ANDROID STATIC ANALYSIS REPORT

MyAtrium (7.0.3)

File Name:	org.carolinas.android.dir_219.apk
Package Name:	org.carolinas.android.dir
Scan Date:	Sept. 1, 2025, 3:01 p.m.
App Security Score:	43/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	18	3	2	2

FILE INFORMATION

File Name: org.carolinas.android.dir_219.apk
Size: 69.75MB
MD5: 00d0cbb0a58be810685d1250843712c4
SHA1: 10bdddcd40754e94351a72ff6d542c01edd47246
SHA256: 35d0401282303b5a0efe183b65a44e3e9b5f52fe8a9e8e43e266e3d9343718b7

APP INFORMATION

App Name: MyAtrium
Package Name: org.carolinas.android.dir
Main Activity: org.carolinas.android.dir.HomeScreenActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 7.0.3

Android Version Code: 219

APP COMPONENTS

Activities: 107
Services: 18
Receivers: 9
Providers: 5
Exported Activities: 3
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: ST=NC, L=Charlotte, O=Carolinas Healthcare System
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-07-20 12:59:58+00:00
Valid To: 2071-07-05 12:59:58+00:00
Issuer: ST=NC, L=Charlotte, O=Carolinas Healthcare System
Serial Number: 0x4e26d14e
Hash Algorithm: sha1
md5: 4538c03021a1b895810cb938bf267386
sha1: 25d8c1faefc9b7a95187c3bf8c3ea3207ad045c4
sha256: 3533efc1c866d6ab2c30d5e2eca48bfed4eb86209b6d26edd101f8fffa56b9c4
sha512: 30c1a8e5fdd835c7c3e4040527c7f9ab9c7fcd01bb3e2f31f7f6124cd5c86130a20b8be979ccc248356de9bed7a631a4db7f245799b719f1f49d008066329ddf
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 27352d398ebca19b5d4aa68ac94d10599eae131780b7f1b13e371d632e58dab8
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_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.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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.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.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
org.carolinas.android.dir.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></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>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.MODEL check
Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table></td></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>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>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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator 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>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.carolinas.android.dir.HomeScreenActivity	Schemes: http://, Hosts: www.atriumhealth.org, Path Prefixes: /MyAtriumHealth,
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: **1** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **7** | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
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	App Link assetlinks.json file not found [android:name=org.carolinas.android.dir.HomeScreenActivity] [android:host=http://www.atriumhealth.org]	high	App Link asset verification URL (http://www.atriumhealth.org/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 307). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
4	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
5	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.
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.
7	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.
8	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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/stickyheader/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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/epic/patientengagement/todo/progress/c.java com/vidyo/LmiDeviceManager/LmiAudioCapturer.java com/vidyo/LmiDeviceManager/LmiAudioPlaybackDevice.java com/vidyo/LmiDeviceManager/LmiDeviceManagerView.java com/vidyo/LmiDeviceManager/LmiScreenManager.java com/vidyo/LmiDeviceManager/LmiScreenManagerCupcakeListener.java com/vidyo/LmiDeviceManager/LmiScreenManagerJellybeanListener.java com/vidyo/LmiDeviceManager/LmiVideoCapturer.java com/vidyo/LmiDeviceManager/LmiVideoCapturerInternal.java com/vidyo/LmiDeviceManager/LmiVideoCapturerManager.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/DeepLinkManager.java epic/mychart/android/library/healthlinks/b.j

