ebccde524934b74d598bab8b07650b26052a640f57e

APP INFORMATION

App Name: NYU Langone Health
Package Name: org.nyulmc.clinical.mychart

Main Activity: org.nyulmc.clinical.mychart.coreactivities.splash.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 2.12.3
Android Version Code: 158

APP COMPONENTS

Activities: 123
Services: 21
Receivers: 19
Providers: 5
Exported Activities: 5
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=New York, L=New York, O=NYULMC, OU=MCIT, CN=NYU Langone Medical Center
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-02-16 14:49:55+00:00
Valid To: 2044-07-04 14:49:55+00:00
Issuer: C=US, ST=New York, L=New York, O=NYULMC, OU=MCIT, CN=NYU Langone Medical Center
Serial Number: 0x48dd4b42
Hash Algorithm: sha256
md5: 95c7691acdbb3e93e0335b4e7d06ff81
sha1: b61a69c8eda6c454a1cdbb19f31c92906125b9f4
sha256: 4eeaec4d7603b3090057fcc02c15df2edf31de33775a36a1542eff469e5784fd
sha512: e8f57247e5436ff643253a829467cd7f228a008657d2573e0fccfc85e7aec5723d585f4ad85e24bf3d3ccbaf4c27c3c9d805b09ac87f418044dd42892b178363
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e76b0b710cefd8ae9842767bbd88963ffa847367a405cdaede6874e8726d18d1
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_PRIVILEGED	SignatureOrSystem	allows privileged Bluetooth operations without user interaction.	Allows applications to pair bluetooth devices without user interaction, and to allow or disallow phonebook access or message access. This is not available to third party applications.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
org.nyulmc.clinical.mychart.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
db945ee5c6b56e34a2547b0797026adf.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check
classes.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes2.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes3.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.nyulmc.clinical.mychart.coreactivities.uriintercept.launcher.UriLauncherActivity	Schemes: nyulangone://, https://, Hosts: app, nyulangone.app.link, nyulangone.app,
epic.mychart.android.library.prelogin.SplashActivity	Schemes: epicmychart://,

NETWORK SECURITY

HIGH: **2** | WARNING: **1** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **13** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/wp_network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (org.nyulmc.clinical.mychart.coreactivities.uriintercept.launcher.UriLauncherActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (epic.mychart.android.library.prelogin.SplashActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Activity (epic.mychart.android.library.healthlinks.HealthConnectPrivacyPolicyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity-Alias (epic.mychart.android.library.HealthConnectViewPermissionsActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Activity (org.nyulmc.clinical.validic.activity.SplashActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
11	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
13	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
14	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://nyu-langone-health.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/1021581772611/namespaces/firebase:fetch?key=AIzaSyD2D5E_w54TZHPoMy2cpsEqRYegHjcY8hY is enabled. Ensure that the configurations are not sensi Portal":"https://nyulangone.app/sQLT82W6yTb"},"imageBase64":"%2F9j%2F4AAQSkZJRgABAQAASABIAAD%2F4QBARXhpZgAATU0AKgAA%0A%20AAgAAYdpAAQAAAABAAAAGgAAAAAAAqACAAQAAAABAAAAyKADAAQAAAABAAAAyAAAAD%2F7({"contactName":"NYU Langone Health","about":"","numbers":{"Contact Us":"646-929-7979","MyChart SMS (do not call)":"69854","Appointment Reminders (do not call)":"332-241-5051","Insurance Verification (do not call)":"855-938-4405","Patien Portal":"https://nyulangone.app/sQLT82W6yTb"},"imageBase64":"%2F9j%2F4AAQSkZJRgABAQAASABIAAD%2F4QBARXhpZgAATU0AKgAA%0A%20AAgAAYdpAAQAAAABAAAAGgAAAAAAAqACAAQAAAABAAAAyKADAAQAAAABAAAAyAAAAD%2F7('whitelisted_domains': '["pixel.sitescout.com","demdex.net","nyulmc.demdex.net","www.demdex.net","www.nyulmc.demdex.net","mychartradviewer-test.nyumc.org","mychartradviewer.nyumc.org","www.mychartradviewer-test.nyumc.org","w

