MOBSF

ANDROID STATIC ANALYSIS REPORT

Sharp (1.16.1)

File Name:	com.shc.mobile_2376.apk
Package Name:	com.shc.mobile
Scan Date:	Sept. 1, 2025, 8:37 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	16	4	3	1

FILE INFORMATION

File Name: com.shc.mobile_2376.apk
Size: 62.23MB
MD5: 8f28b95863f8595ae364c7c42932dcce
SHA1: 2cb6e22cfc509be5b8384625cfb9f50b778f816d
SHA256: e92b6f65cccab3b1759746abc30a782019c5d8800922c3168375a9b353821f76

APP INFORMATION

App Name: Sharp
Package Name: com.shc.mobile
Main Activity: com.shc.mobile.MainActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 1.16.1

Android Version Code: 2376

APP COMPONENTS

Activities: 98
Services: 13
Receivers: 8
Providers: 4
Exported Activities: 1
Exported Services: 1
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=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-05-24 20:04:30+00:00
Valid To: 2053-05-24 20:04:30+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf213fdb611c353facc6538e9326ff548a456c02b
Hash Algorithm: sha256
md5: cd6952a8f23ddb94bef25c1ca1fbaf52
sha1: 206b15412f4c59c63f437265685d119a9178a7aa
sha256: d7836abbcfbbbe625bba5e1ddabfdb662aeb7027e7f6668643229e462821dfcf
sha512: 45fd8be131541f4c48fb9b4136c1f238bd34592f32c8ed235deba449499388fa9173b79a92b983de69bde1c5545498f9ff7804144ef9f94be2b09ae53b7254a1
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 6279ac2a4578f6c5c2cc454e931835641ea2b0d8cd3d86a51b88361330ed01fe
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_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.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.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
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.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.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.shc.mobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>8f28b95863f8595ae364c7c42932dcce.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.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</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.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
SIM operator check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes3.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
possible Build.SERIAL check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<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-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>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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL 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>
</table>

FILE	DETAILS
classes6.dex	<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>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.shc.mobile.MainActivity	Schemes: https://, epicmychart://, epichttp://, Hosts: app.sharp.com, app-nonprod.sharp.com, portal.sharp.com, portal-stg.aws-nonprod.sharp.com, portal-dev.aws-nonprod.sharp.com, *, Path Prefixes: /sharpapp/app, /MyChartTST/app, /appointments,
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: **5** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Broadcast Receiver (com.reactnativeshcrnmychartplugin.services.NotificationClickReceiver) is not Protected. [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.
3	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.
4	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.
5	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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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

HIGH: **1** | WARNING: **8** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/aurelhubert/ahbottomnavigation/AHBottomNavigation.java com/dynatrace/android/agent/util/Utility.java com/dynatrace/android/callback/HttpClientCallback.java com/emeraldsanto/encryptedstorage/RNEncryptedStorageModule.java com/epic/patientengagement/core/session/MyChartOrgToOrgJumpManager.java com/epic/patientengagement/core/ui/ProgressBar.java com/epic/patientengagement/core/ui/buttons/CoreButton.java com/epic/patientengagement/core/ui/buttons/CoreButtonUtils.java com/epic/patientengagement/core/ui/stickyhe

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ader/StickyHeaderAdapter.java com/epic/patientengagement/core/ui/tutorials/PETutorialFragment.java com/epic/patientengagement/core/utilities/PerformanceLogger.java com/epic/patientengagement/core/utilities/broadcast/BroadcastManager.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/epic/patientengagement/todo/progress/c.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/FilterView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/reactnativecommunity/geolocation/AndroidLocationManager.java com/reactnativecommunity/geolocation/PlayServicesLocationManager.java com/reactnativecommunity/webview/RNCWebView.java com/reactnativecommunity/webview/RNCWebViewClient.java com/reactnativecommunity/webview/RNCWebViewManagerImpl.java com/reactnativenavigation/react/DevPermissi