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	ava epic/mychart/android/library/location/fragments/a.java 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/e0.java epic/mychart/android/library/utilities/f0.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/z.java org/altbeacon/beacon/BeaconParser.java org/altbeacon/beacon/logging/ApiTrackingLogger.java org/altbeacon/beacon/logging/InfoAndroidLogger.java org/altbeacon/beacon/logging/VerboseAndroidLogger.java org/altbeacon/beacon/logging/WarningAndroidLogger.java org/altbeacon/beacon/service/ScanHelper.java org/altbeacon/beacon/service/ScanState.java org/altbeacon/beacon/utils/EddystoneTelemetryAccessor.java org/carolinas/android/dir/CarolinasHealthApplication.java org/carolinas/android/dir/HomeScreenActivity.java org/carolinas/android/dir/LanguageSelectActivity.java org/carolinas/android/dir/ProviderSearchByNameActivity.java org/carolinas/android/dir/ProviderSearchPrimaryCareActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/carolinas/android/dir/ProviderSearchResultsActivity.java org/carolinas/android/dir/WayFindingBaseActivity.java org/carolinas/android/dir/WayFindingDestinationActivity.java org/carolinas/android/dir/WayFindingDirectionsActivity.java org/carolinas/android/dir/WayFindingStartingPointActivity.java org/carolinas/android/dir/db/FavoritesDatabase.java org/carolinas/android/dir/manager/DashboardManager.java org/carolinas/android/dir/manager/FacilityManager.java org/carolinas/android/dir/manager/MyCarolinasManager.java org/carolinas/android/dir/manager/ProviderSearchManager.java org/carolinas/android/dir/manager/ServiceCallManager.java org/carolinas/android/dir/manager/WayFindingManager.java org/carolinas/android/dir/model/Education.java org/carolinas/android/dir/model/Provider.java org/carolinas/android/dir/model/ProviderType.java org/carolinas/android/dir/model/WayFindingDirection.java org/carolinas/android/dir/model/WayFindingLocation.java org/carolinas/android/dir/model/WayFindingSubLocation.java org/carolinas/android/dir/ui/widget/CarolinasErrorDialog.java org/carolinas/android/dir/util/BitmapUtil.java org/carolinas/android/dir/util/FingerprintHa

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/carolinas/android/dir/util/FingerprintHandler.java org/carolinas/android/dir/util/Regex.java rx/internal/util/IndexedRingBuffer.java rx/internal/util/RxRingBuffer.java rx/plugins/RxJavaHooks.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/americanwell/sdk/internal/util/APIUtil.java org/carolinas/android/dir/manager/DashboardManager.java org/carolinas/android/dir/manager/ServiceCallManager.java org/carolinas/android/dir/manager/retrofit/CarolinasWebServicesRetrofitManager.java org/carolinas/android/dir/manager/retrofit/EHealthServicesRetrofitManager.java
				com/americanwell/sdk/internal/AWSDKImpl.java com/americanwell/sdk/internal/api/APIConstants.java com/americanwell/sdk/internal/manager/AbsSdkManager.java com/americanwell/sdk/manager/ValidationConstants.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewActivity.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/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/component/IAuthenticationComponentAPI.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/WebSessionWebServiceAPI.java com/epic/patientengagement/core/onboarding/OnboardingHostFragment.java com/epic/patientengagement/core/onboarding/OnboardingPageFragment.java com/epic/patientengagement/core/permissions/PermissionProminentDisclosure.java com/epic/patientengagement/core/security/SecurityPoints.java com/epic/patientengagement/core/ui/VideoCardView.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/utilities/WebUtil.java

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	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 epic/mychart/android/library/api/classes/WPAPIAuthentication.java epic/mychart/android/library/healthlinks/d.java nucleus/view/NucleusActivity.java nucleus/view/NucleusAppCompatActivity.java nucleus/view/NucleusFragment.java nucleus/view/NucleusFragmentActivity.java nucleus/view/NucleusLayout.java nucleus/view/NucleusSupportFragment.java nucleus/view/PresenterLifecycleDelegate.java org/altbeacon/beacon/service/MonitoringData.java org/altbeacon/beacon/service/RangingData.java org/altbeacon/beacon/service/SettingsData.java org/altbeacon/beacon/service/StartRMData.java org/carolinas/android/dir/LanguageSelectActivity.java org/carolinas/android/dir/ProviderSearchResultsActivity.java org/carolinas/android/dir/WayFindingDestinationActivity.java org/carolinas/android/dir/WayFindingDirecti