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	9/44	com.google.android.gms.permission.AD_ID, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
mychart.nyulmc.org	ok	**IP:** 216.120.157.89 **Country:** United States of America **Region:** Michigan **City:** Grandville **Latitude:** 42.898064 **Longitude:** -85.757111 **View:** Google Map
activation.nyulmc.org	ok	**IP:** 216.120.157.55 **Country:** United States of America **Region:** Michigan **City:** Grandville **Latitude:** 42.898064 **Longitude:** -85.757111 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
nyu-langone-health.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
nyulangone.org	ok	**IP:** 216.120.157.19 **Country:** United States of America **Region:** Michigan **City:** Grandville **Latitude:** 42.898064 **Longitude:** -85.757111 **View:** Google Map

EMAILS

EMAIL	FILE
example@example.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AltBeacon		https://reports.exodus-privacy.eu.org/trackers/219
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"Branding_Google_Client_Secret" : "ALNQf1ber_u8Q1jM4B5LjxhN"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://nyu-langone-health.firebaseio.com"
"google_api_key" : "AIzaSyD2D5E_w54TZHPoMy2cpsEqRYegHjcY8hY"
"google_crash_reporting_api_key" : "AIzaSyD2D5E_w54TZHPoMy2cpsEqRYegHjcY8hY"
"nyu_login_password" : "Password"
"nyu_login_username" : "Username"
"username" : "Username"
"wp_key_preferences_about" : "wp_preference_about"
"wp_key_preferences_allow_all_locales" : "wp_key_preferences_allow_all_locales"
"wp_key_preferences_clear_disc_webview_cache" : "wp_key_preferences_clear_disc_webview_cache"
"wp_key_preferences_clear_ram_webview_cache" : "wp_key_preferences_clear_ram_webview_cache"
"wp_key_preferences_clear_webview_cache" : "wp_key_preferences_clear_webview_cache"
"wp_key_preferences_custom_locale" : "wp_key_preferences_custom_locale"
"wp_key_preferences_custom_phone_book" : "wp_preference_custom_phone_book"
"wp_key_preferences_custom_server" : "wp_preference_custom_server"
"wp_key_preferences_custom_server_switch" : "wp_preference_custom_server_switch"

POSSIBLE SECRETS
"wp_key_preferences_enable_webview_cache" : "wp_key_preferences_enable_webview_cache"
"wp_key_preferences_health_connect_switch" : "wp_key_preferences_health_connect_switch"
"wp_key_preferences_health_data_debug_switch" : "wp_key_preferences_health_data_debug_switch"
"wp_key_preferences_screenshots" : "wp_preference_screenshots"
"wp_key_preferences_testing_header" : "wp_preferences_testing_header"
"wp_key_preferences_tool_tip" : "wp_key_preferences_tool_tip"
"wp_key_preferences_webivew_cache_header" : "wp_preferences_webview_cache_header"
"wp_login_password" : "Password"
"wp_login_username" : "Username"
"wp_share_everywhere_dismiss_token_button_title" : "Dismiss"
"wp_two_factor_authenticate_code_button" : "Verify"
"wp_two_factor_authentication_success_accessibility_announcement" : "Success!"

