



**CMS 2010 BI-REGIONAL MEDICARE HEALTH PLAN COMPLIANCE  
CONFERENCE**

**Boston & New York – Serving Our Beneficiaries Together**

Verbatim Transcript  
Security and Privacy  
Eric Brown, J.D.

>> WE SCHEDULED YOU TO LISTEN TO  
POINTERS ABOUT SECURITY AND  
PRIVACY. AND WE HAVE WITH US  
ERIC BROWN, WHO IS FROM THE  
OFFICE FOR CIVIL RIGHTS, WHICH  
IS THE AGENCY CHARGED WITH THE  
OVERSIGHT AND MONITORING AND--I  
WAS GOING TO SAY PROSECUTION,  
BUT THAT'S A LITTLE STRONG.  
HE'LL TELL YOU WHAT THEY DO.  
BUT IT IS THEIR RESPONSIBILITY  
TO MAKE SURE THAT MEDICARE  
BENEFICIARIES ARE NOT TAKEN  
ADVANTAGE OF BY DEVIOUS PEOPLE  
AND THAT THEIR SECURITY--THE  
SECURITY AND PRIVACY OF THEIR  
PERSONAL INFORMATION IS  
MAINTAINED. ERIC BROWN IS THE  
SUPERVISORY EQUAL OPPORTUNITY  
SPECIALIST AT THE U.S.  
DEPARTMENT OF HEALTH IN SERVICES  
IN THE OFFICE FOR CIVIL RIGHTS.  
HE'S RESPONSIBLE FOR OVERSEEING  
INVESTIGATIONS AND COMPLIANCE  
REVIEWS CONCERNING CIVIL RIGHTS  
DISCRIMINATION AND THE HIPAA

PRIVACY AND SECURITY RULES. HE IS THE COORDINATOR OF THE FEDERAL CIVIL RIGHTS ROUNDTABLE FOR THE REGION. PRIOR TO JOINING THE OFFICE FOR CIVIL RIGHTS, HE WAS A--THE CRIMINAL COURT DIRECTOR AT CASES, INCORPORATED. HE'S BEEN FEATURED IN THE WHO'S WHO AMONG EXECUTIVE AND PROFESSIONALS, AND IS AN HONORS GRADUATE OF OHIO STATE UNIVERSITY'S COLLEGE OF LAW. PLEASE WELCOME ERIC BROWN.

>> GOOD AFTERNOON, EVERYONE. I PREPARED SOME REMARKS; HOWEVER, I DON'T IF IT'S GOING TO TAKE A WHOLE HALF AN HOUR TO GET THROUGH WHAT I WANT TO BECAUSE WE HAVE A BREAKOUT SESSION, AS THE YOUNG LADY SAID THIS AFTERNOON, FOR A WHOLE HOUR. WE'RE GOING TO DO TWO SESSIONS ON BOTH, THE SECURITY RULE, THE PRIVACY RULE AS WELL AS THE BREACH NOTIFICATION RULE. SO I THINK YOU'LL GET MORE OUT OF THIS PLENARY SESSION IF I GIVE YOU JUST A BRIEF OVERVIEW OF WHAT WE DO IN THE OFFICE, WHY WE DO WHAT WE DO, AND HOW WE DO WHAT WE DO. I'M GOING TO LEAVE ENOUGH TIME FOR YOU TO MAX SOME BASIC QUESTION. BUT WE'LL GET INTO THESE RULES IN MORE DETAIL THIS AFTERNOON. THE OFFICE OF CIVIL RIGHTS IS RESPONSIBLE FOR ENFORCING VARIOUS FEDERAL CIVIL RIGHTS LAWS. THAT'S WHAT WE DO CHIEFLY, ENFORCE THE CIVIL RIGHTS LAWS. IT WAS NOT UNTIL APRIL OF 2003 WHEN WE WERE GIVEN JURISDICTION TO ENFORCE THE HIPAA PRIVACY RULE ONLY. LAST YEAR, WE WAS GIVEN JURISDICTION TO ENFORCE THE SECURITY RULE AS WELL AS THE PRIVACY RULE. AND THEN SEPTEMBER OF LAST YEAR, WE GOT JURISDICTION TO ENFORCE THE BREACH NOTIFICATION RULE. SO WHAT I'M GOING TO DO IS REFER TO

HIPAA, BUT THE LAWS THAT I'M REFERRING TO UNDER HIPAA CORRELATES TO THE PRIVACY RULE, SECURITY RULE, AND THE BREACH NOTIFICATION RULE. AND LATER-ON THIS AFTERNOON, WE'LL DISCUSS THOSE THREE RULES IN MORE DETAIL. THE CIVIL RIGHTS LAWS THAT WE ENFORCE HELP TO PROTECT YOU FROM UNFAIR TREATMENT AND/OR DISCRIMINATION BECAUSE OF YOUR RACE, COLOR, NATIONAL ORIGIN, AGE, DISABILITY, AND IN SOME CASES, SEX AND RELIGION. WE ENFORCE TITLE TWO OF AMERICAN WITH DISABILITIES ACT, SECTION 504, THE REHABILITATION ACT, OF COURSE, TITLE 6, THE FEDERAL CIVIL RIGHTS ACT OF 1964, AND VARIOUS OTHER STATUS UNDER THE EDUCATION AMENDMENTS ACT. WITH RESPECT TO HIPAA, WE ONLY ENFORCE THE SECURITY RULE, THE PRIVACY RULE, AND THE BREACH NOTIFICATION RULE. BUT AS SOME OF YOU MAY BE AWARE, THERE'S A LOT OF OTHER RULES UNDER THE HIPAA LAW. AND HIPAA IS AN ACRONYM. FOR THOSE WHO DON'T KNOW, I'LL JUST SAY IT AGAIN; IT STANDS FOR THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT. WE FREQUENTLY SEE IN OUR OFFICE PEOPLE REFER TO IT ALL SORTS OF NAME; THE ACRONYM IS H-I-P-P-A, AS IF IT'S ABBREVIATION FOR HIPPOPOTAMUS, WHEN IN FACT, IT'S NOT; IT'S TWO AS AND ONE P. THAT'S SOMETHING THAT, YOU KNOW, FOR SOME REASON BUGS ME WHEN I SEE THAT. AS I SAID EARLIER, THE WENT INTO EFFECT IN APRIL OF 2003, EXACTLY APRIL 14TH OF 2003. AND THAT'S WITH RESPECT TO THE HIPAA PRIVACY RULE AND IT GOVERNS HOW COVERED ENTITIES--IN THIS CASE, WHEN WE SAY COVERED ENTITIES, THE RULE DEFINES THOSE ENTITIES AS HEALTHCARE PROVIDERS, HEALTH