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	onRequest.java com/reactnativenavigation/react/events/EventEmitter.java com/reactnativenavigation/utils/LogKt.java com/reactnativenavigation/utils/Time.java com/reactnativenavigation/utils/WindowInsetsUtils.java com/reactnativenavigation/viewcontrollers/stack/topbar/button/IconResolver.java com/reactnativenavigation/views/sidemenu/SideMenu.java com/reactnativeshcrnmychartplugin/MychartInitialization.java com/reactnativeshcrnmychartplugin/ShcRnMychartPluginModule.java com/reactnativeshcrnmychartplugin/activities/CareTeamAndGoalsActivity.java com/reactnativeshcrnmychartplugin/activities/LoginActivity.java com/reactnativeshcrnmychartplugin/factories/WidgetFactory.java com/reactnativeshcrnmychartplugin/services/DeepLinkListener.java com/reactnativeshcrnmychartplugin/services/PersonManagerService.java com/reactnativeshcrnmychartplugin/services/PushNotificationInterceptorService.java com/reactnativeshcrnmychartplugin/services/WebViewService.java com/snowplowanalytics/core/tracker/DefaultLoggerDelegate.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/keyboard/WindowsInsetsManager.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/ScreensHelper.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/layoutReanimation/TabNavigatorObserver.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/th3rdwave/safeareacontext/SafeAreaView.java com/zoontek/rnpermissions/RNPermissionsModuleImpl.java epic/mychart/android/library/api/classes/WPAPIFirebaseMessagingService.java epic/mychart/android/library/appointments/FutureAppointmentFragment.java epic/mychart/android/library/appointments/c.java epic/mychart/android/library/campaigns/d.java epic/mychart/android/library/customactivities/JavaScriptWebViewActivity.java epic/mychart/android/library/customadapters/StickyHeaderSectionAdapter/c.java epic/mychart/android/library/general/AccessResult.java epic/mychart/android/library/general/f.java epic/mychart/android/library/googlefit/e.java epic/mychart/android/library/location/fragments/a.java epic/mychart/android/library/location/service

NO	ISSUE	SEVERITY	STANDARDS	FILES
				epic/mychart/android/library/location/services/AppointmentArrivalService.java epic/mychart/android/library/pushnotifications/CustomFcmListenerService.java epic/mychart/android/library/trackmyhealth/a.java epic/mychart/android/library/utilities/d0.java epic/mychart/android/library/utilities/e0.java epic/mychart/android/library/utilities/j.java epic/mychart/android/library/utilities/k.java epic/mychart/android/library/utilities/p.java epic/mychart/android/library/utilities/r.java epic/mychart/android/library/utilities/y.java org/greenrobot/eventbus/Logger.java org/greenrobot/eventbus/util/ErrorDialogConfig.java org/greenrobot/eventbus/util/ErrorDialogManager.java org/greenrobot/eventbus/util/ExceptionToResourceMapping.java
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/epic/patientengagement/core/utilities/DeviceUtil.java com/epic/patientengagement/core/utilities/file/FileChooserType.java com/epic/patientengagement/core/utilities/file/FileUtil.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java epic/mychart/android/library/utilities/DeviceUtil.java
				com/dynatrace/android/agent/events/eventsapi/EnrichmentAttribute.java com/dynatrace/android/agent/events/eventsapi/EnrichmentAttributesGenerator.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewActivit

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	y.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/epic/patientengagement/authentication/login/activities/SAMLLoginActivity.java com/epic/patientengagement/authentication/login/fragments/EnterPasscodeDialogFragment.java com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/authentication/login/fragments/LongTextDialogFragment.java com/epic/patientengagement/authentication/login/fragments/OrgFragment.java com/epic/patientengagement/authentication/login/utilities/LoginHelper.java com/epic/patientengagement/authentication/login/utilities/LoginResultCode.java com/epic/patientengagement/authentication/login/utilities/OrganizationLoginHelper.java com/epic/patientengagement/authentication/login/utilities/SamlSessionManager.java com/epic/patientengagement/core/deeplink/DeepLinkLaunchParameters.java com/epic/patientengagement/core/mychartweb/ExternalJumpDialogFragment.java com/epic/patientengagement/core/mychartweb/MyChartWebQueryParameters.java com/epic/patientengagement/core/mychartweb/MyChartWebViewClient.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/epic/patientengagement/core/mychartweb/WebSessionWebServiceAPIHelper.java com/epic/patientengagement/core/onboarding/OnboardingHostFragment.java com/epic/patientengagement/core/onboarding/OnboardingPageFragment.java com/epic/patientengagement/core/permission