NO	ISSUE	SEVERITY	STANDARDS	FILES
				onsActivity.java org/carolinas/android/dir/WayFindingStartingPointActivity.java org/carolinas/android/dir/WebViewActivity.java org/carolinas/android/dir/db/FavoritesDatabase.java org/carolinas/android/dir/manager/FacilityManager.java org/carolinas/android/dir/manager/NetworkManager.java org/carolinas/android/dir/model/Education.java org/carolinas/android/dir/model/Practice.java org/carolinas/android/dir/model/Provider.java org/carolinas/android/dir/model/ProviderType.java org/carolinas/android/dir/model/SearchCriteria.java org/carolinas/android/dir/model/WayFindingDirection.java org/carolinas/android/dir/model/WayFindingLocation.java org/carolinas/android/dir/model/WayFindingSubLocation.java org/carolinas/android/dir/util/Constants.java rx/internal/schedulers/NewThreadWorker.java
4	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/epic/patientengagement/homepage/itemfeed/webservice/items/ZeroStateFeedItem.java com/epic/patientengagement/todo/models/QuestionnaireSeries.java epic/mychart/android/library/utilities/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/americanwell/sdk/AWSDKApplication.java com/epic/patientengagement/core/utilities/DeviceUtil.java com/epic/patientengagement/core/utilities/file/FileChooserType.java com/epic/patientengagement/core/utilities/file/FileUtil.java epic/mychart/android/library/utilities/DeviceUtil.java org/carolinas/android/dir/util/DataUtils.java
6	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	org/carolinas/android/dir/util/FingerprintHandler.java
7	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	org/carolinas/android/dir/db/FavoritesDatabase.java
8	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 epic/mychart/android/library/customviews/PdfViewerActivity.java epic/mychart/android/library/utilities/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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
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/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
12	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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	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 epic/mychart/android/library/utilities/k.java
00013	Read file and put it into a stream	file	com/epic/patientengagement/pdfviewer/utilities/FileUtils.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 org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java org/altbeacon/beacon/service/MonitoringStatus.java org/altbeacon/beacon/service/ScanState.java org/carolinas/android/dir/util/Base64.java org/simpleframework/xml/core/Persister.java
00202	Make a phone call	control	epic/mychart/android/library/utilities/k.java org/carolinas/android/dir/ClinicalTrialsSummaryActivity.java org/carolinas/android/dir/view/PracticeFragment.java
00203	Put a phone number into an intent	control	epic/mychart/android/library/utilities/k.java org/carolinas/android/dir/ClinicalTrialsSummaryActivity.java org/carolinas/android/dir/view/PracticeFragment.java
			com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/epic/patientengagement/authentication/login/activities/SAMLLoginActivity.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