PLANS, AND HEALTHCARE CLEARING HOUSES. SO A LOT OF PEOPLE BELIEVE THAT BECAUSE HIPAA GOVERNS THE PRIVACY OF HEALTH INFORMATION, IT APPLIES IN ALL CONTEXTS AND THAT'S NOT THE CASE. ONLY WITH RESPECT TO PRETTY MUCH HEALTHCARE, SO IF YOU HAVE A SITUATION WHERE YOUR PRIVACY--EVEN IF IT'S YOUR HEALTH INFORMATION, BUT PRIVACY BEING VIOLATED IN THE EMPLOYMENT CONTEXT, THE HIPAA PRIVACY RULE DOES NOT APPLY TO THAT. AND LATER THIS AFTERNOON, WE'RE GOING TO DISCUSS SOME OF THE DISTINCTIONS BETWEEN SOME OF THE OTHER STATUS THAT GOVERN PRIVACY IN OTHER CONTEXT SUCH AS EMPLOYMENT AND EDUCATION. BUT, YEAH, I JUST WANT TO MAKE IT CLEAR AT THE OUTSET THAT HIPAA ONLY APPLIES TO THE CONTEXT OF HEALTHCARE. AND IN THIS INSTANCE, WE ALSO REFER TO HEALTH INSURANCE AS WELL. IT ONLY REFERS TO INFORMATION THAT'S CONTAINED IN A DESIGNATED RECORD SET. IN LAYMAN'S TERMS, THAT'S FOR THE MOST PART YOUR MEDICAL RECORDS. SO ANYTHING OUTSIDE OF THE MEDICAL RECORDS OR THE DESIGNATED RECORD SET, HIPAA DOES NOT APPLY TO. SO ANOTHER SITUATION THAT FREQUENTLY COMES UP IN OUR OFFICE IS SOMEONE WILL FILE A COMPLAINT INDICATING THAT THEY WORK FOR A HOSPITAL, MAYBE NURSE, AND SHE WAS REQUIRED AS PART OF EMPLOYMENT TO GET TESTING FOR TB OR SOME OTHER COMMUNICABLE DISEASE. AND PERHAPS SHE TESTED POSITIVE AND THAT INFORMATION WAS SHARED WITH HER COWORKERS. SHE THEN ALLEGES THAT HER PRIVACY RIGHTS UNDER HIPAA WERE VIOLATED. THAT'S A FREQUENT COMPLAINT THAT WE GET IN THE OFFICE; AND IN THAT

SITUATION, HIPAA DOES NOT APPLY. BECAUSE THE INFORMATION THAT WAS GENERATED WAS GENERATED WITHIN THE CONTEXT OF HER EMPLOYMENT, THE HIPAA PRIVACY RULE PRETTY MUCH IS BARRED FROM ADDRESSING THAT SITUATION. IF SHE WAS A PATIENT AT THE HOSPITAL AND THEN THE INFORMATION WAS DISCLOSED, THEN HIPAA WOULD APPLY. SO, AGAIN, THERE'S SOME SUBTLE DIFFERENCES AND DISTINCTIONS AND WE'LL DISCUSS THEM IN GREATER THIS AFTERNOON. BUT I JUST--YOU KNOW, FOR THOSE WHO MAY NOT BE ATTENDING THE WORKSHOP, I WANT TO GET AS MUCH INFORMATION OUT THERE ABOUT THE HIPAA PRIVACY RULE AS POSSIBLE SO THAT YOU CAN THIS BACK AND SHARE IT WITH YOUR COLLEAGUES AND SOME OF THE STAFF THAT YOU SUPERVISE. THE GOALS OF THE PRIVACY RULE ARE SEVERAL. ONE IS THE RULE WAS PROMULGATED TO GIVE INDIVIDUALS MORE RIGHTS TO THEIR HEALTH INFORMATION. AND THAT'S YOU KNOW THE BASIC PREMISE BEHIND THE HIPAA PRIVACY RULE. IT WAS NOT TO IMPEDE THE FREE FLOW OF INFORMATION. SO AGAIN, YOU HAVE SITUATIONS WHERE A DOCTOR WANTS TO COMMUNICATE SOME INFORMATION TO A COLLEAGUE, AND A PATIENT MAY SAY, "WELL, YOU KNOW, THIS IS A SECOND OPINION AND I DON'T WANT THIS INFORMATION SHARED WITH MY PRIMARY CARE PHYSICIAN." HOWEVER, WHAT WAS LEARNED DURING THE COURSE OF THAT SECOND OPINION IS RELEVANT AND IMPORTANT TO THE PATIENT'S OVERALL HEALTH, AND SO THE DOCTOR SHARES IT MUCH TO THE CHAGRIN OF THE PATIENT. WELL, UNDER HIPAA, THAT'S A PERMISSIBLE DISCLOSURE IN USE OF THE PATIENT'S PROTECTED HEALTH INFORMATION BECAUSE AGAIN IN THE PREAMBLE OF THE HIPAA PRIVACY