PLAYSTORE INFORMATION

Title: NYU Langone Health

Score: 4.6474953 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** org.nyulmc.clinical.mychart

Developer Details: NYU Langone Health, NYU+Langone+Health, None, http://www.nyulangone.org, webteam@nyumc.org,

Release Date: Apr 26, 2017 **Privacy Policy:** Privacy link

Description:

As an NYU Langone Health patient, you can use our app to manage your health information and care on a mobile device. When you log in to the app with your NYU Langone Heath MyChart account, you'll have convenient access to features including: • Health summary: See your current health concerns, medications, immunizations, allergies, and more. • Appointments: Find the right doctor for your needs; schedule or cancel upcoming visits; and see information about previous appointments. • Test results: View lab test results and information about what they mean. • Messages: Communicate conveniently with your care team. • Health advisories: Be notified when it's time for your annual physical, flu shot, and other preventive care needs. • Proxy access: View health information for designated family members, including children. • Remote monitoring: Connect the app with Apple Health or Health Connect (by Google) to monitor and share key health information with your care team, including but not limited to blood glucose, blood pressure, oxygen saturation, steps, temperature, and weight. (Disclaimer: Remote patient monitoring through the NYU Langone Health app requires prior enrollment of the patient by a healthcare provider. The app currently does not support individual usage without clinician consent and support. Patients must always consult with their healthcare provider before making any changes to a care plan.)

SCAN LOGS

Timestamp	Event	Error
2025-09-01 16:08:38	Generating Hashes	OK

2025-09-01 16:08:38	Extracting APK	OK
2025-09-01 16:08:38	Unzipping	OK
2025-09-01 16:08:38	Parsing APK with androguard	OK
2025-09-01 16:08:39	Extracting APK features using aapt/aapt2	OK
2025-09-01 16:08:39	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 16:08:42	Parsing AndroidManifest.xml	OK
2025-09-01 16:08:42	Extracting Manifest Data	OK
2025-09-01 16:08:42	Manifest Analysis Started	OK
2025-09-01 16:08:43	Reading Network Security config from wp_network_security_config.xml	OK
2025-09-01 16:08:43	Parsing Network Security config	OK
2025-09-01 16:08:43	Performing Static Analysis on: NYU Langone Health (org.nyulmc.clinical.mychart)	OK
2025-09-01 16:08:44	Fetching Details from Play Store: org.nyulmc.clinical.mychart	OK
2025-09-01 16:08:46	Checking for Malware Permissions	OK
2025-09-01 16:08:46	Fetching icon path	OK
2025-09-01 16:08:46	Library Binary Analysis Started	OK
2025-09-01 16:08:46	Reading Code Signing Certificate	OK
2025-09-01 16:08:46	Running APKiD 2.1.5	OK

2025-09-01 16:08:49	Detecting Trackers	OK
2025-09-01 16:08:55	Decompiling APK to Java with JADX	OK
2025-09-01 16:25:42	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/db945ee5c6b56e34a2547b0797026adf/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/db945ee5c6b56e34a2547b0797026adf/db945ee5c6b56e34a2547b0797026adf.apk'], 999.9999267086387)
2025-09-01 16:25:42	Converting DEX to Smali	OK
2025-09-01 16:25:42	Code Analysis Started on - java_source	OK
2025-09-01 16:25:42	Android SBOM Analysis Completed	OK
2025-09-01 16:25:42	Android SAST Completed	OK
2025-09-01 16:25:42	Android API Analysis Started	OK
2025-09-01 16:25:42	Android API Analysis Completed	OK
2025-09-01 16:25:50	Android Permission Mapping Started	OK
2025-09-01 16:26:49	Android Permission Mapping Completed	OK
2025-09-01 16:26:49	Android Behaviour Analysis Started	OK
2025-09-01 16:26:50	Android Behaviour Analysis Completed	OK
2025-09-01 16:27:02	Extracting Emails and URLs from Source Code	OK
2025-09-01 16:28:37	Email and URL Extraction Completed	OK
2025-09-01 16:40:39	Extracting String data from APK	OK
2025-09-01 16:40:39	Extracting String data from Code	OK

2025-09-01 16:40:39	Extracting String values and entropies from Code	OK
2025-09-01 16:40:40	Performing Malware check on extracted domains	OK
2025-09-01 16:40:42	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.