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/epic/patientengagement/core/extensibility/ExtensibilityLaunchManager.java com/epic/patientengagement/core/file/FileViewActivity.java com/epic/patientengagement/core/file/FileViewKt.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/epic/patientengagement/core/utilities/IntentUtil.java com/epic/patientengagement/core/utilities/WebUtil.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/DeepLinkManager.java epic/mychart/android/library/general/FDILauncherActivity.java epic/mychart/android/library/general/e.java epic/mychart/android/library/healthlinks/l.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 epic/mychart/android/library/welcomewizard/WelcomeWizardWebViewFragmentManager.java org/carolinas/android/dir/ClinicalTrialsSummaryActivity.java org/carolinas/android/dir/HomeScreenActivity.java org/carolinas/android/dir/JellyBeanWebViewActivity.java org/carolinas/android/dir/ProviderSearchActivity.java org/carolinas/android/dir/WebViewActivity.java org/carolinas/android/dir/view/PracticeFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/utilities/k.java org/carolinas/android/dir/ClinicalTrialsSummaryActivity.java org/carolinas/android/dir/view/PracticeFragment.java
00112	Get the date of the calendar event	collection calendar	epic/mychart/android/library/healthlinks/HealthDataSyncService.java epic/mychart/android/library/healthlinks/b.java epic/mychart/android/library/healthlinks/k.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 org/carolinas/android/dir/HomeScreenActivity.java org/carolinas/android/dir/JellyBeanWebViewActivity.java org/carolinas/android/dir/ProviderDetailActivity.java org/carolinas/android/dir/ProviderSearchResultsActivity.java org/carolinas/android/dir/WayFindingDestinationActivity.java org/carolinas/android/dir/WayFindingDirectionsActivity.java org/carolinas/android/dir/WayFindingStartingPointActivity.java org/carolinas/android/dir/WebViewActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java
00030	Connect to the remote server through the given URL	network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java
00109	Connect to a URL and get the response code	network command	com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java
00022	Open a file from given absolute path of the file	file	com/americanwell/sdk/AWSDKApplication.java com/epic/patientengagement/core/utilities/DeviceUtil.java com/jakewharton/picasso/OkHttp3Downloader.java epic/mychart/android/library/customviews/VideoPlayerActivity.java epic/mychart/android/library/messages/Attachment.java org/altbeacon/beacon/service/ScanState.java
00096	Connect to a URL and set request method	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00153	Send binary data over HTTP	http	epic/mychart/android/library/utilities/g.java
00204	Get the default ringtone	collection	com/americanwell/sdk/activity/GuestVideoActivity.java com/americanwell/sdk/activity/VideoVisitActivity.java
00102	Set the phone speaker on	command	com/americanwell/sdk/activity/GuestVideoActivity.java com/americanwell/sdk/activity/VideoVisitActivity.java
00056	Modify voice volume	control	com/americanwell/sdk/activity/GuestVideoActivity.java com/americanwell/sdk/activity/VideoVisitActivity.java
00018	Get JSON object prepared and fill in location info	location collection	org/carolinas/android/dir/manager/FacilityManager.java
00115	Get last known location of the device	collection location	org/carolinas/android/dir/manager/FacilityManager.java
00113	Get location and put it into JSON	collection location	org/carolinas/android/dir/manager/FacilityManager.java
00016	Get location info of the device and put it to JSON object	location collection	epic/mychart/android/library/location/models/MonitoredForArrivalAppointment.java org/carolinas/android/dir/manager/FacilityManager.java
00125	Check if the given file path exist	file	com/epic/patientengagement/core/pdfviewer/PdfFragment.java com/epic/patientengagement/pdfviewer/PdfViewerFragment.java
00072	Write HTTP input stream into a file	command network file	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java
00177	Check if permission is granted and request it	permission	com/epic/patientengagement/core/permissions/PermissionUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	epic/mychart/android/library/utilities/i.java org/carolinas/android/dir/util/Base64.java
00024	Write file after Base64 decoding	reflection file	epic/mychart/android/library/messages/Attachment.java
00191	Get messages in the SMS inbox	sms	com/epic/patientengagement/core/file/FileViewKt.java
00031	Check the list of currently running applications	reflection collection	com/americanwell/sdk/activity/AbsVideoActivity.java
00183	Get current camera parameters and change the setting.	camera	com/vidyo/LmiDeviceManager/LmiVideoCapturerInternal.java com/vidyo/LmiDeviceManager/LmiVideoCapturerManager.java
00094	Connect to a URL and read data from it	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/healthlinks/d.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
00014	Read file into a stream and put it into a JSON object	file	org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.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
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	14/25	android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECORD_AUDIO, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.VIBRATE, android.permission.ACCESS_WIFI_STATE, android.permission.GET_TASKS
Other Common Permissions	6/44	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.BROADCAST_STICKY, android.permission.CALL_PHONE, android.permission.FOREGROUND_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
www.wakehealth.edu	ok	**IP:** 52.168.33.204 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **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
portal.vidyo.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
my.atriumhealth.org	ok	**IP:** 208.56.200.81 **Country:** United States of America **Region:** Massachusetts **City:** Andover **Latitude:** 42.648373 **Longitude:** -71.161453 **View:** Google Map
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
schemas.xmlsoap.org	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.floyd.org	ok	**IP:** 20.231.3.20 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
buildserver03.americanwell.com	ok	No Geolocation information available.
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
www.google.com	ok	**IP:** 142.250.74.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
inside.asp	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
schemas.datacontract.org	ok	**IP:** 207.46.232.160 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
navicent.orcarestra.com	ok	**IP:** 52.1.18.115 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
atriumhealth.org	ok	**IP:** 13.107.246.41 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
careers.atriumhealth.org	ok	**IP:** 104.17.128.199 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bit.ly	ok	**IP:** 67.199.248.11 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **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
haiku-push-notifications.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
customurl.com	ok	**IP:** 15.197.204.56 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
webservices.atriumhealth.org	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
myatriumhealth.iqhealth.com	ok	**IP:** 159.140.207.154 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.154167 **Longitude:** -94.546669 **View:** Google Map
mycarolinas.iqhealth.com	ok	**IP:** 159.140.207.154 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.154167 **Longitude:** -94.546669 **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
ehealthservices-dev.atriumhealth.org	ok	**IP:** 159.60.151.62 **Country:** Netherlands **Region:** Zuid-Holland **City:** The Hague **Latitude:** 52.076672 **Longitude:** 4.298610 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ehealthservices.atriumhealth.org	ok	**IP:** 159.60.151.62 **Country:** Netherlands **Region:** Zuid-Holland **City:** The Hague **Latitude:** 52.076672 **Longitude:** 4.298610 **View:** Google Map
www.carolinashealthcare.org	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
mychart.et0905.epichosted.com	ok	**IP:** 208.56.200.81 **Country:** United States of America **Region:** Massachusetts **City:** Andover **Latitude:** 42.648373 **Longitude:** -71.161453 **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
api-ssl.bitly.com	ok	**IP:** 67.199.248.20 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
www.twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
mobilepreview.epic.com	ok	**IP:** 199.204.56.221 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
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
s3.amazonaws.com	ok	**IP:** 16.15.187.143 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.409912 **Longitude:** -122.160400 **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
www.mychart.org	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
altbeacon.github.io	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.atriumhealth.org	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
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
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mychart-np.et0905.epichosted.com	ok	**IP:** 45.42.32.200 **Country:** United States of America **Region:** Wisconsin **City:** Verona **Latitude:** 42.990845 **Longitude:** -89.568443 **View:** Google Map