RULE, IT CLEARLY INDICATES THAT IT WAS NOT INTENDED WHEN THE RULE WAS ENACTED TO IMPEDE THE FREE FLOW OF INFORMATION TO PROTECT THE HEALTH OF THE PATIENT. AND AGAIN, WE'LL GET INTO SOME MORE DISCUSSIONS LATER ON ABOUT THAT. THE SECOND GOAL OF THE PRIVACY RULE WAS TO ESTABLISH PERMITTED AND REQUIRED USES IN DISCLOSURES OF PROTECTED HEALTH INFORMATION. AND YOU'RE GOING TO HEAR THIS AFTERNOON THE TERM "PROTECTED HEALTH INFORMATION" OR PHI, DISCUSSED FREQUENTLY. AND WHAT WE MEAN WHEN WE SAY PROTECTED HEALTH INFORMATION IS ANY INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION. SO THAT COULD BE NOT ONLY A PERSON'S NAME, BUT THEIR SOCIALLY NUMBER, THEIR DATE OF BIRTH, AN ADDRESS, ANYTHING THAT COULD BE USED TO ASSOCIATE OR DETECT WHO HEALTH INFORMATION IS RELATED TO IS CONSIDERED INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION. AND WE HAVE SOME INTERESTING EXAMPLES ABOUT HOW COMPLAINTS COME ABOUT JUST ON THAT ISSUE ALONE AS WELL. ANOTHER GOAL OF THE PRIVACY RULE AS WELL AS A SECURITY RULE, I'M GOING TO, YOU KNOW, OFTENTIMES, REFER TO THE PRIVACY RULE BUT THE INFORMATION THAT I'M DISCUSSING ALSO IS APPLICABLE TO THE SECURITY RULE. ANOTHER GOAL OF BOTH OF THOSE RULES ARE TO ESTABLISH REQUIRED SAFEGUARDS TO PROTECT THE PRIVACY OF PROTECTED HEALTH INFORMATION. WITH RESPECT TO THE PRIVACY RULE, WE'RE TALKING ABOUT, FOR THE MOST PART, ELECTRONIC MEDICAL RECORDS AND PAPER RECORDS WHEN WE TALK ABOUT PROVIDING SAFEGUARDS TO PROTECT THE PRIVACY OF PROTECTED HEALTH INFORMATION. WITH RESPECT TO

THE SECURITY RULE, WE'RE ONLY TALKING ABOUT ELECTRONIC HEALTH INFORMATION. SO THERE'S A DISTINCTION BETWEEN THOSE TWO RULES. YOU CAN, IN ONE INSTANCE, BE IN VIOLATION OF THE PRIVACY RULE BUT NOT THE SECURITY RULE. AND AGAIN, WE'LL GET INTO SOME OF THE NUANCES ABOUT HOW THAT CAN COME ABOUT. ANOTHER GOAL OF BOTH OF THOSE RULES IS TO HOLD VIOLATORS OF PATIENT'S PRIVACY RIGHTS ACCOUNTABLE BY REQUIRING CORRECTIVE ACTIONS IN SOME INSTANCES, AND CIVIL AND CRIMINAL PENALTIES IN OTHER INSTANCES. THE GOAL OF OUR OFFICE CURRENTLY AND PERHAPS FOR THE LAST SEVEN YEARS WITH RESPECT TO COMPLAINTS THAT WE RECEIVE IS TO ENGAGE IN VOLUNTARY RESOLUTION OF THOSE COMPLAINTS. IT WAS A COLLABORATIVE POSTURE THAT THE OFFICE HAD TAKEN. SO, SELDOM, AND I ONLY CAN THINK OF MAYBE TWO OR THREE INSTANCES WHERE THE OFFICE ACTUALLY INVESTIGATED A COMPLAINT, DETERMINED THAT A COVERED ENTITY WAS NOT IN COMPLIANCE AND THEN ACTUALLY SOUGHT EITHER CRIMINAL PENALTIES OR CIVIL MONEY PENALTIES. IN PART, I BELIEVE THAT WAS THE CASE BECAUSE THE LAST ADMINISTRATION WAS--THIS IS BEING RECORDED--THE LAST ADMINISTRATION WAS INTERESTED IN ENSURING THAT COVERED ENTITIES WAS NOT PUT OUT OF BUSINESSES AND THAT THEY WERE THERE TO ASSIST THE COMMUNITY, AND THAT THE FUNDING FOR THOSE COVERED ENTITIES WERE NOT PLACED IN JEOPARDY. AND I CAN UNDERSTAND TO SOME EXTENT THAT THAT WAS TO ENSURE THAT THOSE COMMUNITIES WITH LIMITED RESOURCES DID NOT LOSE THOSE SORTS OF SERVICE

PROVIDERS BECAUSE OF VIOLATIONS OF THE PRIVACY AND/OR THE SECURITY RULE. HOWEVER, THERE HAD BEEN TIMES WHERE CERTAIN COVERED ENTITIES REPEATEDLY ENGAGED IN CERTAIN VIOLATIONS OVER AND OVER AND OVER AGAIN. AND I BELIEVE THAT THE ONLY EFFECTIVE DETERRENT IN THOSE INSTANCES WERE PERHAPS TO RATCHET UP THE ANTE, IF YOU WILL, AND SEEK CIVIL MONEY PENALTIES. BUT WE DIDN'T TAKE THAT COURSE OF ACTION. WE CONTINUALLY ENGAGED IN VOLUNTARY RESOLUTION OF THOSE COMPLAINTS. I CAN TELL YOU NOW THIS ADMINISTRATION IS MORE INTERESTED IN ENSURING THAT THERE IS COMPLIANCE WITH THE RULE. AND SO WHAT SOME OF YOU COMPLIANCE OFFICERS AND PRIVACY OFFICERS WILL BE HEARING FROM THE INVESTIGATORS GOING FORWARD IS THAT IF YOU ENGAGE OR IF YOUR ENTITY HAS ENGAGED IN THE SAME SORT OF VIOLATIONS OVER AND OVER AND WE'VE ASKED YOU TO TAKE CORRECTIVE ACTION BY REVISING OR AMENDING YOUR POLICIES AND PROCEDURES, AND YOU'VE DONE THAT AND YOU'VE ALSO TRAINED YOUR STAFF AS PART OF THE CORRECTIVE ACTION PLAN AND IN SOME INSTANCES PERHAPS SANCTIONED YOUR WORKFORCE. ON THE FOURTH, FIFTH, SIXTH, AND SEVENTH VIOLATION, I DON'T KNOW WHAT ELSE WHAT WE CAN DO. YOU'VE ALREADY REVISED THE POLICIES. YOU'VE ALREADY TRAINED THE STAFF. AND YOU'VE GOTTEN RID OF THE EMPLOYEE. SO--AND, YOU KNOW, COMPLAINT SEVENTH, EIGHT, AND NINE, I THINK IT'S NOT A DETERRENT ANYMORE TO TALK ABOUT IT. I THINK SOME ACTION NEED TO BE TAKEN. THE PENALTIES, I MIGHT ADD, FOR VIOLATIONS OF THE PRIVACY RULE HAVE ALSO BEEN