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s/PermissionProminentDisclosure.java com/epic/patientengagement/core/ui/VideoCardView.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/epic/patientengagement/core/utilities/file/FileChooserTypeSelectionDialogFragment.java com/epic/patientengagement/core/webservice/WebService.java com/epic/patientengagement/core/webservice/processor/MyChartResponseProcessor.java com/epic/patientengagement/homepage/HomePageComponentAPI.java com/epic/patientengagement/homepage/onboarding/a.java com/reactnativenavigation/options/params/ThemeColourKt.java com/reactnativenavigation/react/Constants.java com/reactnativeshcrnmychartplugin/utility/CallKeys.java com/snowplowanalytics/core/tracker/TrackerControllerImpl.java com/snowplowanalytics/snowplow/event/MessageNotification.java epic/mychart/android/library/api/classes/WPAPIAuthentication.java epic/mychart/android/library/googlefit/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/utilities/file/FileUtil.java com/epic/patientengagement/pdfviewer/pdf/PdfFile.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java epic/mychart/android/library/customviews/PdfViewerActivity.java epic/mychart/android/library/utilities/k.java
5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/dynatrace/android/agent/db/EventsDbHelper.java com/dynatrace/android/agent/db/ParmDbHelper.java com/snowplowanalytics/core/emitter/storage/EventStoreHelper.java com/snowplowanalytics/core/emitter/storage/SQLiteEventStore.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/dynatrace/android/agent/data/RandomFactory.java com/dynatrace/android/agent/data/Session.java com/epic/patientengagement/homepage/itemfeed/webservice/items/ZeroStateFeedItem.java com/epic/patientengagement/todo/models/QuestionnaireSeries.java epic/mychart/android/library/utilities/a.java epic/mychart/android/library/utilities/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/epic/patientengagement/core/utilities/EncryptionUtil.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/dynatrace/android/agent/RootDetector.java com/dynatrace/android/agent/events/eventsapi/EnrichmentAttributesGenerator.java com/dynatrace/android/agent/events/eventsapi/EventMetrics.java com/dynatrace/android/agent/metrics/AndroidMetrics.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/snowplowanalytics/core/session/FileStore.java com/snowplowanalytics/core/session/Session.java com/snowplowanalytics/snowplow/network/CollectorCookieJar.java
10	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/dynatrace/android/agent/Dynatrace.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java
11	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/dynatrace/android/agent/comm/ssl/SimpleX509TrustManager.java com/snowplowanalytics/core/emitter/TLSArguments.java
13	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	epic/mychart/android/library/utilities/k.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/dynatrace/android/agent/metrics/AndroidMetrics.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/snowplowanalytics/core/utils/DeviceInfoMonitor.java