EMAILS

EMAIL	FILE
example@example.com myatriumhealth@atriumhealth.org	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AltBeacon		https://reports.exodus-privacy.eu.org/trackers/219
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"Branding_Google_Client_Secret" : "CsGDRovrtq5uQfVSV2yTCKk5"
"Branding_MenuApplicationKey" : "CAROLINASHEALTHCAREAPP"
"awsdk_ending_visit_permissions_guest" : "%1$s"
"bitly_key" : "R_07b27400c45b55d6352950f569e9067b"
"bitly_username" : "carolinas2011"
"firebase_database_url" : "https://fifth-liberty-89719.firebaseio.com"
"google_api_key" : "AIzaSyBv776FvkVLGKyvr4AR_IFvkThhUx18A2s"
"google_crash_reporting_api_key" : "AIzaSyBv776FvkVLGKyvr4AR_IFvkThhUx18A2s"
"map_api_debug_key" : "0sdJPMr4nvcp67CaW80u6BFtWKepMPZuBH_UmkA"
"map_api_production_key" : "AIzaSyDhdGgfxV4t09iaSCywCqrFVuxFQJSwuXI"
"password" : "Password"
"test_alt_password" : "Password1"
"test_alt_username" : "kensmith"
"test_feed_password" : "Password1"

POSSIBLE SECRETS
"test_feed_username" : "vapgar"
"test_password" : "Password1"
"test_sdk_client_key" : "sdktest"
"test_sdk_user_auth_key" : "katesmitty"
"test_username" : "katesmith"
"wp_key_preferences_about" : "wp_preference_about"
"wp_key_preferences_allow_all_locales" : "wp_key_preferences_allow_all_locales"
"wp_key_preferences_app_review_header" : "wp_preferences_app_review_header"
"wp_key_preferences_app_review_mode_switch" : "wp_key_preferences_app_review_mode_switch"
"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"

POSSIBLE SECRETS
"wp_key_preferences_custom_server_switch" : "wp_preference_custom_server_switch"
"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!"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
23456789abcdefghjkmnpqrstvwxyz

PLAYSTORE INFORMATION

Title: MyAtriumHealth

Score: 4.372263 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** org.carolinas.android.dir

Developer Details: Atrium Health, Atrium+Health, None, http://www.atriumhealth.org, MobileApps@atriumhealth.org,

Release Date: Jul 28, 2011 **Privacy Policy:** Privacy link

Description:

