

CTS Testing Services Inc

1. Intro
   1. What to say in intro

(scene: CTS logo)

Welcome to the Early Access Alpha release of the CTS Testing Services Covid Test Tracking Application. Our first iteration of this product is geared towards Colleges and Universities and will ship with all the functionality required for these institutions to implement weekly testing policies for student and staff.

(scene: intro\_cts\_np)

The CTS Testing Services Covid Test Tracking Application allows colleges and universities to implement weekly testing policies without being inundated with the logistics of processing and storing test results as well as the struggles of maintaining data privacy and industry standards regarding storing personal medical information.

(scene, midway thru, intro\_sec\_1,2)

We ensure our systems meet the requirements set by modern healthcare privacy laws regarding the maintaining of user accounts and storage of private medical data so your organization can externalize their data privacy risks and focus on education and getting through this pandemic.

The software is presented in the form of a cloud-based service which is accessible from any browser whether it be on a windows, mac, iphone, or android device. The CTS Testing Services Company maintains the web server and database and provides a web gateway to be used by the school’s staff and students.

(scene, roles/permissions)

The software is built around “roles” such that each user that is entered into the system will be assigned a role which determines what sort of access they have to the system. Each user role has the bare minimum access to the system that is required for their function and the roles of the users are segmented in such a way to ensure that each test follows a certain process. A user trying to get to a page they do not have access to will result in a “This page is unavailable” message and a prompt redirect to the login screen.

(scene: results legend)

(scene: doctor\_sign legend)

Tests are signed by two separate medical professionals to ensure accuracy, the results are only accessible to the medical staff and users after they’ve verified their identity, and communications regarding results are sent to specific verified parties to be determined by the customer that purchases the product (for example sending positive results to the registration department to place holds on student accounts).

An example of this is that The medical staff responsible for performing the tests on the samples has access to edit the results of the test to be positive or negative but only the user with the doctor level of permissions has the ability to sign a test which triggers an email notification to be sent to the notifying parties.

End intro (end video 1)

Begin features (part 2)

In the second part of this video presentation we will be going over all the core features and functions that the product offers at launch. The feature breakdown will show in detail the functions that are available to each separate level of user access ------using test or fake accounts that have been created. Demonstrations of these functions will be performed using these fake accounts.

The first quote unquote user we are going to look at will be the “non” user. A “non” user refers to a user without an active logon session – basically, someone who has accessed the public landing page of the product. The publicly accessible features of the product include only the login itself as well as a password reset function. When a user logs in, they are automatically redirected to the appropriate dashboard page based on their permission level. To demonstrate this login, I will log in with a sample patient user, whose credentials I’ve prefilled into the login screen. We’ve logged into an account that has the permission level of a Patient user, which is our first user we will explain in the next section. For now I will sign out and demonstrate the password reset function.

As for the password reset function, in the current implementation of the product any user can change their own password by verifying their username and their social security number. Future iterations of the product will expand this to only allow passwords to be reset after an email verification. To demonstrate the password reset I will reset this fake user’s password and then show how I can log in with newly reset password.

Next we are going to look at the feature-set available to the patient user. The patient level of user access is the most restricted level of access that exists in the product – patients can only do 2 main functions which are viewing their personal test results as well as viewing their personal profile data. Let us log into a test patient user’s account and take a look again at our patient dashboard page.

When a patient dashboard is loaded, the database is queried based on the user’s newly created session data to extract the user’s recent test results and display them in a meaningful way in the table on the center of the screen. The user will see the results of their tests as either Negative, Positive, or Not Ready, depending on whether or not it has gone through the physician signage process.

The second function available to patients is the View Personal Info button. This button will query the database, again based on the user’s active session data, and retrieve the user’s personal profile information. Not all items inside their personal profile are shown, for example the user cannot see their unique USER ID nor their permission level, but the user can see their email verification status which is important because if a user’s email is not verified then result notification emails will not be sent to them.

Next, we are going to look at the feature-set available to the Vendor, or Employee, user. The employee user is one of the most important roles in our product because this is the user responsible for entering new patients and entering new test samples that are submitted during patient’s weekly tests. Let us log into an employee account and take a look at our employee dashboard.

Firstly, because of the nature of the employee’s role, the intention is that the employee will be performing their role from an ipad at the testing facility (ie, the library or classroom where students go to take their tests). For this reason, our employee demonstrations will be scaled to an ipad sized screen so we can more accurately represent the day to day role of the employee.