RULE ID	BEHAVIOUR	LABEL	FILES
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/epic/patientengagement/authentication/login/activities/SAMLLoginActivity.java com/epic/patientengagement/authentication/login/fragments/LoginFragmentKt.java com/epic/patientengagement/authentication/login/fragments/LongTextDialogFragment.java com/epic/patientengagement/authentication/login/fragments/OrgFragment.java com/epic/patientengagement/authentication/login/utilities/PreloginDeeplinkManager.java com/epic/patientengagement/core/extensibility/ExtensibilityLaunchManager.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/epic/patientengagement/core/utilities/IntentUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/proyecto26/inappbrowser/RNInAppBrowser.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/campaigns/c.java epic/mychart/android/library/community/WebCommunityManageMyAccountsActivity.java epic/mychart/android/library/customactivities/JavaScriptWebViewActivity.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/general/FDILauncherActivity.java epic/mychart/android/library/general/e.java epic/mychart/android/library/general/f.java epic/mychart/android/library/insurance/e.java epic/mychart/android/library/letters/WebLettersActivity.java epic/mychart/android/library/personalize/c.java epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/springboard/CustomFeature.java epic/mychart/android/library/todo/PatientAssignedQuestionnaireWebViewActivity.java epic/mychart/android/library/utilities/CommunityUtil.java epic/mychart/android/library/utilities/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/proyecto26/inappbrowser/RNInAppBrowser.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/prelogin/WebServer.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/springboard/CustomFeature.java
00091	Retrieve data from broadcast	collection	com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/appointments/FutureAppointmentFragment.java epic/mychart/android/library/billing/PaymentConfirmationActivity.java epic/mychart/android/library/billing/RecentStatementActivity.java epic/mychart/android/library/healthadvisories/HealthAdvisoryMarkCompleteActivity.java epic/mychart/android/library/medications/MedRefillActivity.java epic/mychart/android/library/messages/ComposeActivity.java epic/mychart/android/library/personalize/PersonalizeFragment.java epic/mychart/android/library/springboard/CustomWebModeJumpActivity.java epic/mychart/android/library/testresults/TestResultDetailActivity.java
00075	Get location of the device	collection location	com/reactnativecommunity/geolocation/AndroidLocationManager.java com/snowplowanalytics/core/utils/Util.java
00137	Get last known location of the device	location collection	com/snowplowanalytics/core/utils/Util.java
00115	Get last known location of the device	collection location	com/snowplowanalytics/core/utils/Util.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/epic/patientengagement/pdfviewer/utilities/FileUtils.java com/snowplowanalytics/core/remoteconfiguration/RemoteConfigurationCache.java com/snowplowanalytics/core/session/FileStore.java epic/mychart/android/library/customobjects/StoredFile.java epic/mychart/android/library/customviews/PhotoViewerActivity.java epic/mychart/android/library/utilities/DeviceUtil.java epic/mychart/android/library/utilities/i.java okio/Okio__JvmOkioKt.java
00108	Read the input stream from given URL	network command	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/customobjects/a.java
00096	Connect to a URL and set request method	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java
00089	Connect to a URL and receive input stream from the server	command network	com/dynatrace/android/agent/comm/CommHandler.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java
00030	Connect to the remote server through the given URL	network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java
00109	Connect to a URL and get the response code	network command	com/dynatrace/android/agent/comm/CommHandler.java com/epic/patientengagement/core/webservice/WebServiceTask.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00147	Get the time of current location	collection location	com/reactnativecommunity/geolocation/AndroidLocationManager.java com/reactnativecommunity/geolocation/PlayServicesLocationManager.java
00177	Check if permission is granted and request it	permission	com/epic/patientengagement/core/permissions/PermissionUtil.java
00072	Write HTTP input stream into a file	command network file	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java
00094	Connect to a URL and read data from it	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/googlefit/c.java
00125	Check if the given file path exist	file	com/epic/patientengagement/core/pdfviewer/PdfFragment.java com/epic/patientengagement/pdfviewer/PdfViewerFragment.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/proyecto26/inappbrowser/RNInAppBrowser.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/utilities/k.java
00202	Make a phone call	control	epic/mychart/android/library/utilities/k.java
00203	Put a phone number into an intent	control	epic/mychart/android/library/utilities/k.java
00022	Open a file from given absolute path of the file	file	com/epic/patientengagement/core/utilities/DeviceUtil.java com/snowplowanalytics/core/remoteconfiguration/RemoteConfigurationCache.java epic/mychart/android/library/customviews/VideoPlayerActivity.java epic/mychart/android/library/messages/Attachment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	epic/mychart/android/library/messages/Attachment.java
00092	Send broadcast	command	com/reactnativeshcrnmychartplugin/MychartInitialization.java
00016	Get location info of the device and put it to JSON object	location collection	epic/mychart/android/library/location/models/MonitoredForArrivalAppointment.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00112	Get the date of the calendar event	collection calendar	epic/mychart/android/library/googlefit/g.java
00153	Send binary data over HTTP	http	epic/mychart/android/library/utilities/g.java
00012	Read data and put it into a buffer stream	file	epic/mychart/android/library/utilities/i.java
00171	Compare network operator with a string	network	com/snowplowanalytics/core/utils/DeviceInfoMonitor.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://haiku-push-notifications.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://fifth-liberty-89719.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/706446232476/namespaces/firebase:fetch?key=AIzaSyBv776FvkVLGKyvr4AR_IFvkThhUx18A2s. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.GET_ACCOUNTS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	9/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.AUTHENTICATE_ACCOUNTS, android.permission.CALL_PHONE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, 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.com	ok	**IP:** 20.118.48.1 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ichart2.epic.com	ok	**IP:** 199.204.56.101 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **View:** Google Map
schemas.datacontract.org	ok	**IP:** 207.46.197.115 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
trace.sharp.com	ok	**IP:** 199.164.159.105 **Country:** United States of America **Region:** California **City:** San Diego **Latitude:** 32.799797 **Longitude:** -117.137047 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.swmansion.com	ok	**IP:** 172.67.142.188 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.epic.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
customurl.com	ok	**IP:** 3.33.243.145 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
mychart.et1275.epichosted.com	ok	**IP:** 208.56.192.34 **Country:** United States of America **Region:** Massachusetts **City:** Andover **Latitude:** 42.648373 **Longitude:** -71.161453 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
haiku-push-notifications.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
rex.webqa.epic.com	ok	No Geolocation information available.
www.shareeverywhere.com	ok	**IP:** 199.204.56.202 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **View:** Google Map
iglucentral.com	ok	**IP:** 18.238.96.128 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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