INCREASED UNDER THE HITECH ACT. SOME OF YOU MAY BE AWARE THAT IN FEBRUARY OF 2009, SHORTLY AFTER THIS PRESIDENT TOOK OFFICE, A LAW WAS PASSED CALLED THE HITECH ACT WHICH PRETTY MUCH PLUGGED UP A LOT OF THE HOLES THAT WAS IN THE PRIVACY RULE. AND SO NOW, WE CAN GET GREATER CIVIL MONEY PENALTIES, PATIENTS HAVE GREATER RIGHTS AND AS YOU KNOW, PROVISIONS FOR MORE TRAINING AND TECHNICAL ASSISTANCE FOR COVERED ENTITIES. FOR EXAMPLE--AND AGAIN, WE'LL DISCUSS THIS IN GREATER DETAIL LATER ON, YOUR BUSINESS ASSOCIATES HERE BEFORE WAS NOT RESPONSIBLE FOR ANY BREACHES OF EITHER THE PRIVACY RULE OR THE SECURITY RULE. NOW, UNDER THE HITECH ACT, THE BUSINESS ASSOCIATES IN AND OF THEMSELVES ARE RESPONSIBLE FOR ANY BREACHES THAT OCCUR, AND SO THE COVERED ENTITIES NO LONGER HAVE TO ASSUME LIABILITY FOR THE MALFEASANCE, IF YOU WILL, OF THE BUSINESS ASSOCIATES. THE LAST GOAL, IF YOU WILL, OF THE PRIVACY RULE THAT I'D LIKE TO DISCUSS IS THE POINT THAT THE PRIVACY RULE IS ALSO ENACTED TO STRIKE A BALANCE BETWEEN THE NECESSITY OF DISCLOSURE FOR PUBLIC PURPOSES OR THE PUBLIC GOOD AND TO ENSURE THE PRIVACY OF PATIENT'S PROTECTED HEALTH INFORMATION. THAT'S ANOTHER OVERARCHING THEME THROUGHOUT THE PRIVACY RULE AS WELL THE SECURITY RULE. THE OFFICE OF CIVIL RIGHTS PROMOTES AND ISSUE THOSE COMPLIANCE WITH THE HIPAA LAWS THROUGH VARIOUS METHODS. AND THESE METHODS ALSO APPLY TO OUR INVESTIGATION OF COMPLAINTS FOR CIVIL RIGHTS AS WELL. WE ENSURE COMPLIANCE THROUGH INVESTIGATION OF COMPLAINTS; THAT'S WHERE AN INDIVIDUAL OR

SOMEONE ON THE INDIVIDUAL'S BEHALF MAY FILE A COMPLAINT ALLEGING THAT A COVERED ENTITY HAS VIOLATED THE INDIVIDUAL'S PRIVACY OR SECURITY RIGHTS. AND WHAT WE DO IS WE WILL NOTIFY THE COVERED ENTITY THAT WE RECEIVED A COMPLAINT AND WE SENT OUT WHAT WE CALL A NOTIFICATION LETTER. WE ALSO SEND OUT AT THE SAME TIME THAT WE SEND OUT THE NOTIFICATION LETTER AN ACCEPTANCE LETTER TO THE INDIVIDUAL WHO SENT IN A COMPLAINT TO INFORM THEM OFFICIALLY THAT THE COMPLAINT HAS BEEN ACCEPTED AND WILL BE INVESTIGATED. AND THEN WE ENGAGE IN THIS VOLUNTARY COLLABORATIVE EFFORT WITH THE COVERED ENTITY TO, ONE, FIND OUT WHETHER OR NOT IN FACT A VIOLATION OF EITHER THE PRIVACY RULE OR SECURITY RULE OCCURED. SO WHAT WE ASKED THE COVERED ENTITIES TO DO IS TO DO AN INTERNAL INVESTIGATION OF THEIR OWN, IF THEY HAVEN'T ALREADY RECEIVED THE COMPLAINT. OFTENTIMES, BEFORE A COMPLAINANT WILL FILE WITH US, THEY'LL FILE A COMPLAINT WITH THE PRIVACY OFFICER OF THE COVERED ENTITY. AND THAT'S THE TIME FOR THE COVERED ENTITY TO REALLY TAKE CHARGE AND LOOK INTO THE MATTER. IF THEY FIND THAT, YOU KNOW, PERHAPS THERE WAS A BREACH OR A VIOLATION, TO COME UP WITH A CORRECTIVE ACTION PLAN. AND IF IT'S NECESSARY, YOU KNOW, REVISE THE POLICIES AND PROCEDURES, TRAIN THE WORKFORCE, AND IN SOME INSTANCES SANCTION THE STAFF. BUT BY THE TIME YOU GET OUR NOTIFICATION LETTER, YOU KNOW, YOU WOULD HAVE SAVED YOURSELF A LOT OF HEARTACHE IF YOU'VE TAKEN THOSE STEPS BECAUSE THEN ALL YOU HAVE TO DO IS SEND IN THAT