The employee user has 3 main functions which are registering patients, submitting tests, and searching for patients. Employees, and all users for that matter, can all participate in the weekly covid testing and therefore have access to their own version of the patient dashboard screen where they can view their own personal test results and ultimately will inherently have all the same permissions as a normal patient user would have.

The employee’s primary function will be entering new patient accounts and submitting test samples, so let’s look at examples of those processes.

The Patient Registration Form requires the following information be filled out in its entirety.

The username, which is the user’s login name, and is required to be an email address. The password, which is strictly set to only allow passwords that are HIPA compliant in length and complexity. First and last name. Social security number. Email address, and the employee will make it clear that this is the email that is used for result notification email purposes, and lastly, date of birth. I’ve prefilled in some information for a sample user we will create. Click.

Once a new patient is registered, a verification email is automatically sent to the user’s email listed in the email field. A flag on the patient’s profile, named “email\_verify” is set to 0 by default and is only set to 1 after the patient verifies their email using the link in the verification email. This flag is checked when results are finalized through the signage process and, if the patient’s email hasn’t been verified, it will not send an email to them with their results.

Let’s skip ahead briefly and use our employee’s search user function to look up our newly created user and check the email verification status. Click click. So we can see that the email is not verified. Let’s log into our fake patient’s email account and see how the email verification process works.

The email verification process uses a randomly generated token which is stored in a hidden field in the user profile table in the database. The token is filled into a URL which targets the email-verify script and processes the verification by checking to ensure that the link that was clicked contains the correct username and email token. Once the token is verified, the email is verified in the patient account. Once the email is verified, the hidden email token field is reset to NULL and further attempts to use the verification link will fail.

Let’s sign back into our test employee account and search that user one more time so we can verify the email verification has been completed and updated in the database.

If a patient loses their verification email, the employee can use the “Resend Verification Link” menu to resend the email. This causes the email token to be re-generated and sent in another link which, like before, once verification is successful the email token gets reset to NULL and the link will no longer work. Let’s try to click that verification email again and see what happens.

CUT VIDEO RESUME LATER for TEST SUBMIT and PERSONAL INFO

The secondary function of the employee will be the new test submission process. When a patient comes back to the testing facility they will be handed a small vial with a serial number on it where they deposit their saliva sample for testing. The employee’s role will be to submit the test using the patient’s username and the serial number on the vial. Once submitted, it is ready to be transported to the laboratory facility and tested by a laboratory technician, which triggers the first of our two-step result signage process.

Lastly, let’s show the employee’s “view personal test results” menu. As mentioned before, every user has access to this menu from their dashboard page so we won’t cover it again after this. Click open. When the employee user clicks the dashboard button, it loads a version of the patient dashboard that we’ve seen before. This patient dashboard automatically retrieves their recent test results and displays them in the table in the center of the screen. The patient dashboard also contains the View personal info button which, click, shows the employee’s personal info including their email verification status.

Once a patient account exists and a test sample of saliva has been submitted to the vendor and thus transported to the testing facility, the next person in our process steps up to complete their tasks. This user is the Laboratory user. Let’s log into our test/fake lab user dashboard and take a look. The lab user has very limited access compared to the employee user. The lab user does not work at the school, but rather is a member of an external or 3rd party testing company which is contracted by CTS. The lab user therefore does not need the ability to enter new patients nor to submit new tests. All the lab user does is process each vial and record the results as Positive or Negative. Lastly, of course, the lab user can view their own personal test results, if they’ve ever submitted any samples to the testing facility (the school).

The lab user starts their day by retrieving all the test samples that were provided on a particular day of testing and then searching that date in their dashboard page. This will query the database and give them a list of all the tests that were submitted on that day. Right from their dashboard page, the lab user modifies the results of the test by first verifying the serial number on the vial with the serial number presented in the system, clicking the radio box indicating the result, and verifying the TEST ID of the test, which is a unique key associated with each and every test sample. The lab user doesn’t know that UID 4 is the new user we just created. Their only job is to record the status of each vial. So let’s say this test was Negative. The lab user would check the Negative radio box and enter the corresponding TEST ID which is 2 and press submit. By searching for the same day again on the lab dashboard, we can see the result has been updated. One thing we also see is the status of the result signature, which can only be provided by a doctor.