DOMAIN	STATUS	GEOLOCATION
ichart1.epic.com	ok	**IP:** 204.187.138.40 **Country:** United States of America **Region:** Wisconsin **City:** Verona **Latitude:** 42.990845 **Longitude:** -89.568443 **View:** Google Map
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.250.74.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
fifth-liberty-89719.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
mychartsupport@epic.com	com/epic/patientengagement/authentication/login/fragments/LoginFragmentKt.java
example@example.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Dynatrace	Analytics	https://reports.exodus-privacy.eu.org/trackers/137
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Snowplow	Analytics	https://reports.exodus-privacy.eu.org/trackers/108

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://fifth-liberty-89719.firebaseio.com"
"google_api_key" : "AIzaSyBv776FvkVLGKyvr4AR_IFvkThhUx18A2s"
"google_crash_reporting_api_key" : "AIzaSyBv776FvkVLGKyvr4AR_IFvkThhUx18A2s"
"password" : "Password"
"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_google_fit_debug_switch" : "wp_key_preferences_google_fit_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!"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

POSSIBLE SECRETS
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
6cb30de6-73df-448d-893b-e0bd54bcd5b0
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
0ba96ffd-44ed-44b2-ad1c-60672175faec
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
1157920892103562487626974469494075735299969552241357603424222590610685120443 69

PLAYSTORE INFORMATION

Title: Sharp HealthCare

Score: 3.58 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.shc.mobile

Developer Details: Sharp HealthCare, Sharp+HealthCare, None, https://www.sharp.com, info@sharp.com,

Release Date: Dec 18, 2023 **Privacy Policy:** Privacy link

Description:

The Sharp HealthCare app is a care management app that helps Sharp patients throughout San Diego County and beyond conveniently manage their health care from a mobile device. From the Sharp app home screen, you can quickly access care options, get reminders, view your recent account activity — and easily click to your medical record and records of family members you're authorized to view. With convenient self-services features, you can: · Message your doctor · Schedule and manage appointments · View test results · Refill prescriptions · Check in for appointments · Pay medical bills and set up payment plans · Get price estimates for the cost of care · Access educational resources during and after a hospital stay · Review medications, immunization history and other health information · And much more Download the Sharp HealthCare app and sign in to your Sharp account or create a new account from the app. ABOUT SHARP HEALTHCARE: As San Diego's leading health care provider, Sharp is not for profit, but for people, which means all resources are dedicated to delivering the highest quality patient-centered care, the latest medical technology and superior service. Every day, approximately 2,700 affiliated physicians and 19,000 employees work to provide patients and their families with the extraordinary level of care called The Sharp Experience. With four acute-care hospitals, three specialty hospitals, three affiliated medical groups and a full spectrum of other facilities and services, Sharp HealthCare makes it easy for patients to get the care they need close to home. Learn more at sharp.com. This mobile medical app for patients is specifically designed for patients of Sharp HealthCare. New features and performance updates are released frequently. Please note: Starting with update 1.13, the Sharp app will no longer be compatible with Android versions below 10.0. Ensure your device is running Android 10.0 or higher to access the latest features and improvements.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 08:37:52	Generating Hashes	OK
2025-09-01 08:37:52	Extracting APK	OK