PACKAGE TO US. AND BECAUSE THIS IS A VOLUNTARY COLLABORATIVE EFFORT, WE'LL TAKE A LOOK AT IT AND SEE IF ANYTHING ELSE NEEDS TO BE DONE. YOU MAY BE ONE OF THESE EFFICIENT PRIVACY OFFICERS WHO REALLY, YOU KNOW, DOT ALL THE I'S AND CROSSED THE T'S. AND AT THAT POINT, WHAT WE'LL DO IS JUST CONTACT YOU TO TELL YOU WHETHER OR NOT, YOU KNOW, WHAT YOU DID WAS SUFFICIENT ENOUGH AND THEN PERHAPS WE CAN CLOSE THE CASE OR, YOU KNOW, PROVIDE YOU WITH SOME TECHNICAL ASSISTANCE AS TO MAYBE ONE OR TWO OTHER THINGS SUCH AS MITIGATION OR PERHAPS ANY HARM THAT MAY HAVE OCCURRED TO THE COMPLAINANT BECAUSE OF THE VIOLATION. ANOTHER WAY THAT WE ENSURE OUR COMPLIANCE WITH THE HIPAA LAWS IS BY CONDUCTING COMPLIANCE REVIEWS. THE COMPLIANCE REVIEW'S, WE BELIEVE, AN EFFECTIVE WAY TO PREVENT ANY COMPLAINT FROM COMING TO THE OFFICE. AND WHAT WE DO BASICALLY IS IF WE HAVE ANY ANECDOTAL INFORMATION ABOUT-- BEING A PROBLEM AT A PARTICULAR ENTITY, WE'LL GO CONTACT THE ENTITY, INFORM THEM THAT WE'RE EITHER GOING TO DO AN ONSITE OR JUST REQUEST DOCUMENTATION, DEPENDING ON THE NATURE OF THE COMPLAINT. AND THEN WE'LL JUST REVIEW, YOU KNOW, A PARTICULAR ISSUE OR WE MAY DO A BROADER REVIEW TO SEE WHETHER OR NOT THE ENTITY IS IN COMPLIANCE WITH EITHER THE HIPAA PRIVACY RULE OR THE SECURITY RULE. COMPLIANCE REVIEWS CAN TAKE, YOU KNOW, QUITE A BIT OF TIME TO COMPLETE. IT'S MY CONTENTION THAT IF YOU HAVE A PROACTIVE COMPLIANCE OFFICER OR PRIVACY OFFICER, THAT THEY'RE CONTINUALLY OR SOME SORT OF PERIODIC BASIS REVIEWING THE

POLICIES AND PROCEDURES TO MAKE SURE THAT THEY STAY CURRENT WITH WHAT'S GOING ON WITH THE HOSPITAL AS THE HOSPITAL CHANGES, OFFICES OF THE SMALL PRACTITIONER AS THE PRACTICE, YOU KNOW, GROWS AS WELL AS CONTINUALLY TRAINING THE WORKFORCE. YOU KNOW, THERE'S A LOT OF TURNOVER IN A LOT OF PLACES. AND AS PEOPLE COME IN AND PEOPLE LEAVE, THE NEW STAFF NEEDS TO BE TRAINED. AND WE OFTENTIME FIND THAT, YOU KNOW, A LOT OF COVERED ENTITIES ENGAGE IN A ONE-SHOT, ONE-SHOT DEAL WITH RESPECT TO TRAINING. AND THEN THAT CAN SET YOU UP FOR A POSSIBLE VIOLATION IF YOU HAVE A WORKFORCE MEMBER WHO'S ACCUSED OF BREACHING ONE OF THE RULES. AND WHEN WE DO AN INVESTIGATION AND PERHAPS INTERVIEW THAT INDIVIDUAL, THE INDIVIDUAL WILL SAY, "WELL, I DIDN'T KNOW ANY BETTER. I NEVER RECEIVED ANY HIPAA TRAINING." WELL, IT'S NOT THE INDIVIDUAL EMPLOYEE WHO'S GOING TO BE HELD ACCOUNTABLE FOR THE BREACH; IT'S THE COVERED ENTITY. SO IT WOULD BEHOOVE YOU TO MAKE SURE AS YOUR STAFFS TURNS OVER THAT YOU HAVE SOME SORT OF TRAINING PROGRAM IN PLACE TO CAPTURE THOSE WHO MAY NOT HAVE BEEN IN ON A FIRST CLASS OF AN ORIENTATION SO THAT, YOU KNOW, NO ONE HAS AN EXCUSE FOR SAYING THAT THEY DIDN'T UNDERSTAND WHAT THOSE TWO RULES REQUIRED. ANOTHER WAY THAT WE PROMOTE AND ENSURE COMPLIANCE WITH THE HIPAA PRIVACY RULE AS WELL AS SECURITY RULE IS BY PROVIDING TECHNICAL ASSISTANCE. AND TECHNICAL ASSISTANCE IS PROVIDED DURING INVESTIGATIONS, DURING COMPLIANCE REVIEWS, AND SOMETIMES DURING PUBLIC EDUCATION AND OUTREACH. WE

ENCOURAGE COVERED ENTITIES TO CONTACT OUR OFFICE. WE ARE ONE OF, I BELIEVE, FEW AGENCIES THAT ACTUALLY HAVE A TOLL-FREE NUMBER WHERE WHEN YOU CALL US, SOMEBODY ACTUALLY ANSWERS THE PHONE. SO YOU CAN CALL OUR OFFICE; WE HAVE THE INVESTIGATORS WHO MAN AND WE CALL IT THE INTAKE LINE. AND ANY QUESTIONS THAT YOU MAY HAVE FROM TIME TO TIME ABOUT EITHER OF THOSE RULES, SOMEONE IS THERE TO ASSIST YOU AND PROVIDE THE TECHNICAL ASSISTANCE. YOU DON'T HAVE TO CONTACT, YOU KNOW, A LAWYER OR A LAW FIRM AND PAY, YOU KNOW, THESE HIGH FEES JUST TO HAVE A SIMPLE QUESTION ANSWERED. WE ALSO HAVE A WEBSITE WITH FREQUENTLY ASKED QUESTIONS OR FAQs, WHERE--THAT YOU COULD USE AT YOUR DISPOSAL WHEN THERE'S AN ISSUE THAT YOU MAY COME ACROSS AND YOU JUST NEED A QUICK ANSWER. I WOULD ENCOURAGE YOU TO LOOK AT THE WEBSITE FIRST BECAUSE THERE'S A TON OF ISSUES THAT HAVE BEEN ADDRESSED ON THE WEBSITE WITH SOME HYPOTHETICALS AND SOME SCENARIOS THAT MAY BE IN LINE WITH YOUR SITUATION. AND THEN IF YOU'RE STILL NOT SURE, THEN YOU CAN GIVE US A CALL. AND LIKE I SAID, YOU KNOW, WE ANSWER THE PHONE AND WE'LL GLADLY ASSIST YOU. WITH RESPECT TO CONDUCTING OUTREACH, IF YOU HAVE A HEALTH FAIR OR AN EMPLOYEE TRAINING DAY OR SOME OTHER EVENT IN YOUR FACILITY AND YOU WOULD LIKE TO INCLUDE THE OFFICE OF CIVIL RIGHTS SO THAT WE COULD PROVIDE LITERATURE AND TECHNICAL ASSISTANCE AND INFORMATION ABOUT THE RULES, BY ALL MEANS, GIVE OUR OFFICE A CALL AND WE CAN SET THAT UP WHERE AN INVESTIGATOR WILL COME OUT. AND IF IT'S MANNING A TABLE AND HANDING OUT