Get all your health info in one convenient place. With the MyAtriumHealth app, you can manage your health and wellness – as well as everyone who counts on you. You can: Manage care for yourself and everyone who counts on you all in one place Find a doctor or location near you View maps and driving directions Save favorite locations for quick access Schedule appointments and get medications for everyone who depends on you Message your providers and care team Pay your bill Check lab and test results Upload health and fitness data, including data from the Health Connect app, when enrolled in self-tracking programs

SCAN LOGS

Timestamp	Event	Error
2025-09-01 15:01:48	Generating Hashes	OK
2025-09-01 15:01:48	Extracting APK	OK

2025-09-01 15:01:48	Unzipping	OK
2025-09-01 15:01:48	Parsing APK with androguard	OK
2025-09-01 15:01:49	Extracting APK features using aapt/aapt2	OK
2025-09-01 15:01:49	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 15:01:52	Parsing AndroidManifest.xml	OK
2025-09-01 15:01:52	Extracting Manifest Data	OK
2025-09-01 15:01:52	Manifest Analysis Started	OK
2025-09-01 15:01:52	Reading Network Security config from wp_network_security_config.xml	OK
2025-09-01 15:01:52	Parsing Network Security config	OK
2025-09-01 15:01:52	Performing Static Analysis on: MyAtrium (org.carolinas.android.dir)	OK
2025-09-01 15:01:54	Fetching Details from Play Store: org.carolinas.android.dir	OK

2025-09-01 15:01:55	Checking for Malware Permissions	OK
2025-09-01 15:01:55	Fetching icon path	OK
2025-09-01 15:01:55	Library Binary Analysis Started	OK
2025-09-01 15:01:55	Reading Code Signing Certificate	OK
2025-09-01 15:01:56	Running APKiD 2.1.5	OK
2025-09-01 15:01:58	Detecting Trackers	OK
2025-09-01 15:02:05	Decompiling APK to Java with JADX	OK
2025-09-01 15:02:36	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 15:02:36	Decompiling classes6.dex with JADX	OK
2025-09-01 15:02:45	Decompiling classes2.dex with JADX	OK
2025-09-01 15:02:50	Decompiling classes4.dex with JADX	OK

2025-09-01 15:02:59	Decompiling classes.dex with JADX	OK
2025-09-01 15:03:08	Decompiling classes3.dex with JADX	OK
2025-09-01 15:03:16	Decompiling classes5.dex with JADX	OK
2025-09-01 15:03:21	Decompiling classes7.dex with JADX	OK
2025-09-01 15:03:24	Decompiling classes6.dex with JADX	OK
2025-09-01 15:03:33	Decompiling classes2.dex with JADX	OK
2025-09-01 15:03:38	Decompiling classes4.dex with JADX	OK
2025-09-01 15:03:47	Decompiling classes.dex with JADX	OK
2025-09-01 15:03:57	Decompiling classes3.dex with JADX	OK
2025-09-01 15:04:05	Decompiling classes5.dex with JADX	OK
2025-09-01 15:04:10	Decompiling classes7.dex with JADX	OK

2025-09-01 15:04:13	Converting DEX to Smali	OK
2025-09-01 15:04:13	Code Analysis Started on - java_source	OK
2025-09-01 15:04:19	Android SBOM Analysis Completed	OK
2025-09-01 15:04:25	Android SAST Completed	OK
2025-09-01 15:04:25	Android API Analysis Started	OK
2025-09-01 15:04:30	Android API Analysis Completed	OK
2025-09-01 15:04:31	Android Permission Mapping Started	OK
2025-09-01 15:04:39	Android Permission Mapping Completed	OK
2025-09-01 15:04:40	Android Behaviour Analysis Started	OK
2025-09-01 15:04:46	Android Behaviour Analysis Completed	OK
2025-09-01 15:04:46	Extracting Emails and URLs from Source Code	OK

2025-09-01 15:04:52	Email and URL Extraction Completed	OK
2025-09-01 15:04:52	Extracting String data from APK	OK
2025-09-01 15:04:52	Extracting String data from Code	OK
2025-09-01 15:04:52	Extracting String values and entropies from Code	OK
2025-09-01 15:05:00	Performing Malware check on extracted domains	OK
2025-09-01 15:05:08	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.