The 2nd step in the 2 step testing process now requires that the test results be looked over by a medical doctor and given a digital signature verifying their results. The doctor user has an identical dashboard to the lab user. The only difference is that the doctor has the ability to adjust the signage status of a test as well as a result. The doctor queries the same date as the lab user, acknowledges the results are Negative, Marks it as Signed, and then verifies the TEST ID.

If the patient email account has been verified the doctor will show a message indicating that the results have been sent to the patient’s email. Let us flip over to our fake patient’s email and view these results for ourselves.

The final level of user permission that our product offers is the Super User, or Administrator, level of access. The super user or admin will be someone at your organization who is responsible for maintaining the system and the accounts. This could be your help desk technician who fields calls related to the system, for example users who forgot their usernames, lab technicians who made a mistake registering a test result, employees who call in stating they entered the wrong information for a user account and need to edit the account, etc. The admin user has all the permissions that all other users have, combined, plus the ability to edit user data which no other user has the ability to do. The one thing the admin user can NOT do is digitally sign a test.

So the admin has BLAH BLAH BLAH show them in and out in and out one at a time bing bang

1. Go over all core features and the function of every user
   1. The “non” user (no active session, logged into any account)
      1. Login
      2. Reset password
   2. Vendor
      1. Register new Patient (counter service)
         1. Newly entered users are created with patient level permission
      2. Register new test
      3. View a user
         1. Resend user’s verification email
      4. View Personal Test Results
         1. View Personal Info (personal profile)
      5. Log out
   3. Lab
      1. Edit test samples
         1. Can only edit results, cannot sign tests
      2. View Personal Test Results
         1. View Personal Info (personal profile)
   4. Doctor
      1. Edit test samples
         1. Can edit results and sign tests
         2. When results are signed, email automatically sent (if user verified email)
   5. Patient
      1. View Personal Test Results
      2. View Personal Info (personal profile)
   6. Admin
      1. Register new User
         1. Admin can edit the user’s permission level
      2. Edit user
      3. Submit a new test
      4. Edit a test
         1. Can only change results, cannot sign as a doctor
      5. View Personal Test Results
         1. View Personal Info (personal profile)
2. Complete simulation of the testing process and each user’s interaction
   1. Student walks into campus library where a fellow peer is acting as the “vendor”
   2. Vendor uses iPad to enter the student’s information to create their account.
      1. Vendor walks through the form and enter information as the patient gives it to them over the counter
      2. The vendor tells the patient that their username will be their email address and that whatever email they enter will be the email that they receive their results notifications on.
      3. Vendor tells patient that they must ensure they verify their email before they will receive any emails with their results
      4. A verification email is sent to the user’s email address
      5. User is given a pre-generated password that the vendor creates, vendor tells user how they can log on and change their password to something personalized
   3. Vendor uses iPad to enter the student’s test sample and then walks student through the saliva collection process
      1. Vendor grabs a test vial from their inventory and takes down the serial number in the form as well as the new patient’s username
      2. Vendor explains saliva collection process to patient and then hands over vial
      3. Student performs test and puts vial in the collection tray
      4. The test sample collection tray is picked up by a transportation company and brought to the lab facility
   4. Lab user gets the tray of samples and tests each one and manually inputs the results of the tests into the CTS testing services software
      1. Lab user logs in to his dashboard and searches tests for that day’s date
      2. Lab user performs test of sample and enters result into CTS software
   5. Lab user reports results to an onsite physician for signing
      1. Doctor logs into his dashboard and searches tests for that day’s date (same view as lab user)
      2. Doctor user confirms results of test sample and Signs test
      3. Once test is signed, an email with the results is sent to the patient’s email address automatically (assuming that the patient verified their email)
3. We can conclude with some examples of niche use cases
   1. User calls the testing site and reports they forgot their username or cannot access their account
      1. Employee can search the account via email and report the logon information to the user
      2. Patient can recover/reset their password by entering their username and social security number into the password recovery menu
   2. User calls the testing site and would like to change their email address on file
   3. Employee emails admin user to edit the user account and then resend verification email
4. We can also conclude with some info about upcoming features
   1. Password reset via email verification
   2. Inventory control system for test vials (new db table for vial inventory for better vial tracking and validation)
   3. More front end overhauls
   4. Analytical data and reporting (print report of the results growth/shrinkage over certain time frame)