2025-09-01 08:37:52	Unzipping	OK
2025-09-01 08:37:52	Parsing APK with androguard	OK
2025-09-01 08:37:53	Extracting APK features using aapt/aapt2	OK
2025-09-01 08:37:53	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 08:37:55	Parsing AndroidManifest.xml	OK
2025-09-01 08:37:55	Extracting Manifest Data	OK
2025-09-01 08:37:55	Manifest Analysis Started	OK
2025-09-01 08:37:57	Reading Network Security config from wp_network_security_config.xml	OK
2025-09-01 08:37:57	Parsing Network Security config	OK
2025-09-01 08:37:57	Performing Static Analysis on: Sharp (com.shc.mobile)	OK
2025-09-01 08:37:58	Fetching Details from Play Store: com.shc.mobile	OK

2025-09-01 08:38:00	Checking for Malware Permissions	OK
2025-09-01 08:38:00	Fetching icon path	OK
2025-09-01 08:38:00	Library Binary Analysis Started	OK
2025-09-01 08:38:00	Reading Code Signing Certificate	OK
2025-09-01 08:38:00	Running APKiD 2.1.5	OK
2025-09-01 08:38:03	Detecting Trackers	OK
2025-09-01 08:38:08	Decompiling APK to Java with JADX	OK
2025-09-01 08:38:31	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 08:38:31	Decompiling classes6.dex with JADX	OK
2025-09-01 08:38:35	Decompiling classes2.dex with JADX	OK
2025-09-01 08:38:39	Decompiling classes4.dex with JADX	OK

2025-09-01 08:38:47	Decompiling classes.dex with JADX	OK
2025-09-01 08:38:56	Decompiling classes3.dex with JADX	OK
2025-09-01 08:39:02	Decompiling classes5.dex with JADX	OK
2025-09-01 08:39:10	Decompiling classes6.dex with JADX	OK
2025-09-01 08:39:14	Decompiling classes2.dex with JADX	OK
2025-09-01 08:39:18	Decompiling classes4.dex with JADX	OK
2025-09-01 08:39:27	Decompiling classes.dex with JADX	OK
2025-09-01 08:39:36	Decompiling classes3.dex with JADX	OK
2025-09-01 08:39:42	Decompiling classes5.dex with JADX	OK
2025-09-01 08:39:50	Converting DEX to Smali	OK
2025-09-01 08:39:50	Code Analysis Started on - java_source	OK

2025-09-01 08:39:54	Android SBOM Analysis Completed	OK
2025-09-01 08:39:58	Android SAST Completed	OK
2025-09-01 08:39:58	Android API Analysis Started	OK
2025-09-01 08:40:01	Android API Analysis Completed	OK
2025-09-01 08:40:01	Android Permission Mapping Started	OK
2025-09-01 08:40:07	Android Permission Mapping Completed	OK
2025-09-01 08:40:07	Android Behaviour Analysis Started	OK
2025-09-01 08:40:11	Android Behaviour Analysis Completed	OK
2025-09-01 08:40:11	Extracting Emails and URLs from Source Code	OK
2025-09-01 08:40:16	Email and URL Extraction Completed	OK
2025-09-01 08:40:16	Extracting String data from APK	OK

2025-09-01 08:40:17	Extracting String data from Code	OK
2025-09-01 08:40:17	Extracting String values and entropies from Code	OK
2025-09-01 08:40:23	Performing Malware check on extracted domains	OK
2025-09-01 08:40:28	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.