LITERATURE OR IF IT'S GIVING A PRESENTATION LIKE THIS TO FURTHER CLARIFY WHAT THE HIPAA RULES AND LAWS MEAN, WE'LL BE GLAD TO DO THAT. SO, YOU GUYS ARE TAXPAYERS AS WELL AND WE WORK FOR YOU. SO, DON'T THINK OF US ALWAYS AS THE BIG BAD GOVERNMENT. WE'RE HERE TO, YOU KNOW, PREVENT ANY BREACHES AND VIOLATION FROM OCCURRING. WE ALSO HAVE OTHER ENFORCEMENT TOOLS THAT WE USE IF NECESSARY TO ENSURE COMPLIANCE. AND AGAIN, THE LAST ADMINISTRATION, YOU KNOW, PREFERRED TO USE THESE AS A LAST RESORT, AND AS RESOLUTION AGREEMENTS AS WELL AS THE CIVIL MONEY PENALTIES. RESOLUTION AGREEMENTS DON'T NECESSARILY HAVE TO RESULT IN CIVIL MONEY PENALTIES. IT COULD BE A SITUATION WHERE YOUR PARTICULAR FACILITY JUST DOESN'T HAVE THE RESOURCES TO BRING IN A CONSULTANT OR HAVE THE EXPERTISE TO PUT TOGETHER YOUR POLICIES AND PROCEDURES OR TRAIN YOUR WORK FORCE. AND SO YOU NEED TIME TO GET UP TO SPEED WITH RESPECT TO THAT OR COULD BE A SMALL PRACTITIONER, YOU KNOW, PRIVATES OR SOLE PRACTITIONER HERE WHO IS ONLY FAMILIAR WITH THE PRIVACY RULE AND REALLY NOT THE SECURITY RULE AND ALL THAT ENCOMPASSES, YOU KNOW, BEING IN COMPLIANCE WITH THE SECURITY RULE. WHAT WE'LL DO IS WE'LL, IF WE GET A COMPLAIN AND WE REALIZE, YOU KNOW, THE SUBSTANTIAL, TECHNICAL ASSISTANCE THAT NEED TO BE PROVIDED HERE, WE MAY ENGAGE IN A RESOLUTION AGREEMENT WHERE SOME MONITORING WOULD TAKE PLACE UNTIL WE HAVE SOME ASSURANCE THAT YOU'RE IN COMPLIANCE AND YOU'LL BE ABLE TO REMAIN IN COMPLIANCE ON YOUR OWN. AND SO

IT DOESN'T NECESSARILY HAVE TO BE A BAD THING WHEN YOU GET AN OFFER FROM US TO ENGAGE IN A RESOLUTION AGREEMENT. BUT THOSE ARE SOME OF THE WAYS THAT WE PROMOTE AND ENSURE COMPLIANCE WITH THE HIPAA PRIVACY AND SECURITY RULE. SINCE APRIL OF 2003 TO APRIL OF THIS YEAR, THE OFFICE FOR CIVIL RIGHTS HAS RECEIVED NATIONALLY ABOUT 51,762 COMPLAINTS. APPROXIMATELY 89% OF THOSE COMPLAINTS HAVE BEEN RESOLVED WHICH COME NOW TO ABOUT 46,315. I HAVE THIS ALL WRITTEN DOWN; I DON'T REMEMBER. ALL INVESTIGATIONS HAVE RESULTED IN CHANGES IN PRIVACY PRACTICES AND CORRECTIVE ACTIONS IN OVER 10,749 OF THOSE CASES. AND THOSE--THAT CORRECTIVE ACTION OBTAINED BY OUR OFFICE HAS RESULTED IN SYSTEMIC CHANGES FOR THE BENEFIT OF THE INDIVIDUALS THAT THE COVERED ENTITY SERVED. SO, AGAIN, BECAUSE WE GET A COMPLAINT, IT'S NECESSARILY A BAD THING; IT'S AN OPPORTUNITY AT LEAST IN OUR OPINION TO MAKE SURE THAT NOT ONLY THAT INDIVIDUAL HAS A REMEDY TO ADDRESS THE ALLEGED WRONG BUT ALL INDIVIDUALS--AS THOSE INDIVIDUALS WHO ARE SIMILARLY SITUATED ALSO ARE NOT ABRIDGED OR THEIR RIGHTS ARE NOT ABRIDGED IN THE SAME WAY. THE COMPLIANCE ISSUES THAT WE'VE INVESTIGATED MOST FREQUENTLY ARE--AND I'LL LIST THEM IN ORDER. THESE ARE THE MOST FREQUENT COMPLAINTS THAT WE GET: IMPERMISSIBLE USES AND DISCLOSURES OF AN INDIVIDUAL'S PROTECTED HEALTH INFORMATION--THE NUMBER ONE COMPLAINT, OVER AND OVER AGAIN; THE LACK OF ADEQUATE SAFEGUARDS TO PROTECT IDENTIFIABLE HEALTH INFORMATION--AND THAT, SOMETIMES, WE GET NOT ONLY WITH

THE PRIVACY RULE BUT ALSO THE SECURITY RULE WITH RESPECT TO THE ELECTRONIC HEALTH INFORMATION OR ELECTRONIC HEALTH RECORDS; THE REFUSAL OR THE FAILURE BY THE COVERED ENTITIES TO PROVIDE INDIVIDUALS WITH ACCESS TO THEIR HEALTH INFORMATION--AND I ALWAYS FIND THAT PUZZLING WHEN WE GET A COMPLAINT WHERE AN INDIVIDUAL SAYS, "WELL, I WENT TO MY DOCTOR'S OFFICE AND I TOLD HIM I WAS RELOCATING TO ANOTHER STATE AND I NEED MY SON'S PEDIATRIC RECORDS," AND THE COVERED ENTITY REFUSES, THE DOCTOR'S OFFICE REFUSES TO GIVE THE PARENT THE RECORDS. I DON'T GET IT. YOU KNOW, MAYBE THERE'S SOME ISSUES THERE. I'M NOT A PHYSICIAN. MY TRAINING IS IN THE LAW. BUT I DON'T UNDERSTAND. I WOULD THINK THAT, YOU KNOW, MOST PEOPLE WOULD UNDERSTAND HOW IMPORTANT PEDIATRIC RECORDS ARE AND THAT, YOU KNOW, THERE'S NOTHING SECRETIVE ABOUT THEM. YOU GIVE THE PARENT THE RECORDS TO LET THEM MOVE ON TO WHATEVER STATE SHE'S GOING TO. BUT YOU'D BE SURPRISED HOW MANY COMPLAINTS WE GET, YOU KNOW, ALONG THOSE LINES OR IN SOME SITUATIONS, THE COVERED ENTITIES, PARTICULARLY THE SMALL PRACTITIONERS DON'T UNDERSTAND THAT YOU DON'T HAVE TO GIVE UP YOUR ORIGINAL RECORDS. I BELIEVE UNDER THE STATE LAWS, MOST STATE LAWS, YOU CAN'T GIVE AWAY YOUR ORIGINAL RECORDS. SO YOU MAKE A COPY OF THE RECORDS AND YOU PROVIDE THEM TO THE PATIENT. BUT WE--YOU KNOW, THAT'S THE THIRD MOST FREQUENT COMPLAINT THAT WE GET, THAT THE PATIENTS CAN'T GET ACCESS TO THEIR HEALTH RECORDS. AND THERE ARE SOME EXCEPTIONS AND WE'LL GET INTO THIS LATER ON



IN THE RULE THAT SAYS CERTAIN RECORDS ARE NOT ACCESSIBLE BY THE PATIENT, YOU KNOW. FOR EXAMPLE, MENTAL HEALTH RECORDS, YOU KNOW, FOR VARIOUS PUBLIC POLICY REASONS. BUT, CERTAINLY, YOU KNOW, ORDINARY, PRIMARY CARE PHYSICIAN RECORDS ARE ACCESSIBLE AND SHOULD BE ACCESSIBLE. THE FOURTH MOST FREQUENT COMPLAINT WE GET IS THE DISCLOSURE BY COVERED ENTITIES OF MORE THAN THE MINIMALLY NECESSARY PROTECTED HEALTH INFORMATION, AND THAT'S THE SITUATION WHERE AN INDIVIDUAL SAYS I'VE BEEN OUT OF WORK, I NEED A DOCTOR'S NOTE. CAN YOU GIVE ME A DOCTOR'S NOTE? OR BETTER YET, CAN YOU FAX A DOCTOR'S NOTE OVER TO MY EMPLOYER, AND WHAT I WANT YOU TO DO IS TELL THE EMPLOYER THAT, YOU KNOW, I WAS HERE, I WAS SEEN ON THIS DATE AND THAT, YOU KNOW, I CAN RETURN TO WORK"; GIVE ME A CLEARANCE TO RETURN TO WORK. YOU'D BE SURPRISED WHERE WE GET COMPLAINTS ALLEGING THAT THE PHYSICIAN SENT THE PATIENT'S ENTIRE MEDICAL RECORD. "WHAT ARE YOU SENDING THAT ENTIRE MEDICAL RECORD FOR?" BY IT HAPPENS, AND IT'S NOT SOMETHING THAT HAPPENS SELDOM; IT HAPPENS OFTEN. AND THAT'S SET UP FOR THE INVESTIGATION. CLEARLY, THERE'S A MINIMUM NECESSARY REQUIREMENT IN A RULE, AND IT'S A COMMONSENSE REQUIREMENT. YOU KNOW, THAT'S THE WHOLE THEME OF THE RULE IS TO PROTECT THE PRIVACY OF THE PATIENT'S HEALTH INFORMATION. SO, CLEARLY, IT DOESN'T MAKE ANY SENSE TO SEND AN ENTIRE RECORD WHEN ALL THE PATIENT WANTS IS AN EXCUSE TO GO BACK TO--A DOCTOR'S NOTE AS AN EXCUSE TO GO BACK TO WORK. THE FIFTH MOST FREQUENT COMPLAINT WE GET IS THE FAILURE BY COVERED

ENTITIES TO ADDRESS COMPLAINTS THAT THEY RECEIVE. YEAH, THAT'S ANOTHER ONE THAT GETS ME SOMETIMES. THE PRIVACY RULE HAS ADMINISTRATIVE REQUIREMENTS IN IT, AND YOU'RE REQUIRED AS PART OF THOSE ADMINISTRATIVE REQUIREMENTS TO HAVE A COMPLAINT PROCESS IN PLACE. SO, I DON'T UNDERSTAND IF A COMPLAINANT SAYS TO, YOU KNOW, THE PRIVACY OFFICER, LISTEN HERE, YOU KNOW, THE DOCTOR WAS SCREAMING IN THE ELEVATOR, YOU KNOW, MY PROTECTED HEALTH INFORMATION AND I ASKED HIM, YOU KNOW, COULD HE, YOU KNOW, LOWER HIS VOICE, AND THE DOCTOR SAID WELL, I JUST TALK LOUD, YOU KNOW, AND REALLY BRUSHED ME OFF. AND THE PATIENT SAYS OK, YOU KNOW, I'M GOING TO GO AND MAKE A COMPLAINT ABOUT THIS; YOU KNOW, THIS IS THE FIRST TIME THAT THIS HAS HAPPENED. AND THEY GO TO THE PRIVACY OFFICER AND THE PRIVACY OFFICER, YOU KNOW, PRETTY MUCH, YOU KNOW, PLACATES THE COMPLAINANT AND THEN THE COMPLAINANT FOLLOWS UP AND FINDS OUT NOTHING ACTUALLY HAPPENED. THEN THE CLAIM GETS, YOU KNOW, FRUSTRATED AND UPSET, AND THEN FILES A COMPLAINT WITH US. AND SO WHEN WE CONTACT THE COVERED ENTITIES--I'M SURE NONE OF YOU IN THE AUDIENCE HAD THIS PROBLEM--THEY SAY, YEAH, WE GOT THE COMPLAINT; YEAH, THE DOCTOR WAS TALKING LOUD BUT WE DIDN'T THINK IT WAS A VIOLATION OF ANY OF THE RULES. SO WE ASK, "WELL, DID YOU DOCUMENT THE COMPLAINT? DID YOU DOCUMENT THE DISPOSITION OF THE COMPLAINT? AND THEN, YOU KNOW, THERE'S AN EERIE SOUND ON THE OTHER END. YEAH, THAT'S UNACCEPTABLE AT THIS STAGE; 70 YEARS INTO THE RULE, YOU SHOULD HAVE A COMPLAINT PROCESS IN

PLACE. THE MOST COMMON TYPES OF COVERED ENTITIES THAT HAVE BEEN REQUIRED TO TAKE CORRECTIVE ACTION ARE PRIVATE PHYSICIAN PRACTICES, THE NUMBER ONE ENTITY THAT'S BEING COMPLAINED ABOUT; HOSPITALS; OUTPATIENT FACILITIES; HEALTH PLANS; AND PHARMACIES, IN THAT ORDER. MY TIME IS ALMOST UP SO I'D LIKE TO LEAVE A LITTLE BIT OF A TIME FOR SOME QUESTION-AND-ANSWERS SO I'D LIKE TO LEAVE YOU WITH JUST SOME TIPS FOR WORKING WITH OUR OFFICE DURING A HIPAA INVESTIGATION, BE IT A PRIVACY RULE INVESTIGATION OR A SECURITY RULE INVESTIGATION. WHEN YOU RECEIVE THE NOTIFICATION LETTER, CONTACT THE INVESTIGATED AS NAMED IN THE LETTER. THAT'S IF YOU'RE INTERESTED IN ENGAGING IN SOME SORT OF VOLUNTARY RESOLUTION OUT OF COMPLAINT. THE INVESTIGATOR IS THERE TO ASSIST YOU. THIS IS NOT A GOT-YOU GAME THAT WE'RE ENGAGING IN HERE. IF YOU HAVE ANY QUESTIONS ABOUT THE INVESTIGATION PROCESS, YOU KNOW, OFTENTIMES, WE FIND THAT FOR SOME OF YOU, IT'S THE FIRST TIME THAT YOU RECEIVED A COMPLAINT FROM OUR OFFICE. SO, BY ALL MEANS, YOU KNOW, ASK QUESTIONS, ASK, YOU KNOW, WHICH SHOULD YOU DO NEXT, OR WHAT INFORMATION IS NEEDED AND WE'LL GLADLY PROVIDE THAT INFORMATION AND THIS IS NOT A SITUATION WHERE YOU HAVE TO INVOKE YOUR FIFTH AMMENDMENT RIGHTS BECAUSE YOU THINK, YOU KNOW, ON THE OTHER END, YOU'RE GOING TO GET SLAMMED. RESPOND TO THE LETTERS THAT YOU RECEIVE WHETHER OR NOT IT'S A DATA REQUEST LETTER OR NOTICE OF A PROPOSED TERMINATION. AND IF YOU CAN'T MAKE THE DUE DATE, THEN CALL THE INVESTIGATOR NAMED AND LET THE INVESTIGATOR KNOW

THAT "HEY, LISTEN HERE, I CAN'T MAKE THE DUE DATE." YOU CAN REQUEST A REASONABLE EXTENSION OF TIME. WE'RE PRETTY MUCH, YOU KNOW, REASONABLE FOLKS WHO ARE WORKING AT THE OFFICE OF CIVIL RIGHTS. WE UNDERSTAND THAT THINGS COME UP AND THAT YOU NEED MORE TIME. SO JUST REQUEST IT. IF YOU'RE AWARE OF A RULE BREACH, AS I SAID EARLIER, THEN, YOU KNOW, TAKE THE INITIATIVE TO DO SOME INTERNAL INVESTIGATION OR AN INQUIRY INTO THE MATTER, FORMULATE YOUR OWN CORRECTIVE ACTION PLAN, AND THEN SEND THAT TO US. IF YOU NEED TECHNICAL ASSISTANCE, ASK FOR IT. AND I HAD SAID BEFORE, BEFORE COMING, ACKNOWLEDGE THE ERRORS, AND THEN, YOU KNOW, DO WHAT'S NECESSARY TO MITIGATE THE HARM. AND UNDERSTAND THAT THESE INVESTIGATIONS TAKE PLACE OVER AN EXTENDED PERIOD OF TIME SO WE MIGHT NOT BE ABLE TO WRAP IT UP, YOU KNOW, NICE AND TIDY IN, YOU KNOW, A WEEK OR TWO WEEKS OR A MONTH. IT MAY TAKE MUCH LONGER; SO JUST BEAR WITH US. IT'S IN YOUR INTEREST. LAST, I JUST LIKE TO SAY THAT I HOPE THESE REMARKS HAVE BEEN HELPFUL TO YOU. I HOPE THIS HAS WHETTED YOUR APPETITE TO LEARN MORE ABOUT THESE TWO RULES. AND THIS AFTERNOON I AND MY COLLEAGUE, KELLY ROBSON, WHO'S SITTING OVER HERE IN THE FIRST ROW TO MY LEFT, WILL BE CONDUCTING A WORKSHOP WITH RESPECT TO THESE RULES. THANK YOU.